ETSI TS 102 887-2 V1.1.1 (2013-09)

Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices; Smart Metering Wireless Access Protocol; Part 2: Data Link Layer (MAC Sub-layer)

Reference
DTS/ERM-TG28-0427-2

Keywords
protocol, smart meter, SRD

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights 6
Foreword 6
Introduction 6
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 7
3 Definitions and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 8
4 Global modifications to normative references 9
5 Overview 10
6 Devices operating in Mode 1 11
6.1 General Description 12
6.2 MAC Protocol 12
6.2.1 MAC Functional Description 12
6.2.1.1 Channel Access 12
6.2.1.2 Starting and Maintaining PANs 12
6.2.1.3 Association and Disassociation 12
6.2.1.4 Transmission, Reception and Acknowledgement 12
6.2.2 MAC Frame Formats 13
6.2.2.1 Beacon Frame Format 13
6.2.2.2 Data Frame Format 13
6.2.2.3 Acknowledgement Frame Format 13
6.2.2.4 MAC Command Frame Format 13
6.2.2.5 Multipurpose Frame Format 13
6.2.2.6 Multipurpose Blink Frame Format 13
6.2.2.7 LE Wake-up Frame Format 13
6.2.2.8 Frame Compatibility 14
6.2.3 Information Elements 14
6.2.3.1 EMSDU IE 14
6.2.3.2 MLM IE 14
6.2.3.3 LE CSL IE 14
6.2.3.4 LE RIT IE 14
6.2.3.5 Rendezvous Time IE 14
6.2.3.6 Channel Hopping IE 14
6.2.3.7 Hopping Timing IE 14
6.2.3.8 EB Filter IE 14
6.2.3.9 MAC Metrics IE 15
6.2.3.10 AllMAC Metrics IE 15
6.2.3.11 SUN Device Capabilities IE 15
6.2.3.12 Unmanaged ID Space IEs 16
6.2.3.13 IE List Termination IE 16
6.2.4 MAC Commands 16
6.3 MAC Services 16
6.3.1 Communication Notification Primitives 16
6.3.2 Primitives for Channel Scanning 17
6.3.3 Primitives for Updating the Superframe Configuration 17
6.3.4 Primitives for Beacon Generation 17
6.3.5 MAC Data Service 17
6.3.6 MAC Constants and PIB Attributes 17
6.4 Security 18

6.5 Protocol Implementation Conformance Statement (PICS) 18
7 Devices Operating in Mode 2 18
7.1 Architecture 18
7.2 Data Transfer Service Provided 19
7.3 Security Services 20
7.4 Data Structures 20
7.5 Representation Order 20
7.6 Addresses 20
7.7 Frame Format 20
7.7.1 Secured Frame Format 20
7.7.1.1 Frame Control 20
7.7.1.2 Destination Address 21
7.7.1.3 Source Address 21
7.7.1.4 Secure Envelope IE 21
7.7.1.5 Frame Check Sequence 21
7.8 Information Elements 21
7.8.1 Node Announcement (NA) IE 22
7.8.2 Secure Envelope (SE) IE 22
7.9 Security Suite Families 22
7.9.1 Auxiliary Security Header (ASH) 22
7.9.1.1 Transmission 23
7.9.1.2 Reception 23
7.9.2 Cipher Suite Tuple 23
7.9.2.1 Authentication HMAC 24
7.9.2.2 Authentication CCM and Encryption None 24
7.9.2.3 Authentication GCM and Encryption None 25
7.9.2.4 Authentication and Encryption CCM 25
7.9.2.5 Authentication and Encryption GCM 25
7.9.2.6 Authentication HMAC and Encryption CTR 26
7.9.3 Negotiated Session (NS) 26
7.9.3.1 Transmission 27
7.9.3.1.1 Authentication HMAC 27
7.9.3.1.2 Authentication CCM and Encryption None 27
7.9.3.1.3 Authentication GCM and Encryption None 28
7.9.3.1.4 Authentication/Encryption Mode CCM 29
7.9.3.1.5 Authentication/Encryption Mode GCM 30
7.9.3.1.6 Authentication HMAC and Encryption CTR 30
7.9.3.2 Reception 31
7.9.3.2.1 Authentication HMAC 32
7.9.3.2.2 Authentication CCM and Encryption None 32
7.9.3.2.3 Authentication GCM and Encryption None 32
7.9.3.2.4 Authentication and Encryption CCM 33
7.9.3.2.5 Authentication and Encryption GCM 34
7.9.3.2.6 Authentication HMAC and Encryption CTR 35
7.9.4 Session Key (SK) IE 36
7.9.4.1 NS New Session Message 36
7.9.4.2 NS Session Created Message 36
7.9.4.3 NS Session Acknowledgement Message 37
7.9.4.4 NS Session Destruction Message 37
7.10 Constants and Parameter Attributes 38
7.11 Service Interfaces 38
7.11.1 M-DATA.request 38
7.11.2 M-DATA.indication 39
7.11.3 MAC Layer Management Negotiated Session Interface (MLM-NS) 39
7.11.4 MLM-NS.request 40
7.11.4.1 MLM-NS New Session Request 40
7.11.4.2 MLM-NS Session Created Request 40
7.11.4.3 MLM-NS Session Acknowledge Request 41
7.11.4.4 MLM-NS Session Destruction Request 41
7.11.5 MLM-NS.indication 41
7.11.5.1 MLM-NS New Session Indication 41

7.11.5.2 MLM-NS Session Created Indication 42
7.11.5.3 MLM-NS Session Acknowledge Indication 42
7.11.5.4 MLM-NS Session Destruction Indication 42
7.12 Functional description 43
7.12.1 Channel Function 43
7.12.2 Channel Table 43
7.12.3 Timing Accuracy 43
7.12.4 Synchronization 43
7.12.5 CSMA 43
7.12.6 Frame Processing 43
7.12.7 Frame Counter 43
7.12.8 Information Element Processing 44
7.12.8.1 EMSDU IE 44
7.12.8.2 Secure Envelope IE 44
7.12.8.3 SK IE 44
7.12.9 Data Transfer Services 46
7.12.9.1 Unicast Data Transfer 46
7.12.9.2 Beacon Data Transfer 46
7.12.9.3 Broadcast Data Transfer 46
7.12.9.4 Multicast Data Transfer 46
7.13 Operating Class 47
7.13.1 Regulatory Domain 47
7.13.1.1 Global Operating Class 47
7.13.1.2 US Operating Class 47
7.13.1.3 Japan Operating Class 47
7.13.1.4 Europe Operating Class 47

8 Negotiation Session (NS) Protocol 47
8.1 NS State Machine Representation 47
8.2 Necessary Conditions 48
8.3 Initiation 48
8.4 Response 49
8.5 Confirmation 49
8.5.1 States 50
8.5.1.1 Start 50
8.5.1.2 Session Wait 50
8.5.1.3 Ack Wait 50
8.5.1.4 Established 50
8.5.2 Events 50
8.5.2.1 Timeout 50
8.5.2.2 Retry Exceeded 50
8.5.2.3 Constants and Attributes 51
8.6 Key Derivation Function 51
8.6.1 KDF 1 - SP800-108-CMAC 51

9 PICS Proforma 51

History 55

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electromagnetic Compatibility and Radio Spectrum matters (ERM)

The present document is part 2 of a multi-part deliverable covering Short Range Devices; Smart Metering Wireless Protocol.

Part 1: "PHY Layer";

Part 2: "**Data Link Layer (MAC sub-layer)**".

Introduction

The present document, together with its associated PHY Technical Specification [1], provide radio communications connectivity for continuously powered or battery operated Smart Metering devices which, when coupled with suitable transport protocols, support advanced metering and other energy related applications. The MAC/PHY combination is also suitable for a wide range of sensor and Machine-to-Machine applications characterised by low device duty cycle and operation in shared spectrum.

This wide range of applications requires efficient connectivity protocol support for intermittent bi-directional data exchanges between devices in both low density (e.g. rural) and high density (e.g. urban) environments covering operations as simple as discovery and connection between one pair of devices (e.g. for walk-by meter reading) up to networks of many devices sharing a Network Point of Attachment to an external wide area network.

Spectrum sharing imposes additional requirements on the lower layer communications protocols governed by regulations limiting power and duty cycle among other characteristics. Such regulations taken into account by the present document include those governing the operation of Short Range Devices. Simple and low density deployments may be supported by distributed or cluster-based control algorithms, e.g. as found in [3] and [4], operating on a single channel. Frequency agility to select or change operating channel to minimise interference is advantageous for these applications but not essential for their operation.

Dense deployments and more complex applications may be constrained by spectrum sharing rules designed to limit the interference to other devices or services from the data traffic generated. In these cases the optimum control algorithms spread the population of devices uniformly over the available spectrum (channels) to minimise the number of devices on any given channel thereby minimising interference from their generated traffic. Device behaviour defined in [2] automatically distributes devices over the available channels by using device-centric pseudo-random channel hopping but also supports single channel operation via a degenerate hopping algorithm always returning the same channel number.

Both approaches to systems design may be deployed using the same PHY protocol and in the same frequency range and it is therefore necessary to include facilities to discriminate between information belonging to each MAC approach. Nothing prevents an implementation choosing to use only one of the alternate approaches or supporting both and the present document provides the necessary data structure encoding to identify each unit of information in its correct context.

1 Scope

The present document is the second part of the Smart Metering Wireless Access Protocol describing the data structures and functional operation of Smart Metering and other applications intending to use spectrum resources covered by TS 102 887-1 [1] Physical Layer.

TS 102 887-1 [1] is derived from IEEE 802.15.4g-2012™ [5] and the present document is derived from IEEE 802 15.4-2011™ [3], IEEE 802.15.4e-2012™ [4] and ANSI/TIA-4957-200 [2] together with specific enhancements or adaptations for the European context.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 102 887-1: "Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices; Smart Metering Wireless Access Protocol; Part 1: PHY layer".

[2] ANSI/TIA-4957.200: "Layer 2 Standard Specification for the Smart Utility Network".

[3] IEEE 802.15.4-2011™: "IEEE Standard for Local and metropolitan area networks-- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)".

[4] IEEE 802.15.4e-2012™: "IEEE Standard for Local and metropolitan area networks-- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer".

[5] IEEE 802.15.4g-2012™: "IEEE Standard for Local and metropolitan area networks-- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks".

[6] FIPS 197 (November 26, 2001): "Advanced Encryption Standard (AES)".

[7] NIST Special Publication 800-108 (October 2009): "Recommendation for Key Derivation Using Pseudorandom Functions", US National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IEEE Standards Association Registration Authority.

NOTE: Available at: http://standards.ieee.org/develop/regauth/

[i.2] IEEE-Standards Association Guidelines for 64-bit Global Identifier (EUI-64™).

NOTE: Available at: http://standards.ieee.org/develop/regauth/tut/eui64.pdf

[i.3] IEEE-Standards Association Standard Group MAC Addresses: A Tutorial Guide.

NOTE: Available at: http://standards.ieee.org/develop/regauth/tut/macgrp.pdf

[i.4] IEEE-Standards Association Use of the IEEE assigned Organizationally Unique Identifier with ANSI/IEEE Std 802-2001 Local and Metropolitan Area Networks.

NOTE: Available at: http://standards.ieee.org/develop/regauth/tut/lanman.pdf

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

beacon: periodically transmitted Frame

channel function: function that computes the channel number from a Channel Table as a function of time

channel table: standardized representation of the channels of a frequency band

frame: data structure carrying a MAC Protocol Data Unit

Protocol Data Unit (PDU): unit of information exchanged by MAC entities and carries client data and/or MAC protocol information

neighbour: node is a neighbour of another node if it is in direct communication range

node: conceptual entity embodying an implementation of MAC functionality as defined in the present document

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACK	ACKnowledgement
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
ASH	Auxiliary Security Header
CCM	Counter with CBC-MAC Mode
CMAC	Cipher-based Message Authentication Code
CSL	Coordinated Sample Listening
CSMA	Carrier Sense Multiple Access
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
CST	Cipher Suite Tuple
CTR	Counter (AES, Counter Mode)
DSME	Deterministic and Synchronous Multi-channel Extension
EB	Enhanced Beacon
EMSDU	Encapsulated MSDU
EUI	Extended Universal Identifier
FC	Flow Control
FCS	Frame Check Sequence
FDI	Fractional Dwell Interval
FSI	Fractional Sequence Interval
GCM	Galois Counter Mode (AES)
GFSK	Gaussian-filtered Shift Keying
GTS	Guaranteed Time Slot
HMAC	Hash-based Message Authentication Code
IE	Information Element
KDF	Key Derivation Function
LE	Low Energy

LE-RIT	Low Energy Receiver Initiated Transmission
LLDN	Low Latency Deterministic Network
LR-WPAN	Low Rate Wireless Personal Area Networks
MAC	Medium Access Control
ME	Management Entity
MHR	MAC Header
MIC	Message Integrity Check
MLM	MAC Layer Management
MLM-NS	MAC Layer Management Negotiated Session
MSDU	MAC Service Data Unit
NA	Node Announcement
NS	Negotiated Session
OCS	Operating Class Switching
OSI	Open Systems Interconnection
PAN	Personal Area Network
PDU	Protocol Data Unit
PIB	Personal Area Network Information Base
PICS	Protocol Implementation Conformance Statement
PPDU	PHY Protocol Data Unit
PRF	Pulse Repetition Factor
PS	Power Saving
QPSK	Quadrature Phase Shift Keying
RDV	Rendezvous
RIT	Receiver Initiated Transmission
SE	Secure Envelope
SK	Session Key
SMEP	Smart Metering Wireless Access Protocol
SSF	Security Suite Family
STD	State Transition Diagram
SUN	Smart Utility Network
TSCH	Time Slotted Channel Hopping
VSL	Vendor Specific Long
VSS	Vendor Specific Short
WPAN	Wireless Personal Area Networks

4 Global modifications to normative references

In order to make use, in the European market context, of the functionality defined in the normative references, the following adaptations are applied:

Table 1: Global Modifications to ANSI/TIA-4957.200

Section Reference in ANSI/TIA-4957.200	Action
2.1 Normative References [1] ANSI/TIA-4957.100 Layer 1 Standard Specification for the Smart Utility Network	Replace normative reference ANSI/TIA-4957.100 [1] with TS 102 887-1 [1].

Table 2: Global Modifications to IEEE 802.15.4-2011™

Section Reference in IEEE 802.15.4-2011™ [3]	Action
2 Normative references	The second Normative Reference (NITS/CWPAN Part 15.4) is not supported in the present document
Clauses 3 and 4	Clauses 3 and 4 of [3] are supported in the present document except for references to Guaranteed Time Slot services in clauses 4.1 and 4.5.1of [3]
Clause 5	Clause 5 of [3] is supported in the present document except for sub-clauses relating to Guaranteed Time Slot control and management. Clauses 5.1.7, 5.2.2.1.3, 5.2.2.1.4, 5.2.2.1.5 and 5.3.9 of [3] are not supported in the present document
Clauses 6 and 7	Clauses 6 and 7 of [3] are supported in the present document, excluding: clause 6.2.6 GTS management primitives, and clause 6.2.15 Primitives for specifying dynamic preamble of [3]
Clauses 8 to 15	Clauses 8 to 15 of [3] are not supported
Annex D PICS	Only those sections of the PICS relating to the clauses supported in the present document are relevant to ([4] Annex D)

Table 3: Global Modifications to IEEE 802.15.4e-2012™

Section Reference in IEEE 802.15.4e-2012™ [4]	Action
	Features of IEEE 802.15.4e-2012™ [4] are supported in the present document except those relating to TSCH, DSME and LLDN

Table 4: Global Modifications to IEEE 802.15.4g-2012™

Section Reference in IEEE 802.15.4g-2011™ [5]	Action
	Enhanced MAC frame formats and 4-octet FCS defined in clauses 5.2.1 and 5.2.2 of IEEE 802.15.4g-2012™ [5] are supported in the present document

5 Overview

This document describes the MAC sub-layer of the Smart Metering Wireless Access Protocol (SMEP). The SMEP PHY layer is derived from external specifications with enhancements specific to the European context. Similarly, the SMEP MAC sub-layer makes use of functionality in appropriate published standards adapted for use in the European context.

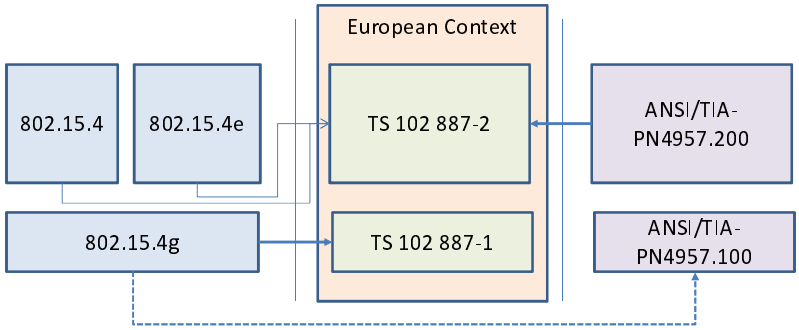

Figure 1: TS 102 887-2 Relation to External Standards

Figure 1 shows the relationship between the present document and the external standards it exploits.

IEEE 802.15.4-2011™ [3] is a multipurpose standard with many options for different application domains. IEEE 802.15.4e™ [4] defines a number of enhancements to 802.15.4 including a multipurpose frame type and information element features for extensibility. The present document exploits the basic 15.4 mode of operation and a subset of 15.4e. Devices operating according these IEEE specifications are said to be operating in Mode 1.

ANSI/TIA-4957.200 [2] is a standard specifically addressing the needs of Smart Utility Networks and the present document incorporates its functionality entirely. Devices operating according to the ANSI/TIA specification [2] are said to be operating in Mode 2.

Although operating over PHY specifications which would allow devices built to either IEEE 802.15.4 [3] or ANSI/TIA-4957.200 [2] to receive each others transmissions, the present document discriminates between them via different values of the Frame Type (see [4], clause 5.2.1.1) and Frame ID (see [2], clause 5.3) fields.

Where the European Context imposes additional requirements on the facilities offered by either IEEE or ANSI/TIA standards, the present document defines those necessary enhancements.

The physical layer supporting either mode of operation, TS 102 887-1 [1], is derived from IEEE 802.15.4g™ [5] adapted for the European context. The present document assumes that the TS 102 887-1 [1] PHY provides:

- One or more communications channels over which packets may be exchanged.
- Immediate access to the communications channel.
- Indication of channel busy via Energy Detection or other means.
- Transfer of frames without modification between source and destination nodes.

6 Devices operating in Mode 1

This clause defines the behaviour of a node operating in Mode 1 at the MAC sub-layer of the OSI communications model.

The IEEE 802.15.4 family of standards (see [3], [4] and [5]) defines a wide range of features that enable simple, low-cost and low-power Low Rate Wireless Personal Area Networks (LR-WPAN). This clause defines a subset of those features chosen for their widespread adoption, applicability to a range of applications and availability of interoperable implementations to provide the necessary functionality for intended applications including Smart Metering.

The key features of a node operating in Mode 1 include:

- Star or Peer-to-Peer network topology.
- Globally unique EUI-64 device address and/or locally assigned 16-bit short address.
- Support for very low power device operation.
- Reliable data transfer using acknowledgements and retransmissions.
- Network discovery using beacon frames.
- Security service that employs symmetric key cryptography to ensure the confidentiality and integrity of the frame contents together with replay protection.
- CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) based channel access scheme allows multiple nodes to operate on same channel.
- Optional super frame structure with active and inactive periods allow synchronized networks for very low power operation.
- Support for frequency hopping.

The IEEE 802.15.4 [3] standard allows the WPAN to operate in one of the following operating modes:

- Legacy mode with or without periodic beacons specified in [3].

- Low latency deterministic network (LLDN) mode specified in [4].
- Time slotted channel hopping (TSCH) mode specified in [4].
- Deterministic and synchronous multi-channel extension (DSME) mode specified in [4].

These modes are mutually exclusive and all nodes in a WPAN shall be in the same operating mode. A node operating in Mode 1 according to the present document will operate in the legacy mode with or without periodic beacons.

6.1 General Description

The general description and architecture shall be as described in [3], clause 4 as amended by [4], clause 4 except:

- The Physical Layer referred to in [3], clause 4.4.1 and elsewhere in [3] shall be replaced by the Physical Layer described in [1].
- The description of Guaranteed Time Slots which shall be a feature not supported by the present document.
- Amendments in [4] to clauses 4.1 and 4.3 are not included in the present document.
- Amendments in [4] to clauses 4.5.1, 4.5.2 are not supported in the present document.
- Amendments in [4] to clauses 4.5.3 referring to LLDN are not supported in the present document.
- Amendments in [4] to clauses 4.5.4 referring to LLDN and referring to TSCH are not supported in the present document.

6.2 MAC Protocol

The MAC protocol shall be as defined in [3], clause 5.

6.2.1 MAC Functional Description

The MAC Functional Description shall be as defined in [3], clause 5.1 except for clause 5.1.7. In addition, functionality defined in [4], clause 5.1.1a for frequency hopping operation and in [4], clause 5.1.11 for low energy operation is supported in the present document.

6.2.1.1 Channel Access

Channel access shall be as defined in [3], clause 5.1.1 (except for references to GTS in [3], clause 5.1.1.1.2 which is a feature not supported in the present document) with the CSMA-CA algorithm as defined in [4], clause 5.1.1.4 and with LE enhancements defined in [4], clause 5.1.1.7.

6.2.1.2 Starting and Maintaining PANs

Starting and maintaining PANs shall be as defined in [3], clause 5.1.2 with scanning through channels as defined in [4], clause 5.1.2.1.

6.2.1.3 Association and Disassociation

Association and disassociation shall be as defined in [3], clause 5.1.3 with the addition of Fast Association as defined in [4], clause 5.1.3.3.

6.2.1.4 Transmission, Reception and Acknowledgement

Frame transmission, reception and acknowledgement shall be as defined in [3], clause 5.1.6 as amended by the following clauses in [4]:

- Clause 5.1.6.2

- Clause 5.1.6.4.2 except LLDN and TSCH which are features not supported in the present document
- Clause 5.1.6.4.3
- Clause 5.1.6.6

6.2.2 MAC Frame Formats

MAC frame formats shall be as defined in [3], clause 5.2 and as amended by [4], clause 5.2.1 and the following clauses of [5], clause 5.2.1.

The Frame Control field shall be as defined in [3], clause 5.2.1.1 and as amended by [4], clause 5.2.1.1 except:

- The Frame Type field value 0b100 (LLDN) defined in [4], clause 5.2.1.1.1 Table 2, shall be Reserved in the present document.
- The Frame Pending field amendment defined in [4], clause 5.2.1.1.3 applies for the Low Energy CSL mode but the TSCH mode is not supported in the present document.

The Destination Address field shall be as defined in [3], clause 5.2.1.4 and as amended by [4], clause 5.2.1.4.

The Auxiliary Security Header field shall be as defined in [3], clause 5.2.1.7 and as amended by [4], clause 5.2.1.7.

6.2.2.1 Beacon Frame Format

The format of a Beacon frame shall be as defined in [3], clause 5.2.2.1 and as amended by [5], clause 5.2.2.1 and [4], clause 5.2.2.1 except that:

- Definitions relating to DSME are not supported.
- Definitions relating to TSCH are not supported.

6.2.2.2 Data Frame Format

The format of the Data frame shall be as defined in [3], clause 5.2.2.2 and as amended by [5], clause 5.2.2.2 and [4], clause 5.2.2.2.

6.2.2.3 Acknowledgement Frame Format

The format of the Acknowledgement frame shall be as defined in [3], clause 5.2.2.3 and as amended by [5], clause 5.2.2.3 and [4], clause 5.2.2.3.

6.2.2.4 MAC Command Frame Format

The format of the MAC Command frame shall be as defined in [3], clause 5.2.2.4 and as amended by [5], clause 5.2.2.4 and [4], clause 5.2.2.4.

6.2.2.5 Multipurpose Frame Format

The format of the Multipurpose frame shall be as defined in [4], clause 5.2.2.6.

6.2.2.6 Multipurpose Blink Frame Format

The format of the Multipurpose Blink frame shall be as defined in [4], clause 5.2.2.7.

6.2.2.7 LE Wake-up Frame Format

The format of the LE Wake-up frame shall be as defined in [4], clause 5.2.2.8.

6.2.2.8 Frame Compatibility

Frame compatibility shall be as defined in [3], clause 5.2.3 and as amended by [4], clause 5.2.3.

6.2.3 Information Elements

Information Elements (IEs) shall be formatted as defined in [4], clause 5.2.4.

Header IEs shall be as defined in [4], clause 5.2.4.2 except that the following IE IDs shall be Reserved in the present document:

- 0x1C (DSME PAN Descriptor);
- 0x1E (ACK/NACK Time Correction);
- 0x1F (Group ACK); and
- 0x20 (LowLatencyNetworkInfo).

Payload IEs shall be as defined in [4], clause 5.2.4.3.

6.2.3.1 EMSDU IE

The EMSDU IE shall be as defined in [4], clause 5.2.4.4.

6.2.3.2 MLM IE

The MLM IE shall be as defined in [4], clause 5.2.4.5 except that the following short sub-IE IDs shall be Reserved in the present document:

- 0x1A (TSCH Synchronization)
- 0x1B (TSCH Slotframe and Link)
- 0x1C (TSCH Timeslot)

6.2.3.3 LE CSL IE

The LE CSL IE shall be as defined in [4], clause 5.2.4.7.

6.2.3.4 LE RIT IE

The LE RIT IE shall be as defined in [4], clause 5.2.4.8.

6.2.3.5 Rendezvous Time IE

The Rendezvous Time IE shall be as defined in [4], clause 5.2.4.10.

6.2.3.6 Channel Hopping IE

The Channel Hopping IE shall be as defined in [4], clause 5.2.4.16.

6.2.3.7 Hopping Timing IE

The Hopping Timing IE shall be as defined in [4], clause 5.2.4.17.

6.2.3.8 EB Filter IE

The EB Filter IE shall be as defined in [4], clause 5.2.4.18.

6.2.3.9 MAC Metrics IE

The MAC Metrics IE shall be as defined in [4], clause 5.2.4.19.

6.2.3.10 AllMAC Metrics IE

The AllMAC Metrics IE shall be as defined in [4], clause 5.2.4.20.

6.2.3.11 SUN Device Capabilities IE

The SUN Device Capabilities IE shall be as defined in [5], clause 5.2.4.20b with the following additions:

- The mode switch feature is not supported.
- The Supported Frequency Bands field shall be as defined in [5], clause 5.2.4.20b with the following additions:
  - Frequency band identifier 14 in [5], Table 68f corresponds to 870 MHz - 876 MHz.
  - Frequency band identifier 15 in [5], Table 68f corresponds to 915 MHz - 921 MHz.
- PHY Types shall be as defined in [5], Table 4k:
  - PHY Type 0 is not supported in the present document.
  - PHY Types 3-6 are not supported in the present document.
  - PHY Type 9 corresponds to PHY Type compliant with the O-QPSK PHY as defined in [1], clause 6.
  - PHY Type values 0, 3-6 and 10-12 shall be Reserved in the present document.
- PHY Type 1, Filtered FSK-B, modes shall be as defined in [5], Table 4m with the following amendments:
  - PHY Mode ID 0 corresponds to [1], Table 1 GFSK Option 1.
  - PHY Mode ID 2 corresponds to [1], Table 1 GFSK Option 4.
  - PHY Mode ID 3 corresponds to [1], Table 1 GFSK Option 2.
  - PHY Mode ID 4 corresponds to [1], Table 1 GFSK Option 5.
  - PHY Mode ID 7 shall be defined as:
    - 100 kb/s; 2FSK; mod index = 0.5; channel spacing = 200 kHz.
  - PHY Mode IDs 1, 5, 6, 8-10 shall be Reserved in the present document.
- PHY Type 2, O-QPSK-A, modes shall be as defined in [5], Table 4n with the following amendments:
  - PHY Mode IDs 1-3 are not supported in the present document.
  - PHY Mode IDs 1-10 are Reserved in the present document.
- PHY Type 9 modes shall be as defined in Table 5.

Table 5: Additional O-QPSK PHY Modes

PHY Mode ID	O-QPSK PHY Mode	Comment
0	PHY Option 1 ([1], Table 9) with PPDU Type 1 ([1], Figure 1)	Compliant to O-QPSK-A with PHY Mode ID 0
1	PHY Option 1 (1 Table 9) with PPDU Type 2 ([1], Figure 2)	
2	PHY Option 2 (1 Table 9) with PPDU Type 1 ([1], Figure 1)	
3	PHY Option 2 ([1], Table 9) with PPDU Type 2 ([1], Figure 2)	

6.2.3.12 Unmanaged ID Space IEs

The unmanaged IE ID range shall be as defined in [4], clause 5.2.4.21.

6.2.3.13 IE List Termination IE

The IE List Termination IEs shall be as defined in [4], clause 5.2.4.22.

6.2.4 MAC Commands

MAC Commands shall be as defined in [3], clause 5.3, except for the GTS Request command which is not supported in the present document, and as amended as follows by [4]:

- Clause 5.3.1 with the addition of the Association Request command identifier value 0x20 LE-RIT data request. Command identifier values 0x0D to 0x1F shall be reserved in the present document.
- Clause 5.3.2 except that in clause 5.3.2.3 the Association Status value 0x03 shall be Reserved in the present document.
- Clause 5.3.7.
- The addition of clauses 5.12 and 5.13.

6.3 MAC Services

MAC Services shall be as defined in [3], clause 6.2 as amended by [4]:

- Clause 6.2.2.1
- Clause 6.2.2.2
- Clause 6.2.2.3
- Clause 6.2.2.4
- Clause 6.2.2.5

except for the LowLatencyNetworkInfo parameters and references to Low Latency Networks which are not supported by the present document.

6.3.1 Communication Notification Primitives

Communication notification primitives shall be as defined in [3], clause 6.2.4 as amended by [4], clause 6.4.2 except for PanDescriptor Elements in [4], clause 6.4.2.1 relating to DSME which is not supported in the present document.

6.3.2 Primitives for Channel Scanning

Primitives for channel scanning shall be as defined in [3], clause 6.2.10 as amended by [4], clause 6.2.10.

For the two frequency bands defined in [1], clause 4.3, Table 3, clause 6.2.3.11 of the present document extends the definitions in [5], Table 68f.

The Channel Page structure shall be as defined in [5], Figure 64a with the following amendments:

- For PHY Type 9 in [5], Figure 64a an additional Modulation scheme shall be defined:
  - O-QPSK compliant with [1], clause 6.
- For Frequency band identifiers 14 and 15 the Channel Page supports 29 valid Channel Numbers indicating centre frequencies as defined in [1], clause 4.3.

6.3.3 Primitives for Updating the Superframe Configuration

Primitives for updating the superframe configuration shall be as defined in [3], clause 6.2.12 as amended by [4], clause 6.4.12 except for references to DSME which is not supported by the present document.

6.3.4 Primitives for Beacon Generation

Primitives for Beacon generation shall be as defined in [4], clause 6.2.18.

6.3.5 MAC Data Service

The MAC data service shall be as defined in [3], clause 6.3 as amended by [4], clause 6.3, except for references to GTS operations which are not supported by the present document.

6.3.6 MAC Constants and PIB Attributes

MAC Constants and PIB Attributes shall be as defined in [3], clause 6.4, except for:

- aGTSDescPersistenceTime
- macGTSPermit

which are not supported in the present document, as amended by [4], clause 6.4.2 together with the attributes:

- macLEcapable
- macHoppingCapable
- macAMCACapable
- acMetricsCapable
- macLEenabled
- macHoppingEnabled
- macAMCAenabled
- macMetricsEnabled

as defined in [4], clause 6.4.3.2 and attributes defined in [4], clauses 6.4.3.4, 6.4.3.7, 6.4.3.8, 6.4.3.9, 6.4.3.10 and 6.4.3.11 and [5], clause 6.4 with the attributes:

- aUnitBackoffPeriod defined as aTurnaroundTime + aCCATime;
- macFCSType supporting only the 4-octet FCS value.

6.4 Security

Security facilities shall be as defined in [3], clause 7 as amended by [4], clause 7.

6.5 Protocol Implementation Conformance Statement (PICS)

The PICS functionality defined in [3], Annex D as amended by [4], Annex D shall be included in the present document with the following qualifications:

- Major capabilities of the PHY defined in clause D7.2 are not included and are replaced by PICS declarations relevant to [1].
- MLF5 and subordinates (5.1 and 5.2) which concern GTS operation which is not supported by the prsent document.
- MLF15 and subordinates (15.1 through 15.8) which concern TSCH operation which is not supported by the present document.
- MLF16 and subordinates (16.1 through 16.5) which concern LLDN operation which is not supported by the present document.
- MLF17 and subordinates (17.1 through 17.3) which concern DSME operation which is not supported by the present document.
- MF4.9 which concerns GTS operation which is not supported by the present document.

7 Devices Operating in Mode 2

7.1 Architecture

This clause defines the behaviour of a *node* operating in Mode 2 at the MAC sub-layer of the OSI communications model. Nodes are members of a de-centralised network with all control functions being implemented equally by each node. Nodes do not have any pre-assigned or negotiated roles (see [2], clause 4), all nodes being equivalent. Higher layer functionality imposed on MAC sub-layer operation may provide star, peer-to-peer or other network configurations.

The present document only deals with the exchange of f*rames* between *neighbour nodes*. All exchanges are single hop.

The MAC sub-layer assumes that the services provided by its supporting PHY layer include the facility to transfer complete frames without modification or interpretation by the PHY layer. Such transfers take place on the PHY medium over a single channel corresponding to a PHY centre frequency. The PHY may also be required to provide an indication of whether the channel is free or occupied at a given instant. The MAC in turn provides its client layer with the services of data transfer to single or multiple neighbours with indication of success. Data transfers to a single destination are via the Unicast Data Service or to multiple neighbours via the Beacon, Multicast or Broadcast Data Services. The Unicast Data Service provides explicit acknowledgment (see [2], clause 7.4.4) of packets carrying MAC Client data which may be split over multiple fragments with re-transmission of unacknowledged fragments.

Node management may change the PHY operating channel but not within the transmission of a frame. The node may operate on a single channel, or may use a set of channels to distribute its frames over the operating frequency band.

Advantages may be gained by distributing transmissions over multiple channels when sharing spectrum with other networks or services and when operating in time varying channels subject to impairments such as frequency selective fading. In such cases the uniform distribution of devices over available channels may also lead to further benefits. Consequently, the present document defines means of communication when nodes operate either on a single channel or are pseudo-randomly distributed over available channels.

Nodes are identified and addressed using IEEE EUI-64™ identifiers (see [i.2] and [i.3]). When the communications context permits, addresses may be omitted to improve communications efficiency.

The channels in a frequency band are maintained in a Channel Table, built in a standardized way (see [2], Annex B). The operating channel is defined as a function of time by a Channel Function. A node tracks its neighbour's Channel Function and timing in order to be able to schedule transmissions on the correct channel at the scheduled time.

A Channel Function always returns the same channel number for operation on a single channel, or a channel dependent on a pseudo-random traversal of the Channel Table with specific intervals spent at each step. The Channel Function may be derived from the MAC Address or declared in a Node Announcement during initial operation. The Channel Function, traversal and dwell interval are properties of the node.

Data is accumulated from one or more client requests, possibly with additional protocol or management data, into an aggregated data set. The data set is divided into one or more fragments which are the units of information exchanged between a pair of nodes via the Unicast Data Service.

The Unicast Data Service commences with transmission of a short Initial Frame containing Flow Control information. The initial frame is sent on the destination node's Channel Function i.e. on the channel the destination node should be occupying when the frame is transmitted. If the destination node receives this Initial Frame and wishes to continue with the exchange it creates the Unicast Data Service link by replying with a frame indicating the Flow Control it will allow. The exchanges may allow bi-directional data flow with each transmitted frame acknowledging the previously received frame. All frames carrying Fragment IEs (see [2], clause 5.4.2.3) shall be acknowledged and re-transmission may occur if a frame carrying a Fragment IE is not acknowledged. If the transfer of a fragment sequence is interrupted for any reason, it may continue at a later time by transmitting a new Initial Frame to create a new Unicast Data Service link.

If a frame carrying a fragment is not acknowledged, it may be re-transmitted up to a pre-determined maximum number of times. Re-transmissions take place before continuing the data set transfer. If the re-transmission limit is exceeded the data set transfer is aborted.

All frame transmissions have an associated transmission reference time which is the local node time of transmission of the first bit of the PHY header structure. Reference to this local time may be carried in synchronization IEs to allow correction of clock drift between nodes.

As well as direct, or unicast, data exchange between neighbours, a node may transmit to group addresses to provide beacon, broadcast or multicast data services. A beacon is a special case of a broadcast frame sent periodically on a defined Channel Function. Because the interval between beacon frames is defined, beacon frames are self-synchronizing.

If used, broadcast and multicast data services apply a simple CSMA algorithm (see [2], clause 7.4.3) to reduce collisions.

During initial operation, a node declares certain information in Node Announcement IEs about its operation such that neighbour nodes receiving a Node Announcement IE can compute the channel functions for the device and its beacon transmissions.

If a node saves power by using wake/sleep cycles, the information in Power Saving IEs may be declared such that neighbour nodes can compute active periods in the power saving node's channel function.

If operating conditions require, a node may need to change its operating frequency band. Such changes are facilitated by standardized representation of frequency bands as Operating Classes and the provision of IE structures to indicate relocation to a new Operating Class at a future scheduled time.

7.2 Data Transfer Service Provided

The Data Transfer Service provided to the MAC Client shall be as described in [2], clause 4.

The Management services defined include:

- Neighbourhood exploration and announcement of node operation.
- Time synchronization between neighbours.

7.3 Security Services

A frame transmitted via the Unicast data service may be secured by including a single Secure Envelope IE as defined in clause 7.7.1. The format of the Secure Envelope IE shall be determined by the value of a Security Suite Family field (see clause 7.9).

Frames transmitted via the Beacon, Multicast or Broadcast data services may not be secured.

Information to be protected within a secured frame may be enclosed in an Encryption Envelope IE whose Content field shall be encrypted. There may be no more than one Encryption Envelope IE in any Secure Envelope IE.

7.4 Data Structures

The data structures used in the representation and exchange of information shall be as defined in [2], clauses 5 and 7 of the present document.

7.5 Representation Order

Field order within data structures and bit order within fields shall be as defined in [2], clause 5.1.

7.6 Addresses

All individual MAC addresses shall be as defined in [2], clause 4.3.1.

The Broadcast Address shall be as defined in [2], clause 4.3.2.

Multicast addresses shall be as defined in [2], clause 4.3.3.

Address fields shall be organised and transmitted as defined in [i.3] and [i.4].

7.7 Frame Format

The general format of a frame shall be as defined in [2], clauses 5.2 and 5.3.

The supported Version field value shall be 0b00.

All data shall be encapsulated in Information Elements (IEs) as defined in [2], clauses 4.7 and 5.4 and the present document, clause 7.8.

7.7.1 Secured Frame Format

The present document adds the definition of a Secured Frame as shown in Figure 2.

Octets:2	0/8	0/8	Variable	4
Frame Control	Destination Address	Source Address	Secure Envelope IE	Frame Check Sequence

Figure 2: General Secured Frame Format

A Secured Frame carries a single Secure Envelope IE which encapsulates all other IEs carried in the frame.

7.7.1.1 Frame Control

The Secured Frame Frame Control field shall be as defined in [2], clause 5.3.1.

The supported Version field value shall be 0b00.

7.7.1.2 Destination Address

The Destination Address field shall be as defined in [2], clause 5.3.2.

7.7.1.3 Source Address

The Source Address field shall be as defined in [2], clause 5.3.3.

7.7.1.4 Secure Envelope IE

The Secure Envelope IE structure shall be as defined in clause 7.8.2.

7.7.1.5 Frame Check Sequence

The Secured Frame Frame Check Sequence (FCS) shall be as defined in [2], clause 5.3.4.

7.8 Information Elements

IE structures and information content as defined in [2], clause 5.4 shall be included in the present document with the following additional IEs and definitions.

The IE summary shall be as defined in [2], clause 5.4 with the changes in Table 6.

Table 6: Information Element Summary

Type	ID	Precedence (0x0-0xF)	Description	Collective
Short	0x48	1	Session Key	No
Short	0x49-0x7F		Reserved	
Long	0x2	0	Secure Envelope	No
Long	0x3-0xB		Reserved	

Table 7 defines the support required of each defined IE:

Table 7: Information Element Support

Information Element	Generation Support	Reception Support
Fractional Sequence Interval	Mandatory	Mandatory
Fractional Dwell Interval	Optional	Optional
Node Announcement	Mandatory	Mandatory
Flow Control	Mandatory	Mandatory
Power Saving	Optional	Optional
Rendezvous	Optional	Optional
Operating Class Switching	Optional	Optional
Probe	Optional	Mandatory
Negotiated Session	Optional	Optional
Short Vendor Specific	Optional	Optional
EMSDU	Mandatory	Mandatory
MLM	Optional	Optional
Fragment	Mandatory	Mandatory
Long Vendor Specific	Optional	Optional
Secure Envelope	Mandatory	Mandatory
Long Vendor Specific	Optional	Optional

The conditions for the generation and the processing on reception of IEs shall be as defined in [2], clauses 7.3 and 7.12.8 of the present document.

7.8.1 Node Announcement (NA) IE

The NA IE shall be as defined in [2], clause 5.4.1.3. The C(t) and B(t) fields have the form shown in Figure 3.

Octets:2	2
FirstElement	Stepsize

Figure 3: C(t) and B(t) Field Format

FirstElement shall be encoded as a 16-bit unsigned integer.

Stepsize shall be encoded as a16-bit unsigned integer.

7.8.2 Secure Envelope (SE) IE

The Secure Envelope IE shall be a Long IE (see [2], clause 5.4) formatted as shown in Figure 4.

Bits:1	4	11	Octets:1	Variable
1	ID = 0x2	Length	Security Suite Family	Security Suite Family Dependent

Figure 4: Secure Envelope IE Format

The ID field shall be set to 0x2 for a Secure Envelope IE.

The Length field shall be set to the sum of the lengths of the Security Suite Family and the Security Suite Family Dependent fields.

The Security Suite Family (SSF) field shall be set according to Table 8.

Table 8: Security Suite Field Values

SSF Value	SE IE Format
0	Auxiliary Security Header
1	Negotiated Session
2..255	Reserved

The Security Suite Family Dependent field shall be set depending on the value of the SSF field (see clause 7.9).

7.9 Security Suite Families

In this clause the term 'of Big Endian form' shall be used when a value is interpreted as a bit string representation of an unsigned integer where the most significant bit occurs on the left and the least significant bit occurs on the right of the representation.

7.9.1 Auxiliary Security Header (ASH)

The ASH security Suite provides frame authentication and data confidentiality as defined in in [3], clause 7.4. If the SSF field is set to a value identifying ASH, the SE IE shall be formatted as shown in Figure 5.

Bits:1	4	11	Octes:1	Variable	Variable	Variable	Variable
1	ID = 0x2	Length	SSF = 0x00	Security Descriptor	Unencrypted IE List	Fragment IE	Integrity Check

Figure 5: SE IE Format for ASH

The ID and Length fields shall be set as defined for an SE IE (see clause 7.8.2).

The SSF field shall be set to 0x00 to identify ASH format.

The Unencrypted IE List field shall be set to zero or more IEs.

The Fragment IE field shall be set to at most one Fragment IE.

The Integrity Check field shall be set depending on the value of the Security Descriptor field.

The Security Descriptor field shall be formatted as the Auxiliary Security Header as defined in [3], clause 7.4 and with reference to that clause:

- Security Levels 0 and 4 are not supported.
- The MHR shall be interpreted as the concatenation of the Frame Control, Destination Address and Source Address fields of the secured frame.
- The Open Payload field shall be interpreted as the octet sequence formed by the Unencrypted IE List plus, if a Fragment IE is present, the 2-octet descriptor of the Fragment IE + 2-octet Fragment control fields (see [2], clause 5.4.2.3).
- If a Fragment IE is present, the Private Payload field shall be interpreted as the octet sequence formed by the Fragment Data field of the Fragment IE otherwise the Private Payload field shall be the empty octet string.

7.9.1.1 Transmission

On transmission, if the Security Level provides confidentiality and a Fragment IE is present, the octet sequence of the Fragment Data field of the Fragment IE and Integrity Check field shall be replaced by the c data output as defined in [3], clause 7.3.4.3. If the Security Level does not provide confidentiality or if no Fragment IE is present, the Integrity Check field shall be set to the c data output as defined in [3], clause 7.3.4.3.

7.9.1.2 Reception

On reception, providing the Integrity Check field value is valid, if the Security Level provides confidentiality the Fragment Data field of the Fragment IE shall be replaced by the m data output as defined in [3], clause 7.3.5.3.

7.9.2 Cipher Suite Tuple

A Cipher Suite Tuple (CST) describes a specific set of algorithms and parameter properties to be used in a secure session. A CST is an ordered structure of 6 elements {Symmetric Encryption Algorithm, Symmetric Key Size, Encryption Mode, Integrity Mechanism, Integrity Check Size, Key Derivation Function} where each element is a one octet value as defined in Table 9. When transmitted, the Symmetric Encryption Algorithm octet occurs first.

Table 9: Cipher Suite Tuple Elements

Tuple Element	Defined Values	Notes
Symmetric Encryption Algorithm	0x00 - Reserved 0x01- AES 0x02-0xFF - Reserved	See note 1
Symmetric Key Size (bits)	0x00 - Specified by Algorithm 0x01 - 128-bit 0x02 - 192-bit 0x03 - 256-bit 0x04-0xFF - Reserved	
Encryption Mode	0x00 - None (Authentication Only) 0x01 - CCM 0x02 - GCM 0x03 - CTR (see [i.4]) 0x04-0xFF - Reserved	CTR mode may only be used with HMAC SHA-256
Integrity Mechanism	0x00 - Specified by Encryption Mode 0x01 - HMAC SHA-256 0x02 - CCM Authentication Only 0x03 - GCM Authentication Only 0x02-0xFF - Reserved	The output of the HMAC SHA-256 function shall be truncated to the necessary size as specified by the Integrity Check Size
Integrity Check Size	0x08 0x0C 0x10 0x20 All other values - Reserved	Permitted Integrity Check Sizes for CCM shall be 0x08, 0x0C and 0x10 Permitted Integrity Check Sizes for GCM shall be 0x0Cand 0x10 Permitted Integrity Check Sizes for HMAC shall be 0x08, 0x0C, 0x10, 0x20
Key Derivation Function	0x00 - None 0x01 - SP800-108-CMAC (section 5.1) using same encryption algorithm and key length defined above 0x02 - -0xFF - Reserved	See note 2
NOTE 1: The Symmetric Encryption Algorithm shall be the Advanced Encryption Standard as defined in [6]. NOTE 2: The SP800-108-CMAC Key Derivation Function shall be as defined in [7].		

7.9.2.1 Authentication HMAC

All values in this clause shall be of Big Endian form:

- The SHA-256 HMAC function shall be used to produce a 32 octet HMAC value from the a-data and the authentication key (see clause 8.6) associated with the Session ID. The key size shall be as indicated by the Symmetric Key Size value of the CST associated with the Session ID. The output of that function is a 32-byte HMAC value.
- The t-data shall be set to the leftmost n octets of the HMAC value where n is the Integrity Check Size value of the CST associated with the Session ID.

7.9.2.2 Authentication CCM and Encryption None

- All values in this clause shall be of Big Endian form:
- The CCM parameter L shall be set to 2.
- The CCM parameter M shall be set to the value of the Integrity Check Size of the CST associated with the Session ID.
- The t-data of length M shall be produced by the AES cipher encryption function in CCM mode used together with:
  - the L and M parameters;
  - the key associated with the Session ID;

- the 13-octet Nonce;
- the a-data.

7.9.2.3 Authentication GCM and Encryption None

All values in this clause shall be of Big Endian form:

- The GCM parameter t shall be set to the value of the Integrity Check Size of the CST associated with the Session ID.
- The t-data of length t shall be produced by the AES cipher encryption function in GCM mode used together with:
  - the t parameter;
  - the key associated with the Session ID;
  - the 12-octet Nonce;
  - the a-data.

7.9.2.4 Authentication and Encryption CCM

All values in this clause shall be of Big Endian form:

- The CCM parameter L shall be set to 2.
- The CCM parameter M shall be set to the value of the Integrity Check Size of the CST associated with the Session ID.
- The c-data of length equal to the length of the m-data and t-data of length M shall be produced by the CCM Authenticated Encryption function used together with:
  - the L and M parameters;
  - the key associated with the Session ID;
  - the 13-octet Nonce;
  - the a-data and m-data.

7.9.2.5 Authentication and Encryption GCM

All values in this clause shall be of Big Endian form:

- The GCM parameter *t* shall be set to the value of the Integrity Check Size of the CST associated with the Session ID.
- The c-data of length equal to the length of the m-data and t-data of length *t* shall be produced by the GCM Authenticated Encryption function used together with:
  - the *t* parameter;
  - the key associated with the Session ID;
  - the 12-octet Nonce;
  - the a-data and m-data.

7.9.2.6 Authentication HMAC and Encryption CTR

All values in this clause shall be of Big Endian form:

- The 16-octet Nonce shall be formed as the concatenation of:
  - the Destination MAC Address;
  - the Frame Counter associated with the Session ID;
  - a 32-bit block of zero bits.
- The CTR counter block incrementing function will increment the integer represented by the right-most 32-bits in big-endian order.
- The c-data of length equal to the length of the m-data shall be produced by the CTR Encryption function used together with:
  - the key associated with the Session ID;
  - the 16-octet Nonce;
  - the m-data.
- The SHA-256 HMAC function shall be used to produce a 32-octet HMAC value from:
  - the concatenation of the a-data with the c-data;
  - the authentication key (see 9.6) associated with the Session ID:
    - the key size shall be as indicated by the Symmetric Key Size value of the CST associated with the Session ID;
  - the output of that HMAC function shall be a 32-byte HMAC value.
- The t-data shall be set to the leftmost n octets of the HMAC value where n is the Integrity Check Size value of the CST associated with the Session ID.

7.9.3 Negotiated Session (NS)

The Negotiated Session security suite supports the negotiation of the authentication and encryption algorithm and key and integrity check size to be used in authenticating a frame and protecting data (see clause 8 of the present document). If the SSF field is set to a value identifying NS, the SE IE shall be formatted as shown in Figure 6.

Bits:1	4	11	Octes:1	2	4	Variable	Variable	Variable
1	ID = 0x2	Length	SSF = 0x01	Session ID	Sequence Number	Unencrypted IE List	Fragment IE	Integrity Check

Figure 6: SE IE Format for NS

The ID and Length fields shall be set as defined for an SE IE (see clause 7.8.2).

The SSF field shall be set to 0x01 for NS format.

The Session ID field shall be set to a value identifying a secure session between the source and destination nodes.

The Sequence Number field shall be set to the next valid transmit Frame Counter (see clause 7.12.7) value for the session identified by the value of the Session ID field.

The Unencrypted IE List field shall be set to a list of zero or more IEs which are to be authenticated but not encrypted.

The Fragment IE field shall be set to at most one Fragment IE. If a Fragment IE is present and the value of the Session ID identifies both authentication and encryption, its Fragment Data field contains data to be protected by the encryption procedures of the security suite identified by the SE IE Session ID field value. On transmission, the Fragment Data field of the Fragment IE shall be replaced with the output of the encryption procedure applied to the Fragment Data field.

The Integrity Check field shall be set to a value computed over the Frame Control, Destination Address, Source Address and SE IE excluding the Integrity Check field. The specific computation shall be according to the procedures of the security suite identified by the value of the Session ID field. If the Frame Control field Address Mode (see [2], clause 5.3.1.3) indicates that an address is not present, the value of the address shall be used as if it were present in the frame.

7.9.3.1 Transmission

The Frame Counter shall be incremented to the next permitted value (see clause 7.12.7).

7.9.3.1.1 Authentication HMAC

All values in this clause shall be of Big Endian form.

If the CST associated with the value of the Session ID field of the SE IE identifies:

- HMAC as the Integrity Mechanism.
- None as the Encryption Mode:
  - If a Fragment IE is present:
    - a-data shall be formed from:
      - The Frame Control field (see clause 7.7.1) || Destination node 64-bit MAC Address || Source node 64-bit MAC Address || Unencrypted IE List || Fragment IE.
  - If no Fragment IE is present:
    - a-data shall be formed from:
      - The Frame Control field (see clause 7.7.1) || Destination node 64-bit MAC Address || Source node 64-bit MAC Address || Unencrypted IE List.
- The Integrity Check field shall be set to the t-data generated according to clause 7.9.2.1.

7.9.3.1.2 Authentication CCM and Encryption None

All values in this clause shall be of Big Endian form.

If the CST associated with the value of the Session ID field of the SE IE identifies:

- Encryption Mode specified as None.
- Integrity Mechanism specified as CCM:
  - The Nonce shall be formed by the concatenation of:
    - the Destination MAC Address;
    - the Frame Counter associated with the Session ID;
    - the SSF.
  - If a Fragment IE is present:
    - a-data shall be formed by the concatenation of:
      - the Frame Control field (see clause 7.7.1);
      - destination node 64-bit MAC Address;
      - source node 64-bit MAC Address;
      - unencrypted IE List;

- 2-octet descriptor of the Fragment IE and 2-octet Fragment control fields (see [2], clause 5.4.2.3);
- the Fragment IE Fragment Data field (see [2], clause 5.4.2.3).

- m-data shall be set to the empty octet string.
- The Integrity Check field shall be set to the t-data generated according to 7.9.2.4.

- If no Fragment IE is present:
  - a-data shall be formed by the concatenation of:
    - the Frame Control field (see clause 7.7.1);
    - destination node 64-bit MAC Address;
    - source node 64-bit MAC Address;
    - unencrypted IE List.
  - m-data shall be set to the empty octet string.
  - The Integrity Check field shall be set to the t-data generated according to clause 7.9.2.4.

7.9.3.1.3 Authentication GCM and Encryption None

All values in this clause shall be of Big Endian form.

If the CST associated with the value of the Session ID field of the SE IE identifies:

- Encryption Mode specified as None.
- Integrity Mechanism specified as GCM:
  - The 12-octet Nonce shall be formed by the concatenation of:
    - The Destination MAC Address.
    - The Frame Counter associated with the Session ID.
  - If a Fragment IE is present:
    - a-data shall be formed by the concatenation of:
      - the Frame Control field (see clause 7.7.1);
      - destination node 64-bit MAC Address;
      - source node 64-bit MAC Address;
      - unencrypted IE List;
      - 2-octet descriptor of the Fragment IE and 2-octet Fragment control fields (see [2], clause 5.4.2.3);
      - the Fragment IE Fragment Data field (see [2], clause 5.4.2.3).
    - m-data shall be set to the empty octet string.
    - The Integrity Check field shall be set to the t-data generated according to clause 7.9.2.5.
  - If no Fragment IE is present:
    - a-data shall be formed by the concatenation of:
      - the Frame Control field (see clause 7.7.1);

- destination node 64-bit MAC Address;
- source node 64-bit MAC Address;
- unencrypted IE List.

- m-data shall be set to the empty octet string.
- The Integrity Check field shall be set to the t-data generated according to clause 7.9.2.5.

7.9.3.1.4 Authentication/Encryption Mode CCM

All values in this clause shall be of Big Endian form.

If the CST associated with the value of the Session ID field of the SE IE identifies:

- CCM as the Encryption Mode.
- Integrity Mechanism as specified by Encryption Mode or CCM:
  - The Nonce shall be constructed by the concatenation of:
    - the Destination MAC Address;
    - the Frame Counter associated with the Session ID;
    - the SSF.
  - If a Fragment IE is present:
    - a-data shall be formed by the concatenation of:
      - the Frame Control field (see clause 7.7.1);
      - destination node 64-bit MAC Address;

        source node 64-bit MAC Address;
      - unencrypted IE List;
      - 2-octet descriptor of the Fragment IE + 2-octet Fragment control fields (see [2], clause 5.4.2.3).
    - m-data shall be formed from:
      - the Fragment IE Fragment Data field (see [2], clause 5.4.2.3);
      - the Fragment IE Fragment Data field shall be set to the c-data generated according to clause 7.9.2.4;
      - the Integrity Check field shall be set to the t-data generated according to clause 7.9.2.4.
  - If no Fragment IE is present:
    - a-data shall be formed by the concatenation of:
      - the Frame Control field (see clause 7.7.1);
      - destination node 64-bit MAC Address;
      - source node 64-bit MAC Address;
      - unencrypted IE List.
    - m-data shall be set to the empty octet string.
    - The Integrity Check field shall be set to the t-data generated according to clause 7.9.2.4.

7.9.3.1.5 Authentication/Encryption Mode GCM

If the All values in this clause shall be of Big Endian form.

CST associated with the value of the Session ID field of the SE IE identifies:

- GCM as the Encryption Mode.
- Integrity Mechanism as specified by Encryption Mode or GCM:
  - The Nonce shall be constructed by the concatenation of:
    - the Destination MAC Address;
    - the Frame Counter associated with the Session ID.
  - If a Fragment IE is present:
    - a-data shall be formed by the concatenation of:
      - the Frame Control field (see clause 7.7.1);
      - destination node 64-bit MAC Address;
      - source node 64-bit MAC Address;
      - unencrypted IE List;
      - 2-octet descriptor of the Fragment IE + 2-octet Fragment control fields (see [2], clause 5.4.2.3).
    - m-data shall be formed from:
      - the Fragment IE Fragment Data field (see [2], clause 5.4.2.3).
    - The Fragment IE Fragment Data field shall be set to the c-data generated according to clause 7.9.2.5.
    - The Integrity Check field shall be set to the t-data generated according to clause 7.9.2.5.
  - If no Fragment IE is present:
    - a-data shall be formed from:
      - the Frame Control field (see clause 7.7.1);
      - destination node 64-bit MAC Address;
      - source node 64-bit MAC Address;
      - unencrypted IE List.
    - m-data shall be set to the empty octet string.
    - The Integrity Check field shall be set to the t-data generated according to clause 7.9.2.5.

7.9.3.1.6 Authentication HMAC and Encryption CTR

All values in this clause shall be of Big Endian form.

If the CST associated with the value of the Session ID field of the SE IE identifies:

- Encryption Mode specified as CTR.
- Integrity Mechanism specified as HMAC:
  - If no Fragment IE is present the Integrity Check field shall be set according to clause 7.9.3.1.1.

- If a Fragment IE is present:
  - The 16-octet Initial Counter Block shall be constructed by the concatenation of:
    - the Destination MAC Address;
    - the Frame Counter associated with the Session ID;
    - a 32-bit block of zeros.
  - a-data shall be formed by the concatenation of:
    - the Frame Control field (see clause 7.7.1);
    - destination node 64-bit MAC Address;
    - source node 64-bit MAC Address;
    - unencrypted IE List;
    - 2-octet descriptor of the Fragment IE and 2-octet Fragment control fields (see [2], clause 5.4.2.3).
  - m-data shall be formed from:
    - the Fragment IE Fragment Data field (see [2], clause 5.4.2.3).
  - The Fragment IE Fragment Data field shall be set to the c-data generated according to 7.9.2.6.
  - The SHA-256 HMAC function shall be used to produce a 32 octet HMAC value from:
    - the concatenation of the a-data with the c-data.
  - The authentication key (see clause 9.6) associated with the Session ID:
    - the key size shall be as indicated by the Symmetric Key Size value of the CST associated with the Session ID.
    - Integrity Check field shall be set to the leftmost n octets of the HMAC value where n is the Integrity Check Size value of the CST associated with the Session ID.

7.9.3.2 Reception

When an SE IE is received with:

- The value of the SSF field identifying NS.
- The value of the Session ID field not identifying a secure relationship between the local node and the source node of the frame carrying the SE IE.
- An SK IE formatted for a Session Created message.

The MAC Entity:

- Derives a Session ID according to clause 8.4 using:
  - the received SK IE Session Created message;
  - a New Session parameter set identified by:
    - the value of the I_{nonce} field of the received SK IE.
- If the derived Session ID doe not match the value of the Session ID field of the received SE IE the MAC Entity:
  - discards the SE IE.

- If the derived Session ID matches the value of the Session ID field of the received SE IE the MAC Entity:
  - processes the received SE IE according to the following clauses.

7.9.3.2.1 Authentication HMAC

All values in this clause shall be of Big Endian form.

If the CST associated with the value of the Session ID field of the SE IE identifies:

- HMAC as the Integrity Mechanism.
- None as the Encryption Mode:
  - The a-data shall be formed according to clause 7.9.3.1.1.
  - If the Integrity Check field:
    - Matches the t-data generated according to clause 7.9.2.1 the frame carrying the SE IE shall be valid.
    - Does not match the t-data generated according to clause 7.9.2.1 the frame carrying the SE IE shall be invalid.

7.9.3.2.2 Authentication CCM and Encryption None

All values in this clause shall be of Big Endian form.

If the CST associated with the value of the Session ID field of the SE IE identifies:

- Encryption Mode specified as None.
- Integrity Mechanism specified as CCM:
  - The Nonce & a-data shall be formed according to clause 7.9.3.1.4.
  - c-data shall be set to the empty octet string.
  - If the Integrity Check field:
    - Matches the t-data generated according to clause 7.9.2.4 the frame carrying the SE IE shall be valid.
    - Does not match the t-data generated according to clause 7.9.2.4 the frame carrying the SE IE shall be invalid.

7.9.3.2.3 Authentication GCM and Encryption None

All values in this clause shall be of Big Endian form.

If the CST associated with the value of the Session ID field of the SE IE identifies:

- Encryption Mode specified as None.
- Integrity Mechanism specified as GCM:
  - The Nonce and a-data shall be formed according to clause 7.9.3.1.5.
  - c-data shall be set to the empty octet string.
  - If the Integrity Check field:
    - Matches the t-data generated according to clause 7.9.2.5:
      - the frame carrying the SE IE shall be valid.

- Does not match the t-data generated according to clause 7.9.2.5 the frame carrying the SE IE shall be invalid.

7.9.3.2.4 Authentication and Encryption CCM

All values in this clause shall be of Big Endian form.

If the CST associated with the value of the Session ID field of the SE IE identifies:

- CCM as the Encryption Mode.
- Integrity Mechanism as specified by Encryption Mode or CCM:
  - The Nonce shall be constructed by the concatenation of:
    - The value of the 8-octet local node MAC Address.
    - The 4-octet Sequence Number field of the SE IE.
    - The 1-octet SSF of the SE IE.
  - If a Fragment IE is present:
    - a-data shall be formed by the concatenation of:
      - The Frame Control field (see clause 7.7.1).
      - The value of the 8-octet local node MAC Address.
      - The value of the 8-octet source node MAC Address.
      - The Unencrypted IE List.
      - 2-octet descriptor of the Fragment IE + 2-octet Fragment control fields (see [2], clause 5.4.2.3).
    - c-data shall be formed by the concatenation of:
      - The Fragment IE Fragment Data field (see [2], clause 5.4.2.3).
    - t-data shall be set to the value of the Integrity Check field of the SE IE.
  - If no Fragment IE is present:
    - a-data shall be formed by the concatenation of:
      - The Frame Control field (see clause 7.7.1).
      - The value of the 8-octet local node MAC Address.
      - The value of the 8-octet source node MAC Address.
      - Unencrypted IE List.
    - c-data shall be set to the empty octet string.
    - t-data shall be set to the value of the Integrity Check field of the SE IE.
  - The CCM parameter L shall be set to 2.
  - The CCM parameter M shall be set to the value of the Integrity Check Size of the CST associated with the Session ID.
  - The m-data of length equal to the length of the c-data and t-data of length M shall be produced by the CCM Authenticated Decryption function used together with:
    - The L and M parameters.
    - The key associated with the Session ID.

- The 13-octet Nonce.
- The a-data and c-data.

- If the t-data:
  - Matches Integrity Check field of the SE IE:
    - The frame carrying the SE IE shall be valid.
    - If a Fragment IE is present in the SE IE:
      - The Fragment Data field of the Fragment IE shall be replaced with m-data.
  - Does not match the Integrity Check field of the SE IE the frame carrying the SE IE shall be invalid.

7.9.3.2.5 Authentication and Encryption GCM

All values in this clause shall be of Big Endian form.

If the CST associated with the value of the Session ID field of the SE IE identifies:

- GCM as the Encryption Mode.
- Integrity Mechanism as specified by Encryption Mode or GCM:
  - The 12-octet Nonce shall be constructed by the concatenation of:
    - The value of the 8-octet local node MAC Address.
    - The 4-octet Sequence Number field of the SE IE.
  - If a Fragment IE is present:
    - a-data shall be formed by the concatenation of:
      - The Frame Control field (see clause 7.7.1).
      - The value of the 8-octet local node MAC Address.
      - The value of the 8-octet source node MAC Address.
      - The Unencrypted IE List.
      - 2-octet descriptor of the Fragment IE + 2-octet Fragment control fields (see [2], clause 5.4.2.3).
    - c-data shall be formed by the concatenation of:
      - The Fragment IE Fragment Data field (see [2], clause 5.4.2.3).
    - t-data shall be set to the value of the Integrity Check field of the SE IE
  - If no Fragment IE is present:
    - a-data shall be formed by the concatenation of:
      - The Frame Control field (see clause 7.7.1).
      - The value of the 8-octet local node MAC Address.
      - The value of the 8-octet source node MAC Address.
      - Unencrypted IE List.
    - c-data shall be set to the empty octet string.
    - t-data shall be set to the value of the Integrity Check field of the SE IE.

- The GCM parameter *t* shall be set to the value of the Integrity Check Size of the CST associated with the Session ID.
- The m-data of length equal to the length of the c-data and t-data of length *t* shall be produced by the GCM Authenticated Decryption function used together with:
  - The *t* parameter.
  - The key associated with the Session ID.
  - The 23-octet Nonce.
  - The a-data and c-data.
- If the t-data:
  - Matches Integrity Check field of the SE IE:
    - The frame carrying the SE IE shall be valid.
    - If a Fragment IE is present in the SE IE:
      - The Fragment Data field of the Fragment IE shall be replaced with m-data.
  - Does not match the Integrity Check field of the SE IE the frame carrying the SE IE shall be invalid.

7.9.3.2.6 Authentication HMAC and Encryption CTR

All values in this clause shall be of Big Endian form.

If the CST associated with the value of the Session ID field of the SE IE identifies:

- The Encryption Mode as CTR.
- The Integrity Mechanism as HMAC.
- If the Integrity Check field:
  - Matches the t-data generated according to clause 7.9.3.1.1:
    - the frame carrying the SE IE shall be valid.
    - If a Fragment IE is present:
      - The 16-octet Nonce shall be formed as the concatenation of:
        - The local node MAC Address.
        - The Sequence Number field of the SE IE.
        - A 32-bit block of zero bits.
      - The CTR counter block incrementing function will increment the integer represented by the right-most 32-bits in big-endian order.
      - The m-data of length equal to the length of the c-data shall be produced by the CTR Decryption function used together with:
        - The key associated with the Session ID.
        - The 16-octet Nonce.
        - The c-data.
      - The Fragment IE Fragment Data field shall be set to the m-data.
    - Does not match the t-data generated according to clause 7.9.3.1.1 the frame carrying the SE IE shall be invalid.

7.9.4 Session Key (SK) IE

The SK IE shall be used to establish, maintain or destroy a secure session relationship between a pair of nodes. The SK IE shall be formatted as shown in Figure 7.

Bits:1	8	7	Octes:1	Variable
0	ID = 0x48	Length	NS Message	NS Message Dependent

Figure 7: SK IE Format

The ID field shall be set to 0x48 for the SK IE.

The Length field shall be set to 1 + the number of octets in the NS Message Dependent field.

The NS Message field shall be set to one of the values for NS operations defined in the following clauses.

The NS Message Dependent fields shall be as defined in the corresponding NS Message field clause below.

7.9.4.1 NS New Session Message

A New Session message shall be indicated by an SK IE formatted as shown in Figure 8.

Bits:1	8	7	Octes:1	8	12	8	n*6
0	ID = 0x48	Length	NS Message = 0x01	Initiator Nonce	Key ID	Initiator Random Value	CST List

Figure 8: New Session Message SK IE Format

The NS Message field shall be set to 0x01 for a New Session message.

The Initiator Nonce field shall be set to random value generated by the initiating node.

The Key ID field shall be set to a value shared between the initiator and responder nodes to identify the key to be used in this secure session.

The Initiator Random Value shall be set to a further random value generated by the initiator node.

The CST List field shall be set to a list of one or more Cipher Suite Tuples identifying possible cipher suites to be used for this secure session.

7.9.4.2 NS Session Created Message

A Session Created message shall be indicated by an SK IE formatted as shown in Figure 9.

Bits:1	8	7	Octes:1	8	8	6	Variable
0	ID = 0x48	Length	NS Message = 0x02	I_{nonce}	Responder Random Value	Selected CST	Message Integrity Check

Figure 9: Session Created Message SK IE Format

The NS Message field shall be set to 0x02 for a Session Created message.

The I_{nonce} field shall be set to the value of the Initiator Nonce field of the New Session message for which the Session Created message is being sent.

The Responder Random Value shall be set to a random value generated by the responding node.

The Selected CST field shall be set to the Cipher Suite Tuple identifying the security cipher suite to be used for this secure session.

The Message Integrity Check field shall be set to a value depending on the Selected CST value with:

- The Nonce formed from the leftmost n octets of the concatenation of:
  - The 8-octet I_{nonce} in Big Endian form
  - The 8-octet Responder Random Value in Big Endian form

The value of n shall be dependent on the Integrity Mechanism indicated by the Selected CST.

The value shall be computed using the indicated CST integrity mechanism (see clauses 7.9.2.1 to 7.9.2.6) and derived keys (see clause 8.6) over:

- The Source and Destination MAC Address values.
- The SK IE as shown in Figure 9 excluding the Message Integrity Check field.

7.9.4.3 NS Session Acknowledgement Message

A Session Acknowledgement message shall be indicated by an SK IE formatted as shown in Figure 10.

Bits:1	8	7	Octes:1	8	Variable
0	ID = 0x48	Length	NS Message = 0x03	I_{nonce}	Message Integrity Check

Figure 10: Session Acknowledgement Message SK IE Format

The NS Message field shall be set to 0x03 for a Session Acknowledgement message.

The I_{nonce} field shall be set to the value of the Initiator Nonce field of the New Session message being acknowledged.

The Message Integrity Check field shall be set to a value depending on the selected CST with:

- The Nonce formed from the leftmost n octets of the concatenation of:
  - The 8-octet I_{nonce} in Big Endian form.
  - The 8-octet MAC Address of the Initiator in Big Endian form.

The value of n shall be dependent on the Integrity Mechanism indicated by the Selected CST.

The value shall be computed using the selected CST integrity mechanism (see clauses 7.9.2.1 to 7.9.2.6) and derived keys (see clause 8.6) over:

- The Source and Destination MAC Address values.
- The SK IE as shown in Figure 10 excluding the Message Integrity Check field.

7.9.4.4 NS Session Destruction Message

A Session Destruction message shall be indicated by an SK IE formatted as shown in Figure 11.

Bits:1	8	7	Octes:1	8	8	2	Variable
0	ID = 0x48	Length	NS Message = 0x04	I_{nonce}	R_{rande}	Session ID	Message Integrity Check

Figure 11: Session Destruction Message SK IE Format

The NS Message field shall be set to 0x04 for a Session Destruction message.

The I_{nonce} field shall be set to the I_{nonce} value of the New Session message used to establish the secure relationship being destroyed.

The R_{rand} field shall be set to the value of the Responder Random Value field of the Session Created message used to establish the secure relationship being destroyed.

The Session ID field shall be set to the value of the Session ID of the secure relationship which is being destroyed.

The Message Integrity Check field shall be set to a value depending on the CST associated with the Session ID with:

- The Nonce formed from the leftmost n octets of the concatenation of:
  - The value of the 8-octet I_{nonce} field in Big Endian form.
  - The value of the 8-octet R_{rand} field in Big Endian form.

The value of n shall be dependent on the Integrity Mechanism indicated by the Selected CST.

The value shall be computed using the selected CST integrity mechanism (see clauses 7.9.2.1 to 7.9.2.6) and derived keys (see clause 8.6) over:

- The Source and Destination MAC Address values.
- The SK IE as shown in Figure 11 excluding the Message Integrity Check field.

7.10 Constants and Parameter Attributes

Constants and parameters with attributes as defined in [2], clause 6.3 shall be included in the present document together with the following:

Table 10: Additional Constants & Parameters

Name	Type	Value	Description
cClockAccuracy	Integer	10ppm	Nominal Clock Accuracy for MAC timing estimation
macDefaultKeySource			As defined in [3], clause 7.5

7.11 Service Interfaces

Models for MAC Data Service and MAC Layer Management Service Interface as described in [2], clause 6 shall be included in the present document with the following extensions to support the Secure Envelope and Negotiated Session facilities.

7.11.1 M-DATA.request

The M-DATA.request primitive shall be as defined in [2], clause 6.1.1 plus the additional parameters defined in Table 11.

Table 11: Additional M-DATA.request Parameters

Parameter Name	Type	Valid Range	Description
Security Suite Family	Integer	0,1	Present if the Data request is to be secured using an SE IE with specified SSF
Security Level			Present if SSF = 0. As defined in [3], clause 6.3.1
KeyIdMode			Present if SSF = 0. As defined in [3], clause 6.3.1
KeySource			Present if SSF = 0. As defined in [3], clause 6.3.1
KeyIndex			Present if SSF = 0. As defined in [3], clause 6.3.1
Session ID	Integer	0x0000..0xFFFF	Present if SSF = 1. Session ID value to be used in the SE IE

If the Security Suite Family parameter is present the data transfer shall be protected by a Secured Frame with an SE IE formatted according to the value of the Security Suite Family parameter.

If the Security Suite Family parameter identifies ASH then:

- The Security Level parameter shall be set as defined in [3], clause 6.3.1.
- The KeyIdMode parameter shall be set as defined in [3], clause 6.3.1.
- The KeySource parameter shall be set as defined in [3], clause 6.3.1.

If the Security Suite Family parameter identifies NS then:

- The Session ID parameter shall be set to the value to be used in the Session ID field of the SE IE.
- The Sequence Number parameter shall be set to the value to be used in the Sequence Number field of the SE IE.

7.11.2 M-DATA.indication

The M-DATA.indication primitive shall be as defined in [2], clause 6.1.3 plus the additional parameters defined in Table 12.

Table 12: Additional M-DATA.indication Parameters

Parameter Name	Type	Valid Range	Description
Security Suite Family	Integer	0,1	Present if the received frame was secured with an SE IE with specified SSF
Security Level			Present if SSF = 0. As defined in [3], clause 6.3.3
KeyIdMode			Present if SSF = 0. As defined in [3], clause 6.3.3
KeySource			Present if SSF = 0. As defined in [3], clause 6.3.3
KeyIndex			Present if SSF = 0. As defined in [3], clause 6.3.3
Session ID	Integer	0x0000..0xFFFF	Present if SSF = 1. Session ID value of the received SE IE

If the received frame was a Secured Frame:

- The Security Suite Family parameter shall be set to the value of the SSF field of the received SE IE.

If the Security Suite Family parameter identifies ASH then:

- The Security Level parameter shall be set as defined in [3], clause 6.3.3.
- The KeyIdMode parameter shall be set as defined in [3], clause 6.3.3.
- The KeySource parameter shall be set as defined in [3], clause 6.3.3.

If the Security Suite Family parameter identifies NS then:

- The Session ID parameter shall be set to the value of the Session ID field of the received SE IE.

7.11.3 MAC Layer Management Negotiated Session Interface (MLM-NS)

The MLM-NS interface is expressed via the following primitives:

- MLM-NS.request.
- MLM-NS.indication.

7.11.4 MLM-NS.request

The MLM-NS.request primitive should be generated to transmit a Negotiated Session protocol message.The general format of parameters qualifying the MLM-NS.request primitive is shown in Table 13.

Table 13: MLM-NS.request General Parameter Format

Parameter Name	Type	Valid Range	Description
Request Type	Enumeration	New Session Session Created Session Acknowledgement Session Destruction	Transmit SK IE New Session message Transmit SK IE Session Created message Transmit SK IE Session ACK message Transmit SK IE Session Destruction message
Destination Address	EUI-64	Valid EUI-64	Unicast MAC Address of the destination node
Session ID	Integer	0x0000..0xFFFF	Present if the SK IE should be sent in a secured frame. Session ID value for SE IE
Request Type Dependent	-	-	Specific parameters for each Request Type

7.11.4.1 MLM-NS New Session Request

If the Request Type parameter indicates New Session the Request Type Dependent parameters shall be as shown in Table 14.

Table 14: MLM-NS.request New Session Parameters

Parameter Name	Type	Valid Range	Description
I-nonce	Integer	8-octet value	Initiator Nonce value for New Session message
I-rand	Integer	8-octet value	Initiator Random Value for New Session message
Key ID	Integer	12-octet value	Key ID value for New Session message
CST List	Octet Sequence	Set of one or more valid Cipher Suite Tuples	CST List for New Session message

A New Session SK IE (see clause 7.9.4.1) shall be created according to clause 7.9.4.1.

7.11.4.2 MLM-NS Session Created Request

If the Request Type parameter indicates Session Created the Request Type Dependent parameters shall be as shown in Table 15:

Table 15: MLM-NS.request Session Created Parameters

Parameter Name	Type	Valid Range	Description
Session ID	Integer	0x0000.. 0xFFFF	If present the Session ID value to be used in the SE IE to carry the Session Created message
I-nonce	Integer	8-octet value	Initiator Nonce value for Session Created message
R-rand	Integer	8-octet value	Responder Random Value for Session Created message
Selected CST	Octet Sequence	Valid Cipher Suite Tuple	Selected CST for Session Created message

A Session Created SK IE (see clause 7.9.4.2) shall be created according to clause 7.9.4.2.

7.11.4.3 MLM-NS Session Acknowledge Request

If the Request Type parameter indicates Session Acknowledge the Request Type Dependent parameters shall be as shown in Table 16:

Table 16: MLM-NS.request Session Acknowledge Parameters

Parameter Name	Type	Valid Range	Description
Session ID	Integer	0x0000.. 0xFFFF	If present the Session ID value to be used in the SE IE to carry the Session Acknowledge message
I-nonce	Integer	8-octet value	Initiator Nonce value for Session Acknowledge message

A Session Acknowledge SK IE (see clause 7.9.4.3) shall be created according to clause 7.9.4.3.

7.11.4.4 MLM-NS Session Destruction Request

If the Request Type parameter indicates Session Destruction the Request Type Dependent parameters shall be as shown in Table 17:

Table 17: MLM-NS.request Session Destruction Request Parameters

Parameter Name	Type	Valid Range	Description
Session ID	Integer	0x0000.. 0xFFFF	The Session ID value to be destroyed

A Session Destruction SK IE (see clause 7.9.4.4) shall be created according to clause 7.9.4.4.

7.11.5 MLM-NS.indication

The MLM-NS.indication primitive should be generated for each received Negotiated Session protocol message.The general format of parameters qualifying the MLM-NS.indication primitive is shown in Table 18.

Table 18: MLM-NS.indication General Parameter Format

Parameter Name	Type	Valid Range	Description
Request Type	Enumeration	New Session Session Created Session Acknowledgement Session Destruction	SK IE New Session message was received SK IE Session Created message was received SK IE Session ACK message was received SK IE Session Destruction message was received
Source Address	EUI-64	Valid EUI-64	Unicast MAC Address of the originating node
Session ID	Integer	0x0000..0xFFFF	Present if the SK IE was received in a secured frame. Session ID value of received SE IE
Message Type Dependent	-	-	Specific parameters for each NS Message received

7.11.5.1 MLM-NS New Session Indication

If the received NS message was a New Session message the Message Type Dependent parameters shall be as shown in Table 19.

Table 19: MLM-NS. indication New Session Parameters

Parameter Name	Type	Valid Range	Description
I-nonce	Integer	8-octet value	Initiator Nonce value of the received New Session message
I-rand	Integer	8-octet value	Initiator Random Value of the received New Session message
Key ID	Integer	12-octet value	Key ID value of the received New Session message
CST List	Octet Sequence	Set of one or more valid Cipher Suite Tuples	CST List of the received New Session message

7.11.5.2 MLM-NS Session Created Indication

If the received NS message was a Session Created message the Message Type Dependent parameters shall be as shown in Table 20:

Table 20: MLM-NS. indication Session Created Parameters

Parameter Name	Type	Valid Range	Description
Session ID	Integer	0x0000.. 0xFFFF	If present the Session ID value to be used in the SE IE to carry the Session Created message
I-nonce	Integer	8-octet value	Initiator Nonce value of the received Session Created message
R-rand	Integer	8-octet value	Responder Random Value of the received Session Created message
Selected CST	Octet Sequence	Valid Cipher Suite Tuple	Selected CST of the received Session Created message

7.11.5.3 MLM-NS Session Acknowledge Indication

If the received NS message was a Session Acknowledge message the Message Type Dependent parameters shall be as shown in Table 21:

Table 21: MLM-NS. indication Session Acknowledge Parameters

Parameter Name	Type	Valid Range	Description
Session ID	Integer	0x0000.. 0xFFFF	If present the Session ID value to be used in the SE IE to carry the Session Acknowledge message
I-nonce	Integer	8-octet value	Initiator Nonce value of the received Session Acknowledge message

7.11.5.4 MLM-NS Session Destruction Indication

If the received NS message was a Session Destruction message the Message Type Dependent parameters shall be as shown in Table 22:

Table 22: MLM-NS.indication Session Destruction Parameters

Parameter Name	Type	Valid Range	Description
Session ID	Integer	0x0000.. 0xFFFF	If the Session Destruction message was received in a secured frame, the value of the Session ID field of the received SE IE
I-nonce	Integer	8-octet value	If the Session Destruction message was received in a non-secured frame, Initiator Nonce field value of the received Session Destruction message

7.12 Functional description

7.12.1 Channel Function

The operating channel shall be determined according to a Channel Function as defined in [2], clause 4.4. If first element and step size are derived from a device MAC Address the procedure shall be as defined in [2], clause 7.1.

An implementation may operate on a single channel or on multiple channels as a Frequency Hopping device.

7.12.2 Channel Table

The Channel Table used by the Channel Function shall be constructed as defined in [2], Annex B.

7.12.3 Timing Accuracy

All time references in the present document shall be to a nominal accuracy of cClockAccuracy.

All predicted future event times shall be to be calculated with guard intervals dependent on the interval since the last synchronization was performed with the device concerned and at the nominal clock accuracy.

7.12.4 Synchronization

Relative timing information shall be exchanged between nodes as described in [2], clause 4.8 using data structures as described in [2], clauses 5.4.1.1 and 5.4.1.2.

7.12.5 CSMA

Where applied, CSMA shall be performed as described in [2], clauses 4.6.5 and 7.4.6.1.

7.12.6 Frame Processing

Frames shall be considered transmitted and received as defined in [2], clause 7.2.1.

7.12.7 Frame Counter

In addition to the per-neighbour Unicast sequence number maintained as defined in [2], clause 7.2.2 each node maintains a Frame Counter for each secure relationship maintained with any neighbour:

- The initial value of the Frame Counter is not specified.
- The maximum value of the Frame Counter shall be the largest number that can be represented by the size of the Sequence Number or Frame Counter field of SE IEs used for the secure relationship communications.
- The value of the Frame Counter shall be increased by 1 before each frame transmitted by the node to the neighbour with whom the secure relationship has been established.
- If the value of the Frame Counter after incrementing is zero:
    - The secure relationship for which the Frame Counter is being incremented shall be terminated before the frame is transmitted.

7.12.8 Information Element Processing

IEs shall be generated and interpreted as defined in [2], clause 7.3 together with the following:

7.12.8.1 EMSDU IE

EMSDU IEs shall be generated as defined in [2], clause 7.3.7 for M-Data.request primitives without SSF parameter and shall be associated with a non-secure data set as described in [2], clause 7.4.1.

EMSDU IEs generated for M-Data.request primitives with the SSF parameter present shall be associated with a secure data set. Each member of a given secure data set shall be associated with the same Destination Address parameter value, Service Request set to Unicast, SSF parameter value and SSF-dependent parameter values. There shall be one secure data set for each secure relationship between a pair of nodes.

7.12.8.2 Secure Envelope IE

On generation of any frame containing a Fragment IE derived from a secure data set the MAC Entity:

- Generates an SE IE according to clause 7.8.2 with:
  - The SSF field set to the value of the Security Suite Family associated with the secure data set.
  - The SSF dependent fields set to the values of the SSF dependent parameters associated with the secure data set.
  - The Unencrypted IE List field set to a list of IEs intended for the destination node which do not require confidentiality protection.
  - The Fragment IE field set to the Fragment IE derived from the secure data set.

On receipt of a frame containing an SE IE the MAC Entity:

- If the Session ID field value indicates data confidentiality:
  - If the Fragment IE field contains a Fragment IE:
    - Its Fragment Data field shall be replaced with unencrypted data according to the procedures defined for the value of the SSF field and SSF dependent fields of the SE IE.
    - The Fragment IE shall be processed according to [2], clause 7.4.2.
- For each IE contained in the Unencrypted IE List field:
  - Processes the IE according to the procedures defined in clause 7.12.8 of the present document.

7.12.8.3 SK IE

On receipt of an MLM-NS.request primitive the MAC Entity:

If the Request Type field = New Session:

- Generates a SK IE according to clause 7.9.4.1 with:
  - Initiator Nonce field set to the value of the MLM-NS.request I-nonce parameter.
  - Key ID field set to the value of the MLM-NS.request Key ID parameter.
  - Initiator Random Value field set to the value of the MLM-NS.request I-rand parameter.
  - CST List field set to the value of the MLM-NS.request CST List parameter.

If the Request Type field = Session Created:

- Generates a SK IE according to clause 7.9.4.2 with:
  - Initiator Nonce field set to the value of the MLM-NS.request I-nonce parameter.
  - Responder Random Value field set to the value of the MLM-NS.request R-rand parameter.
  - Selected CST field set to the value of the MLM-NS.request Selected CST parameter.

If the Request Type field = Session Acknowledgement:

- Generates a SK IE according to clause 7.9.4.3 with:
  - Initiator Nonce field set to the value of the MLM-NS.request I-nonce parameter.

If the Request Type field = Session Destruction:

- Generates a SK IE according to clause 7.9.4.4 with:
  - If the I-nonce parameter is present in the MLM-NS.request:
    - I_{nonce} field set to the value of the MLM-NS.request I-nonce parameter.

The MAC Entity associates the SK IE with the node whose MAC Address matches the value of the Destination Address parameter of the MLM-NS.request for transmission using:

- A secured frame if a Session ID parameter was present in the MLM-NS.request.
- A non-secured frame if no Session ID parameter was present in the MLM-NS.request.

On receipt of a SK IE the MAC Entity:

If the value of the NS Message field identifies a New Session message:

- Generates an MLM-NS.indication according to clause 7.11.5.1 with:
  - I-nonce parameter set to the value of the received SK IE Initiator Nonce field.
  - Key ID parameter set to the value of the received SK IE Key ID field.
  - I-rand parameter set to the value of the Initiator Random Value field.
  - CST List parameter set to the value of the received SK IE CST List field.

If the value of the NS Message field identifies a Session Created message:

- Generates an MLM-NS.indication according to clause 7.11.5.2 with:
  - I-nonce parameter set to the value of the received SK IE Initiator Nonce field.
  - R-rand parameter set to the value of the received SK IE Responder Random Value field.
  - Selected CST parameter set to the value of the received SK IE Selected CST field.

If the value of the NS Message field identifies a Session Acknowledgement message:

- Generates an MLM-NS.indication according to clause 7.11.5.3 with:
  - I-nonce parameter set to the value of the MLM-NS Initiator Nonce field.

If the value of the NS Message field identifies a Session Destruction message:

- Generates an MLM-NS.indication according to clause 7.11.5.4 with:
  - If the Session Destruction message was received in a secured frame:
    - Session ID parameter set to the value of the Session ID field of the SE IE carrying the SK IE.

- If the I-nonce field is present in the SK IE:
  - I-nonce parameter set to the value of the received SK IE I_{nonce} field.

7.12.9 Data Transfer Services

Data Transfer services, as described in [2], clause 4.6 and as defined in [2], clause 7.4 shall be included in the present document.

7.12.9.1 Unicast Data Transfer

Unicast data transfer between two specific nodes described in [2], clause 4.6 and as defined in [2], clause 7.4.4.4 shall be included in the present document. Any frame exchanged via the Unicast Data Service:

- May be a Secured Frame as defined in clause 7.7.1 if a secure relationship has previously been established between the two specific nodes.

The basis for deciding to use a secured frame for frames without Fragment IEs is beyond the scope of the present document.

A frame containing a Fragment IE derived from a non-secure data set should not be a secured frame.

A frame containing a Fragment IE derived from a secure data set shall be a secured frame using:

- The SSF and SSF-dependent parameters from the one or more M-Data.request primitives from which the secure data set was generated.
- The next valid Frame Counter value for the secure relationship between the local node and the destination node.
  - All Unicast Data Service exchanges as defined in [2], clause 7.4.4.4:
- Shall operate in an identical manner irrespective of whether the frames so exchanged are secured frames or non-secured frames.
- If a frame is a secured frame:
  - Its content shall be as defined in [2], clause 7.4.4.4 encapsulated in an SE IE.
  - The SE IE shall be processed as defined in clause 7.9.

7.12.9.2 Beacon Data Transfer

Transmission of Beacon frames as described in [2], clause 4.6 shall be included in the present document as described in [2], clause 7.4.5.

7.12.9.3 Broadcast Data Transfer

Transmission of information on the Broadcast data service as described in [2], clause 4.6 shall be included in the present document as described in [2], clause 7.4.6.

7.12.9.4 Multicast Data Transfer

Transmission of information on Multicast data services as described in [2], clause 4.6 shall be included in the present document as defined in [2], clause 7.4.7.

7.13 Operating Class

The representation of frequency bands and centre frequencies corresponding to Channel Numbers shall be as described in [2], Annex A.

7.13.1 Regulatory Domain

The encoding of Regulatory Domain shall be as defined in [2], clause A1.

7.13.1.1 Global Operating Class

The encoding of frequency band and corresponding channel centre frequencies for the Global Regulatory Domain shall be as defined in [2], clause A2.

7.13.1.2 US Operating Class

The encoding of frequency band and corresponding channel centre frequencies for the US Regulatory Domain shall be as defined in [2], clause A3.

7.13.1.3 Japan Operating Class

The encoding of frequency band and corresponding channel centre frequencies for the Japan Regulatory Domain shall be as defined in [2], clause A4.

7.13.1.4 Europe Operating Class

The encoding of frequency band and corresponding channel centre frequencies for the Europe Regulatory Domain shall be as defined in [2], clause A5 with the addition of the classes shown in Table 23.

Table 23: Additional European Specific Operating Classes

Operating Class	Frequency Band	Channel Starting Frequency	Channel Spacing	Channel Set
4	870-876	870,2	0,2	29
5	915-921	915,2	0,2	29
6-255	Reserved	Reserved	Reserved	Reserved

8 Negotiation Session (NS) Protocol

The following protocol should be implemented by a MLM-NS Entity to generate, and process received, NS messages via the MLM-NS management interface.

8.1 NS State Machine Representation

The setup of a security session is described via an NS State Transition Diagram (STD) as shown in Figure 12.

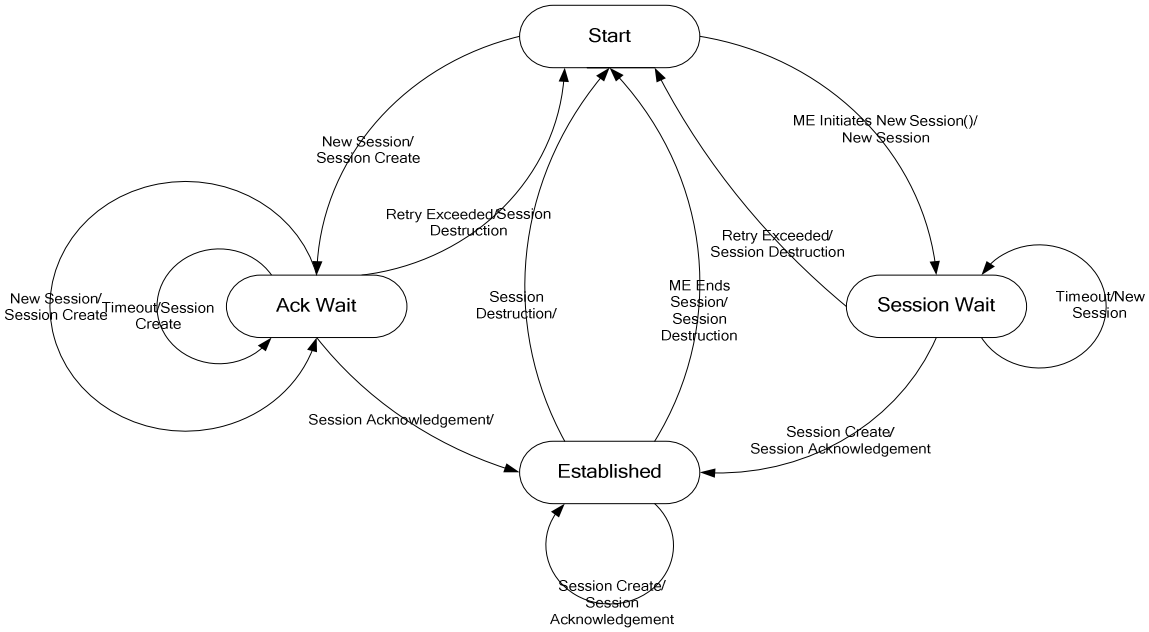

Figure 12: NS State Transition Diagram

There may be multiple NS state machines instantiated at any given time. The I_{nonce} in each SK IE (or the Session ID for a Session Destruction transition from Established to Start) shall be used to allow the NS Management Entity (ME) to differentiate between the state machines.

In Figure 12, the trigger for state transition is separated from the action taken by a "/". For example, "Open Session()/New Session" means that the services on the node initiated a new session with the Open Session() command to the NS ME which then sent an NS New Session message (see clause 7.9.4.1). Likewise "Session Destruction/" means that the NS ME received a Session Destruction message and took no other action besides the state transition.

The protocol is described in terms of the actions of an 'Initiator' node which transmits the New Session message and a 'Responder' node which transmits the Session Created message.

8.2 Necessary Conditions

If two nodes share a secret, and implement a common security suite, they may negotiate a session dynamically:

- Nodes share one or more shared secrets of lengths depending on the security requirements.
- Each shared secret shall be tagged with a 12 octet key identifier.
- Each shared secret shall be tagged with the MAC Address of the nodes with which is it shared.
- The nodes share at least one cipher suite.

How the secret is shared and how the key ID's are generated are out of scope of the present document.

8.3 Initiation

The Initiator:

- Generates two 8 octet random values I_{nonce} and I_{rand}
- Generates an MLM-NS.request with:
  - Request Type parameter set to indicate New Session message (see clause 7.9.4.1).
  - The Initiator Nonce parameter set to $I_{nonce.}$

- The Key ID parameter set to a key ID of a key it shares with the destination.
- The Initiator Random Value parameter set to $I_{rand.}$
- The CST List parameter set to the list of security suites it supports, in preference order:

To be sent in an unprotected (e.g. no security) frame.

8.4 Response

The Responder inspects the New Session message and, if it decides to proceed with the negotiation:

- Selects a supported cipher suite from the CST List field of the received New Session message.
- Confirms it has a common shared secret, $K_{ss,}$ tagged by the value of the Key ID field in the received New Session message.
- Generates an 8 octet random value $R_{rand.}$
- Derives the Session ID using:
  - The leftmost 2 octets (Imac xor Rmac xor Irand xor Rrand):
    - where I_{mac} and R_{mac} shall be the 8 octet MAC addresses of the Initiator and Responder respectively.
    - Note that the Session IDs are pairwise and the Responder shall ensure that the value of the Session ID so computed is unique for the Initiator, and if not, selects a new R_{rand} value and re-computes the XOR function above.
- Derives the Initiator's sending keys and its own (Responder's sending) keys using the Key Derivation Function (see clause 8.6) and shared secret associated with the Key ID indicated in the Selected CST.
- Generates an MLM-NS.request with:
  - Request Type parameter set to indicate Session Created message (see clause 7.9.4.2).
  - The I_{nonce} parameter set to the $I_{nonce.}$
  - The R_{rand} parameter set to $R_{rand.}$
  - The Selected CST parameter set to the CST value of the selected cipher suite.

To be sent unencrypted in a secured frame using:

- The computed Session ID.
- Sequence Number set to 1.

8.5 Confirmation

The initiator should send one more frames to set up its sequence number and to prove to the responder that both sides have the same set of keys. Any specific verification of the sequence number and key information is beyond the scope of the present document.

The Initiator derives the Responder's sending keys using the Key Derivation Function identified by the CST associated with the Session ID.

The Initiator validates the MIC (see clause 7.8.2) of the received frame using the Responder's sending keys. If the secured frame is valid, the Initiator knows the Responder shares the same secrets, same keys and has the same idea of the Responder's sequence number.

The Initiator generates an MLM-NS.request with:

- Message Type parameter set to a value indicating a Session Acknowledge message.

- The I_{nonce} parameter set to value of I_{nonce} for the session.
- Session ID parameter set to the value of the Session ID field of the received Session Created message.
- Sequence Number parameter set to 1.

When the Responder receives this frame and verifies it, the session setup is complete.

At this point both sides have the same keys, they have the same crypto suite, and they have securely set the sequence number for the mutual secure relationship identified by Session ID.

8.5.1 States

8.5.1.1 Start

This is the STD state where a session has not yet been created, or has been terminated. A transition from this state is initiated either with the reception of a New Session message, or by the ME initiating a new session.

8.5.1.2 Session Wait

This is an Initiator only state. At this point the Initiator is awaiting a Session Create message from the Responder. Upon timeout, it will retransmit the New Session message. Upon retries exceeded, it will abandon the session creation.

8.5.1.3 Ack Wait

This is a responder only state. At this point, the Responder has received a New Session message and sent a corresponding Session Create message to the Initiator. Upon timeout, it will retransmit the Session Create message. Upon retries exceeded, it will abandon the session creation.

8.5.1.4 Established

At this point the ME has received or sent the Session Acknowledgement message and has established the session. If it's sent Session Acknowledgement message is lost it may receive another duplicate Session Create message and shall respond with a duplicate Session Acknowledgement. An ME leaves this state and returns to Start either upon termination of the session, or upon receipt of a Session Destruction message. As part of the session termination process it shall send a Session Destruction message.

8.5.2 Events

Each state associated with transmission of an NS message has an associated retry counter and timer. The retry counter shall be initialized to cNSRetryCount (see clause 8.5.2.3) on first entry to the state but not on re-entry after a timeout.

The timer shall be set to NSTimeout on each entry to the state and cleared on exit from the state.

8.5.2.1 Timeout

If the timer expires before the state is exited, the retry counter shall be decremented, and the timeout action (generally re-sending a message) shall be taken.

8.5.2.2 Retry Exceeded

If, on decrementing after a timeout event, the value of the retry counter is zero, the action being re-tried shall be abandoned and the state shall be set to Start.

8.5.2.3 Constants and Attributes

Table 24: NS Protocol Constants and Attributes

Name	Type	Value	Description
NSTimeout	Integer	1 000 ms - 10 000 ms	NS Message timeout value. The value should be a random value in the range when each timer is initiated. It SHALL be set to a random rather than a fixed value.
cNSRetryCount	Integer	5	NS message retry count value.

8.6 Key Derivation Function

8.6.1 KDF 1 - SP800-108-CMAC

The following values shall be used to derive keys using this KDF function:

- Initiator's sending keys: KDF (K_{ss}, Label, I_{rand} || R_{rand}).
- Responder's sending keys KDF (K_{ss}, Label, R_{rand} || I_{rand}).
- Where || denotes the concatenation operator.
- K_{ss} shall be the shared secret key identified by the Key ID in the session negotiation. For each use of the KDF the length of K_{ss} shall be equal to the value of the Symmetric Key Size of the CST associated with the secure relationship for which the KDF is being invoked.
- Label shall be the 4 byte constant - { 0x05 0xE5 0x51 0x04}.
- Context shall be the concatenation of I_{rand} || R_{rand} for the initiator's sending keys, and R_{rand} || I_{rand} for the responder's sending keys.
- The PRF shall be the CMAC as specified in [7] with the algorithm and key size the same as that specified in the CST associated with the secure relationship for which the KDF is being invoked.

If a single key is being generated (e.g. for an AEAD cipher), generate enough key material to instantiate the key from the KDF and assign that material to the key. For example, an AES 128 bit key needs 16 octets of data.

If multiple keys are being derived, they shall be derived in this order from the KDF stream:

- Integrity Key.
- Encryption Key.

For example, to use the KDF to derive an AES 128 bit key and an HMAC 256 bit key, generate 48 octets of data from the KDF and assign the first 32 octets to the HMAC key and the last 16 octets to the AES key.

9 PICS Proforma

The PICS information for devices operating in Mode 1 shall be as in clause 6.5 of the present document.

The PICS information for devices operating in Mode 2 shall be as shown in Table 25.

Table 25: PICS for Devices in Mode 2

Specification Reference TS 102 887-2	Specification Reference ANSI/TIA 4957.200	Description	Mandatory Optional Conditional	Support Declared (Y/N)
	4.3	ADDRESSING		
	4.3.1	Node Address	M	
	4.3.2	Broadcast Address	O	
	4.3.3	Multicast Addresses	O	
	4.4	THE CHANNEL FUNCTION	M	
	4.5	COMMUNICATIONS LINK	M	
	4.6	DATA TRANSFER SERVICES		
	4.6.1	Unicast data service	M	
	4.6.2	Beacon data service	M	
	4.6.3	Broadcast data service	O	
	4.6.4	Multicast data service	O	
	4.6.5	Collision avoidance	O	
	4.9	NODE ANNOUNCEMENT AND NEIGHBOUR DISCOVERY SERVICE	M	
	4.1	POWER SAVING	O	
	4.11	OPERATING CLASS SWITCHING	O	
	5.2	MAC FRAME FORMAT		
	5.3	MAC HEADER		
	5.3.1	Frame Control Field		
	5.3.1.1	Frame ID	M	
	5.3.1.2	Frame ID Extension	M	
	5.3.1.3	Addressing Mode fields	M	
	5.3.1.4	Version Field	M	
	5.3.2	Destination Address Field	M	
	5.3.3	Source Address Field	M	
	5.3.4	Frame check sequence	M	
7.7.1		Secure Frame Format	M	
	5.4	INFORMATION ELEMENTS (IEs)		
	5.4.1	Short Information Elements		
	5.4.1.1	Fractional Sequence Interval (FSI) IE	M	
	5.4.1.2	Fractional Dwell Interval (FDI) IE	O	
	5.4.1.3	Node Announcement (NA) IE	M	
	5.4.1.4	Flow Control (FC) IE	M	
	5.4.1.5	Power Saving (PS) IE	O	
	5.4.1.6	Rendezvous (RDV) IE	O	
	5.4.1.7	Operating Class Switching (OCS) IE	O	
	5.4.1.8	Probe IE	M	
7.9.4		Session Key	M	
	5.4.1.9	Vendor Specific Short (VSS) IE	O	
	5.4.2	Long Information Elements		
	5.4.2.1	Encapsulated MSDU (EMSDU) IE	M	
	5.4.2.2	MAC Layer Management (MLM) IE	O	
	5.4.2.3	Fragment IE	M	
7.8.2		Secure Envelope	M	
	5.4.2.4	Vendor Specific Long (VSL) IE	O	
7.9		Security Suite Families	M	
7.9.1		Auxiliary Security Header	O	
7.9.2		Cipher Suite Tuples	O	
7.9.3		Negotiated Session	O	
7.10	6.3	MAC SUB-LAYER INFORMATION ATTRIBUTES	M	
	7	MAC SUB-LAYER FUNCTIONAL SPECIFICATION		
	7.1	CHANNEL FUNCTION	M	
	7.2	FRAME TRANSFER		
	7.2.2	Sequence Numbers	M	
7.12.7		Frame Counter	M	

Specification Reference TS 102 887-2	Specification Reference ANSI/TIA 4957.200	Description	Mandatory Optional Conditional	Support Declared (Y/N)
	7.3	INFORMATION ELEMENTS		
	7.3.1	Fractional Sequence Interval IE	M	
	7.3.2	Fractional Dwell Interval IE	O	
	7.3.3	Flow Control (FC) IE	M	
	7.3.4	Power Saving (PS) IE	O	
	7.3.5	Rendezvous (RDV) IE	O	
	7.3.6	Operating Class Switching IE	O	
7.12.8.1	7.3.7	EMSDU IE	M	
	7.3.8	MLM IE	O	
	7.3.9	Node Announcement IE	M	
	7.3.10	Probe IE	M	
7.12.8.3		Session Key	O	
7.12.8.2		Secure Envelope	M	
	7.3.11	Vendor Specific IE	O	
	7.4	DATA TRANSFER SERVICES		
	7.4.1	Aggregation and Fragmentation	M	
	7.4.2	Re-Assembly	M	
	7.4.3	Re-transmission	M	
	7.4.4	Unicast Data Service		
	7.4.4.1	Instantiation of the Communications Link	M	
	7.4.4.2	Termination of the Communications Link	M	
	7.4.4.3	Conclusion of the Communications Link	M	
	7.4.4.4	Unicast Transmission		
	7.4.4.4.1	Initial Frame Transmission	M	
	7.4.4.4.2	Subsequent Frame Transmission	M	
	7.4.4.5	Unicast Reception		
	7.4.4.5.1	Initial Frame Reception	M	
	7.4.4.5.2	Subsequent Frame Reception - Fragment IE	M	
	7.4.4.5.3	Subsequent Frame Reception - No Fragment IE	M	
	7.4.4.5.4	Subsequent Frame Reception	M	
	7.4.5	Beacon Data Service	M	
	7.4.6	Broadcast Data Service	O	
	7.4.6.1	Busy Channel Deferral	O	
	7.4.7	Multicast Data Service	O	
	ANNEX B	CHANNEL TABLE		
		Channel Table Population Function	M	

Table 26: Operating Class Support

Specification Reference	Page #	Description		Mandatory Optional Conditional	Support Declared (Y/N)
ANNEX A	39	OPERATING CLASS			
A.1	39	REGULATORY DOMAIN (see note)			
A.2	39	**GLOBAL OPERATING CLASS**		O	
		Operating Class	Frequency Band		
		1	2400-2483.5	C	
		2	2400-2483.5	C	
A.3	40	**US OPERATING CLASS**		O	
		Operating Class	Frequency Band		
		1	470-510	C	
		2	470-510	C	
		3	779-787	C	
		4	779-787	C	
		5	863-870	C	
		6	863-870	C	
		7	902-928	C	
		8	902-928	C	
		9	917-923.5	C	
		10	917-923.5	C	
		11	169.4-175	C	
		12	450-470	C	
		13	896-901	C	
		14	896-901	C	
		15	896-901	C	
		16	902-902	C	
		17	902-902	C	
		18	902-902	C	
		19	928-960	C	
		20	928-960	C	
		21	928-960	C	
		22	1427-1518	C	
		23	1427-1518	C	
		24	1427-1518	C	
		25	54-698	C	
		26	54-698	C	
A.4	41	**JAPAN OPERATING CLASS**		O	
		Operating Class	Frequency Band		
		1	950-958	C	
		2	950-958	C	
		3	950-958	C	
		4	920-928	C	
		5	920-928	C	
		6	920-928	C	
		7	470-770	C	
		8	470-770	C	
		9	470-770	C	
A.5	41	**EUROPE OPERATING CLASS**		O	
		Operating Class	Frequency Band		
		1	863-870	C	
		2	863-870	C	
		3	169.400-169.475	C	
		4	870-876	C	
		5	915-921	C	
NOTE: Shall support at least one Region and at least one Operating Class in each Region supported.					

History

Document history		
V1.1.1	September 2013	Publication