

# ISO/IEC/IEEE 8802-15-9:2024-11 (E)

## Telecommunications and information exchange between systems - Local and metropolitan area networks specific requirements - Part 15-9: Transport of Key Management Protocol (KMP) Datagrams

---

Contents	Page
1. Overview.....	12
1.1 General.....	12
1.2 Scope.....	12
1.3 Purpose.....	12
1.4 Deprecated features.....	12
1.5 Word usage .....	12
2. Normative references.....	13
3. Definitions, acronyms, and abbreviations.....	13
3.1 Definitions .....	13
3.2 Acronyms and abbreviations .....	13
4. Introduction.....	14
4.1 Overview.....	14
4.2 System view .....	15
4.3 Network view.....	16
4.4 Security associations.....	16
4.5 Process flow.....	16
4.6 State machine.....	17
4.7 Address formats .....	17
4.8 KMP payload size.....	17
4.9 Format conventions.....	17
5. MPX data service.....	17
5.1 Description.....	17
5.2 MPX data primitives .....	18
5.3 MPX-PURGE primitive.....	25
5.4 MPX PIB attributes.....	27
6. KMP transport service .....	27
6.1 Overview.....	27
6.2 KMP-CREATE primitives.....	28
6.3 KMP-FINISHED primitives.....	33
6.4 KMP-DELETE primitives .....	35
6.5 KMP-PURGE primitives .....	37
7. MPX IE format .....	39
7.1 IE overview.....	39
7.2 Payload IE group ID .....	39
7.3 MPX IE content .....	39
8. KMP Service.....	43
8.1 KMP ID.....	43
8.2 Vendor-specific KMPs .....	43

9.	State machines .....	44
9.1	Inbound state machine .....	44
9.2	Outbound state machine.....	46
	Annex A (informative) KMP specifics—IEEE 802.1X/MKA.....	47
A.1	Description.....	47
A.1.1	Device authentication.....	47
A.1.2	Device authentication and cryptographic key agreement.....	48
A.2	Use cases.....	51
A.2.1	Overview .....	51
A.2.2	Isolated enclave .....	52
A.2.3	Star topology .....	52
A.2.4	Mesh .....	52
A.3	IEEE 802.15 specifics.....	52
A.3.1	EAPOL message framing.....	52
A.3.2	EAPOL-MKA .....	52
A.3.3	EAPOL-KEY .....	54
A.3.4	ETSI TS 102 887-2 .....	54
A.3.5	Group Traffic Key Generation .....	54
	Annex B (informative) KMP specifics—IKEv2 .....	56
B.1	Description.....	56
B.2	Use cases.....	56
B.2.1	General .....	56
B.2.2	Minimal IKEv2 use cases.....	56
B.2.3	Enterprise or large-scale IKEv2 use cases .....	57
B.3	IKEv2 and IEEE 802.15 specifics .....	57
B.3.1	Overview .....	57
B.3.2	Supported IKEv2 features .....	57
B.3.3	Unused IKEv2 features .....	57
B.3.4	Message framing .....	57
B.3.5	Algorithm negotiation .....	58
B.3.6	Key derivation.....	58
B.3.7	Broadcast and multicast key distribution .....	58
	Annex C (informative) KMP specifics—HIP.....	59
C.1	Description.....	59
C.2	Use cases.....	59
C.2.1	General .....	59
C.2.2	Isolated enclave .....	59
C.2.3	Home net .....	60
C.2.4	City net .....	60
C.2.5	RFID networks .....	60
C.2.6	Infrastructure sensor nets.....	60
C.3	IEEE 802.15TM specifics.....	60
C.3.1	Message framing .....	60
C.3.2	Key derivation and security PIB interaction .....	60
C.3.3	Deployment recommendations.....	60
C.3.4	HIT authentication.....	61

Annex D (informative) KMP specifics—PANA .....	62
D.1 Description.....	62
D.2 Use cases.....	62
D.3 IEEE 802.15 specifics.....	62
Annex E (informative) KMP specifics—Dragonfly.....	65
E.1 Description.....	65
E.1.1 General .....	65
E.1.2 Device authentication.....	65
E.1.3 Device authentication and cryptographic key establishment .....	65
E.2 Use cases.....	67
E.3 Dragonfly and IEEE 802.15 specifics.....	67
E.3.1 Overview .....	67
E.3.2 Algorithm negotiation .....	68
E.3.3 Key derivation .....	68
E.3.4 Message framing .....	68
E.3.5 Broadcast and multicast key distribution .....	69
Annex F (informative) IEEE 802.15.4 security.....	70
F.1 Description.....	70
F.2 Link keys.....	70
F.3 Group keys.....	71
F.3.1 Overview .....	71
F.3.2 Key Identifier Mode 0x01 .....	71
F.3.3 Key Identifier Mode 0x02 .....	71
F.3.4 Key Identifier Mode 0x03 .....	72
Annex G (informative) Bibliography .....	73