

IQRF[®] Smarter Wireless. Simply.

IQRF Standard Specification (PREVIEW)

rev: 240303

Specification can be changed without notice

1 Abstract

2 Since 2004, MICRORISC s.r.o. and IQRF Tech s.r.o. have developed a low-cost, low-power, two-way, wireless mesh
3 communication technology. Thanks to the 2-decades continuous development for and with our customers, we created state-
4 of-art communication technology for wireless mesh networks featuring values:

- 5 • Industrial reliability,
- 6 • simple integration,
- 7 • ultimate security,
- 8 • interoperability and huge ecosystem,
- 9 • true low power efficiency.

10 Dozens of patents were granted, protecting the IQRF® and its implementors from plagiarism and saving their investments.

11 The IQRF® moves to the third decade as an open standard. This document discloses the specifications needed for the IQRF
12 standard implementation. The IQRF standard implementations and use of all IQRF standard-related essential patents are
13 allowed under a single royalty-free license.

14 Keywords

15 Wireless; Mesh; Networks; IQRF; Standard; Open; Free

16 Patents and licensing

17 Specific protocols, arrangements, and solutions described in this specification are protected by one or more patents in Czech,
18 EU, USA, China, and Japan. A single royalty-free license allows the IQRF standard implementation and use of all IQRF Standard
19 related essential patents. For details, check the website <https://standard.iqrf.org>.

20 Copyright

21 Copyright © 2023, IQRF Standards Association z.s. All Rights Reserved. This information within this document is the property
22 of IQRF Standards Association z.s. and its use and disclosure are restricted.

23 This document and the information contained herein are provided on an “as is” basis and IQRF Standards Association z.s.
24 disclaims all warranties, including but not limited to (a) any warranty that the use of the information herein will not infringe
25 any rights of third parties (including without limitation any intellectual property rights including patent, copyright or
26 trademark rights) or (b) any implied warranties of merchantability, fitness for a particular purpose, title or noninfringement.
27 In no event will IQRF Standards Association be liable for any loss of profits, loss of business, loss of use of data, interruption
28 of business, or for any other direct, indirect, special or exemplary, incidental, punitive or consequential damages of any kind,
29 in contract or in tort, in connection with this document or the information contained herein, even if advised of the possibility
30 of such loss or damage. All Company, brand and product names may be trademarks that are the sole property of their
31 respective owners.

32 The above notice and this paragraph must be included on all copies of this document that are made.

33

34 IQRF Standards Association z.s.

35 Prumyslova 1275

36 506 01 Jicin

37 Czech Republic, EU

38

39

40 [Quick link to Table of contents](#)

1 **1. DOCUMENT**

2 **1.1. HISTORY AND REVISIONS**

revision	date	description
230807	August 07, 2023	preliminary documentation draft
231117	November 17, 2023	The EAP release under NDA only, v ISS 0.91
24030	March 03, 2024	The first public release, ISS v 0.95

3 **1.2. AUTHORS AND CHAPTERS SUPERVISORS**

- 4 • General concept and the first public release of the Specification
 - 5 ○ Vladimír Šulc, Ph.D., MICRORISC s.r.o.,
- 6 • Chapter 10 Security specification:
 - 7 ○ Ondřej Hujňák, Brno Technical University, Faculty of Informatics,
- 8 • Annex A – Region related setup:
 - 9 ○ Pavel Plecháč, Jiří Poš, MICRORISC s.r.o.,
- 10 • Special thanks to:
 - 11 ○ MICRORISC R&D team for the continual support and the IQRF legacy implementations,
- 12 • Acknowledgements:
 - 13 ○ Ministry of Industry and Trade of Czech Republic for the financial support of IQRF-related projects,
 - 14 ○ The Brno University of Technology, Faculty of Electrical Engineering and Communication, for cooperation
 - 15 in IQRF-related projects,
 - 16 ○ The Technical University of Ostrava, Faculty of Electrical Engineering and Computer Science, for
 - 17 cooperation in IQRF-related projects.

18 **1.3. SCOPE**

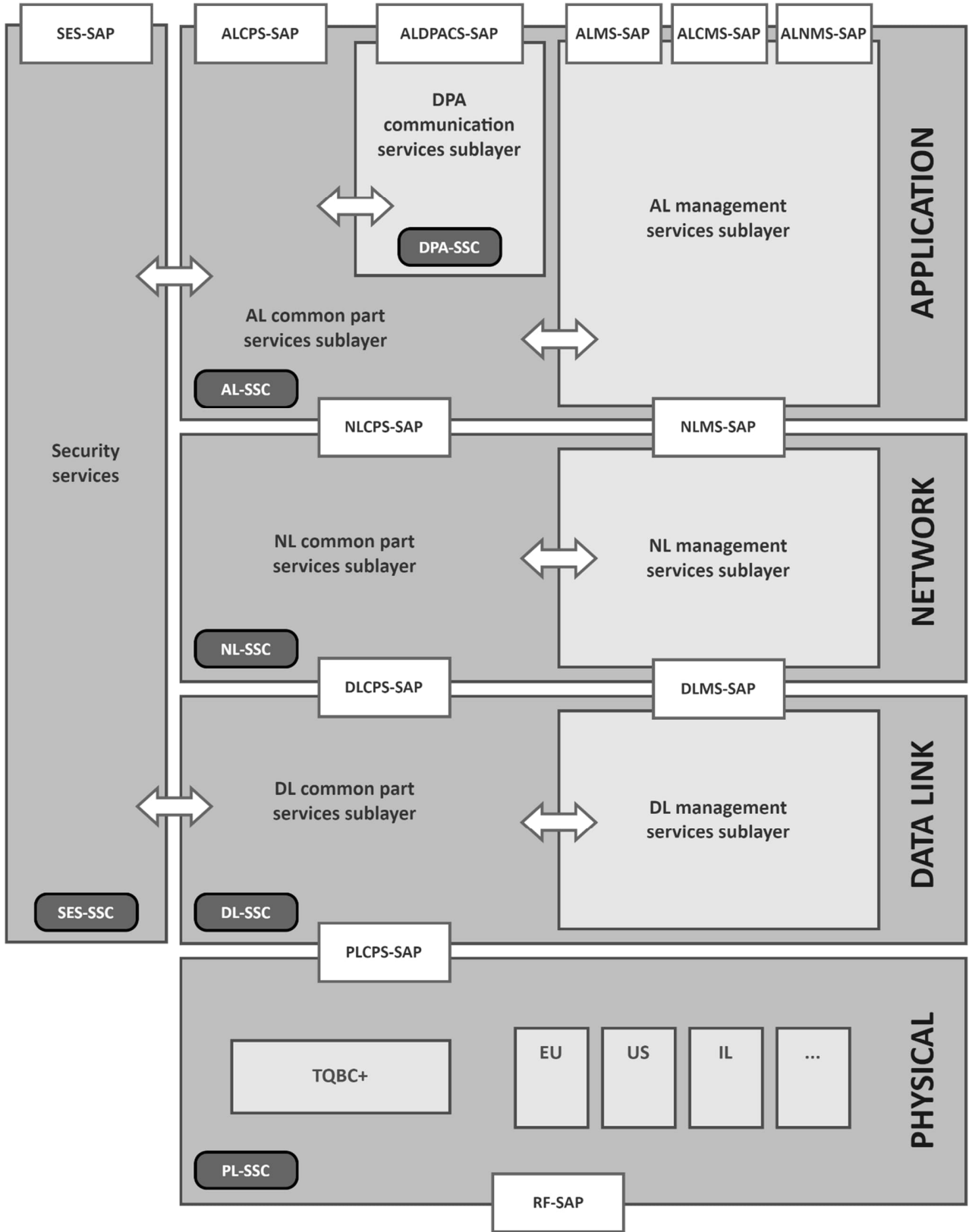
19 This document contains specifications and descriptions of processes, data structures, security, interfaces, protocols, timings,
 20 and algorithms related to the IQRF standard.

21 **1.4. PURPOSE**

22 The purpose of this document is to provide a complete description of the IQRF standard as a basis for implementing
 23 interoperable, low-cost, highly reliable, and usable products for wireless mesh applications. Implementations of the IQRF
 24 standard shall keep definitions and rules described in this specification, especially data structures, process flows, and timings,
 25 to ensure devices interoperability. Implementations, on the other hand, should be optimized for the ported MCUs and radios.

26 **1.5. DESIGN ARCHITECTURE**

27 The IQRF layered architecture design is based on the ISO OSI standard recommendations. Each layer performs a specific set
 28 of services for the layer above. Detailed architecture is depicted in Figure 1.



1

2

Figure 1: IQRF standard design architecture

1 1.6. ACRONYMS

AES	Advanced encryption standard
AL	Application layer
ALCMS-SAP	ALMS service access point (coordinator)
ALCPS	Application layer common part services (sublayer)
ALDPACS	Application layer DPA communication services (sublayer)
ALMS	Application layer management services
ALNMS-SAP	ALMS service access point (node)
AL-SSC	Application Layer System Setup and Configuration
ASID	Association ID
ASPS	Association PHY setup
BED	Beaming device (device class)
BEN	Beaming node
BNCK	Base Network Communication Key
CBC	Cipher Block Chaining
CBC-MAC	Cipher block chaining message authentication code
CCM	Counter with CBC-MAC
CRC	Cyclic redundancy check
CSMA	Carrier sense multiple access
CSMA-CA	Carrier sense multiple access with collision avoidance
DFR	Data link footer
DHR	Data link header
DJK	Device joining key
DL	Data Link or Data Link Layer
DLCPS	Data Link Common Part Services (sublayer)
DLK	Data link key
DLMS	Data Link Management Services (sublayer)
DL-SSC	System Setup and Configuration for Data link Layer
DPA	Direct Peripheral Access
F-ASA	ASSOCIATED frame for active association
F-ASP	ASSOCIATED frame for passive association
FCE	Frame Control Element
FCS	Frame control setup
F-JR	JOIN-REQUEST frame
FNF	Fixed network frame
FRC	Fast response command
FRE	Frame element
FRXE	SSC FRX element
FSK	Frequency shift keying
FTXE	SSC FTX element
GFSK	Gaussian frequency-shift keying
IMAC	IQRF MAC address

IQRF-SA	IQRF Standards Association
ISS	IQRF Standard Specification
IUK	Individual unicast key
IWMN	IQRF wireless mesh network
KDF	Key derivation function
LBT	Listen before talk
LPLN	Low power and lossy network
LPRX	Low power receive (mode)
LPTX	Low power transmission (mode)
LSb	Least significant bit
LSB	Least significant byte
MAC	Message authentication code
MAC	Medium access control
MSb	Most significant bit
MSB	Most significant byte
NAK	Network access key
NHL	Next higher layer
NHLE	Next Higher Layer Entity
NHR	Network header
NID	Network identification
NL	Network layer
NLCPS	Network layer common part services
NLL	Next Lower Layer
NLMS	Network layer management services
NL-SSC	Network layer system setup and configuration
NRN	Non-routing node
OFMO	Offline mode
PDU	Protocol data unit
PFR	PHY footer
PHR	PHY header
PHY	Physical or PHY (layer)
PL	PHY layer
PLCPS	Physical link layer common part services
PL-SSC	Physical layer system setup and configuration
PNPS	Particular network PHY setup
PPS	Primitive parameters setup
RF	Radio frequency
RFIC	Radio frequency integrated circuit
RIDX	Rotation index
RON	Routing node
RON/A	RON or RONA
RONA	Routing node with aggregation
ROR	Router (device class)

ROR/A	ROR or RORA
RORA	Aggregating router (device class)
RRPS	Region related PHY setup
RRPS	Region related PHY setup
RSSI	Received signal strength indication
RTHR	Routing header
RX	Receive or Receiver
RXMO	Online mode
SAP	Service access point
SES	Security services (layer/block)
SES-SSC	SES system setup and configuration
SNF	Standard network frame (no routing)
SNFR	Standard network frame (routing)
SNNF	Standard non-network frame
SSC	System setup and configuration
SSCE	SSC element
SSC-FRX	SSCE Frame RX
SSC-FTX	SSCE Frame TX
SSCID	SSC element ID
STDRX	Standard receive (mode)
STDTX	Standard transmission (mode)
TDMA	Time division multiple access
TIQBC	Time quanta bit coding
TISS	This IQRF standard specification
TLL	Time-Limited loop
TX	Transmit or Transceiver
VRN	Virtual routing number
WMN	Wireless mesh network
XLPTX	Extra low power transmission (mode)

1

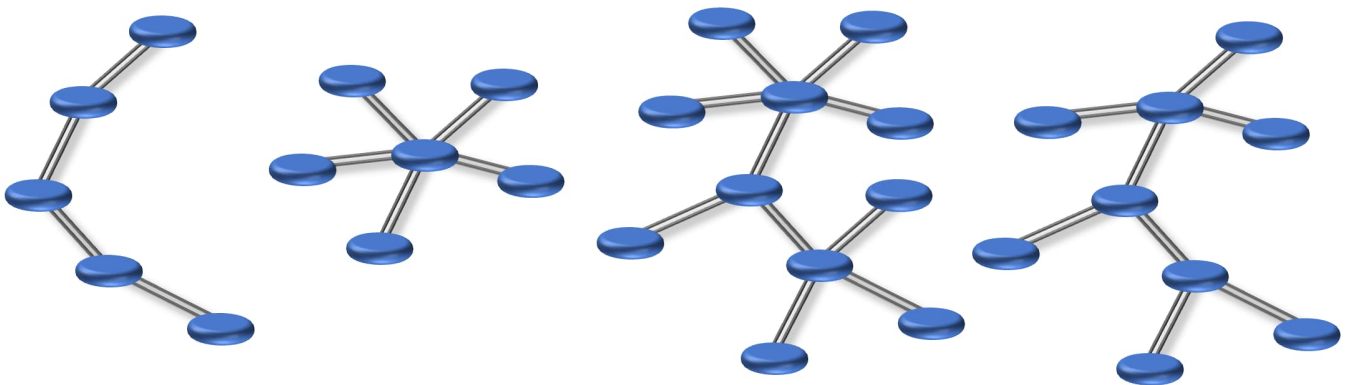
2

1 **4. IQRF BRIEF OVERVIEW**

2 Only fundamental principles are described here. A detailed functional description is available in Chapter 11.

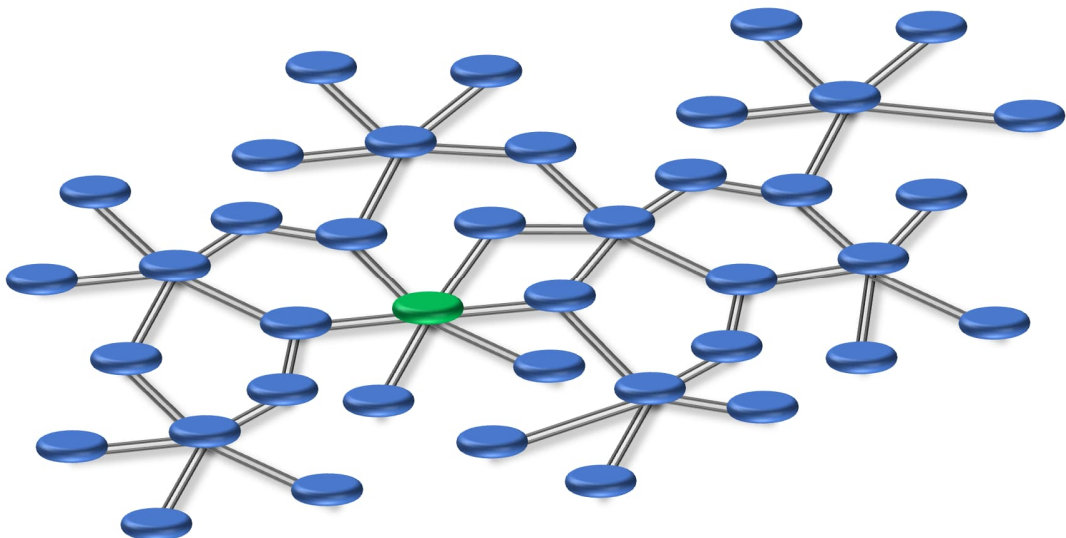
3 **4.1. GENERAL WIRELESS MESH NETWORKS**

4 Wireless mesh networks are a type of network setup that involves multiple wireless router nodes or points spreading across
 5 a large area to provide Internet or network coverage. Unlike traditional networks, which rely on a small number of wired
 6 access points or wireless routers, mesh networks consist of many wireless nodes that communicate with each other to spread
 7 the network coverage over a vast area. This setup allows data to be relayed across the nodes, finding the fastest and most
 8 efficient path to its destination. Mesh network topology is the most general network arrangement, including many other
 9 distinguished topologies, like the chain, star, or tree. Examples of mesh networks are depicted in the figure below.



10 **4.2. IQRF MESH NETWORK**

11 IQRF networks are organized and orchestrated. The coordinator is such a conductor for other network devices called nodes.
 12 Nodes with the routing capability are called routers. The network communication is always encrypted and authenticated
 13 according to the latest security standards. The IQRF networks support up to 1024 devices and up to 255 routing hops. Typical
 14 IQRF network arrangement is depicted in figure below.



1 4.3. NETWORK DEVICES

2 4.3.1. COORDINATOR

3 Coordinator is a device orchestrating the IQRF network and associating other devices, nodes, to the network. Network
4 address of the coordinator and its Virtual routing number are always 0x00.

5 4.3.2. NODE

6 Node is a general device joining the IQRF network.

7 4.3.2.1. ROUTING NODE

8 Routing nodes are nodes associated to the network with addresses 1 – 255. Routing nodes participate in the routing and in
9 the aggregation phase of the FRC protocol.

10 4.3.2.2. ROUTING NODE WITH THE AGGREGATION

11 Routing nodes with aggregation are routing nodes with the capability of listening to the beaming nodes, store their
12 transmissions and provide requested data from these transmissions through the FRC protocol.

13 4.3.2.3. NON-ROUTING NODE

14 Non-routing nodes are node devices associated to the network with addresses 256 – 511. Non-routing nodes are always in
15 receiving and processing incoming transmissions, they do not participate in the routing.

16 4.3.2.4. BEAMING NODE

17 Beaming node is a low power node associated to the network with addresses 512 – 1023. Beaming nodes awake periodically
18 or upon defined conditions to transmit their data. Beaming nodes do not participate in the routing and due to the minimizing
19 consumption are not responding to the standard network communication unless they do not switch to the receive mode.

20 4.4. CREATING THE NETWORK

21 4.4.1. ASSOCIATION OF JOINING DEVICES

22 The association is the process controlled by the coordinator and used to establish membership in a network for joining nodes.
23 The coordinator shares bonding information, such as communication keys and network setup, with nodes in a secure way
24 through the encrypted payload and dedicates a unique network address to each node. The IQRF MAC address is used for
25 authentication as a unique identifier of IQRF devices.

26 4.4.2. DISCOVERY OF ROUTING DEVICES TOPOLOGY

27 The discovery is the process by which the coordinator discovers routing nodes' topology and dedicates them the Virtual
28 Routing Number, a unique number reflecting distance from the coordinator in hops and defining a time slot during routing.

29 4.5. NETWORK COMMUNICATION

30 In most application scenarios, the coordinator initiates communication, and nodes respond through the IQMESH and FRC
31 protocols. Routed networking communication is always orchestrated while beaming nodes transmit their data
32 asynchronously.

1 4.5.1. DATA AND SYSTEM COMMUNICATION

2 There are two basic types of communication – data communication and system communication.

3 Data communication is realized through the standard data frames and enables data delivery to the next higher layer above
4 the application layer.

5 The system communication supports protocols and functionality described in the IQRF standard specification; the application
6 and lower layers process it, and data are not provided to the layers above the application layer. The system communication
7 is realized through standard non-network, standard networking, and fixed network frames.

8 4.5.2. COMMUNICATION SECURITY

9 System non-networking and complete networking communication is always encrypted and authenticated as described in this
10 specification.

11 4.6. ADDRESSING

12 The IQRF supports following addressing modes without acknowledgment

- 13 • Unicast from the coordinator to any node,
- 14 • unicast from the routing node to the coordinator,
- 15 • broadcast sent by the coordinator to all network devices,
- 16 • broadcast sent by the coordinator or by the node to the neighboring devices,

17 The IQRF supports following acknowledged addressing modes:

- 18 • Broadcast initiated by the coordinator (FRC protocol),
- 19 • multicast initiated by the coordinator (FRC protocol),
- 20 • selectivecast initiated by the coordinator (FRC protocol),
- 21 • broadcast initiated by the node (local FRC protocol),
- 22 • selectivecast initiated by the node (local FRC protocol),

23 4.7. IQMESH® ROUTING PROTOCOL

24 IQMESH routing protocol is collision-free, based on the TDMA and oriented flooding, supporting unicast, broadcast,
25 groupcast, and selectivecast. It is deterministic and reliable and perfectly works even under challenging environments.

26 The coordinator detects routing nodes topology during the discovery. Based on the discovered topology the coordinator
27 dedicates the Virtual Routing Number to routing nodes. The virtual routing number is a unique number reflecting distance
28 from the coordinator in hops and defining a time slot during routing. Thanks to the virtual routing number each router knows
29 its position in the network and its dedicated time slot.

30 TDMA and VRN-based directional flooding guarantees deterministic and collision-free routing.

31 4.8. FRC® DATA AGGREGATION PROTOCOL

32 The FRC protocol is based on the IQMESH network arrangements and routing protocol. It enables fast data aggregation and
33 acknowledged broadcasts/multicasts. The FRC protocol further increases IQMESH protocol reliability and provides high-level
34 robustness and successful delivery even under very challenging conditions, being an excellent solution for lossy, low-rate
35 wireless mesh networks.

36 FRC protocol supports acknowledged broadcast and multicast, and thanks to its high efficiency and reliability, it can be used
37 as an excellent tool for network management.

1 4.9. IQRF DPA PROTOCOL

2 Direct Peripheral Access (DPA) protocol is a simple byte-oriented protocol used to control services and peripherals of the
3 IQRF network devices directly from device interfaces such as SPI or UART. IQRF standard specification defines only data
4 communication service support via the DPA protocol. A complete description of the IQRF DPA protocol is available at
5 <https://iqrf.org/dpa>.

6 4.10. IQRF SECURITY

7 The Security Services layer is responsible for ensuring the following security objectives:

- 8 • Frame integrity
- 9 • Networking frame authenticity
- 10 • Footer and Payload confidentiality
- 11 • Replay protection

12 The IQRF uses authenticated encryption with associated data (AEAD) based on the NIST standardized CCM scheme.

1 17. LIST OF FIGURES

2

3 FIGURE 1: IQRF STANDARD DESIGN ARCHITECTURE 4

4 FIGURE 2: FLOW DIAGRAM EXAMPLE 10

5 FIGURE 3: CONCEPT OF PRIMITIVES 14

6 FIGURE 4: APPLICATION LAYER 20

7 FIGURE 5: NETWORK LAYER 50

8 FIGURE 6: DATA LINK LAYER 62

9 FIGURE 7: STANDARD NON-NETWORK FRAME 74

10 FIGURE 8: SNNF DETAILED STRUCTURE BY OCTETS 74

11 FIGURE 9: STANDARD NETWORK FRAME (NO ROUTING) 74

12 FIGURE 10: SNF DETAILED STRUCTURE BY OCTETS 75

13 FIGURE 11: STANDARD NETWORK FRAME (ROUTING) 75

14 FIGURE 12: STANDARD NETWORK FRAME (ROUTING) 76

15 FIGURE 13: FIXED NETWORK FRAME 76

16 FIGURE 14: FNF DETAILED STRUCTURE 76

17 FIGURE 15: F-JR FRAME STRUCTURE AND SETUP 77

18 FIGURE 16: F-JR FRAME PAYLOAD STRUCTURE 77

19 FIGURE 17: F-ASA FRAME (ACTIVE ASSOCIATION) 78

20 FIGURE 18: F-ASA FRAME PAYLOAD STRUCTURE 78

21 FIGURE 19: F-ASP FRAME (PASSIVE ASSOCIATION) 79

22 FIGURE 20: F-ASP FRAME PAYLOAD STRUCTURE 80

23 FIGURE 21: FRC FRAME BROADCAST (F-FB) 80

24 FIGURE 22: FRC FRAME SINGLES (F-FS) 81

25 FIGURE 23: FRC FRAME SINGLES (F-FC) 81

26 FIGURE 24: PHYSICAL LAYER 85

27 FIGURE 25: BITSTREAM STRUCTURE 93

28 FIGURE 26: PHY HEADER 93

29 FIGURE 27: SECURITY SERVICES LAYER 98

30 FIGURE 28: EXAMPLES OF THE REPLY PROTECTION PROCESSING 125

31 FIGURE 29: BONDING INFORMATION 128

32 FIGURE 30: ASSOCIATION BASED ON THE REQUEST TO JOIN 128

33 FIGURE 31: PASSIVE ASSOCIATION 129

34 FIGURE 32: TIMING FOR BROADCASTED F-ASP FRAME 130

35 FIGURE 33: ADDRESSING IS REALIZED THROUGH THE NADDR FRAME ELEMENT 131

36 FIGURE 34: DISCOVERY CONSISTS OF REPEATEDLY CALLED FRC/DATA PRIMITIVES UNTIL NO NEW ROUTER REPLIES 135

37 FIGURE 35: TIME SYNCHRONIZATION BETWEEN SENDER AND RECIPIENTS (INSIDE TIMESLOT) 138

38 FIGURE 36: COORDINATOR TRANSMITS STANDARD ROUTED NETWORK FRAME (SNFR) 139

39 FIGURE 37: NODE SNFR FORWARDING 139

40 FIGURE 38: DEDICATED TIMESLOTS DURING ROUTING ORIGINATED BY THE COORDINATOR 140

41 FIGURE 39: DEDICATED TIMESLOTS DURING ROUTING ORIGINATED BY THE NODE WITH THE VRN_x 140

42 FIGURE 40: RTPAR FRAME ELEMENT IN F-FB FRAMES IS USED FOR FRC CONFIGURATION 142

43 FIGURE 41: FRC TIMING 144

44 FIGURE 42: FRC COMMUNICATION FLOW BETWEEN COORDINATOR AND ADDRESSED RON 145

45 FIGURE 43: FRC COMMUNICATION FLOW BETWEEN THE COORDINATOR AND ADDRESSED NRN 146

46 FIGURE 44: FRC COMMUNICATION FLOW BETWEEN THE COORDINATOR AND NOT ADDRESSED RON 147

47 FIGURE 45: FRC COMMUNICATION FLOW BETWEEN THE COORDINATOR AND NOT ADDRESSED NRN 148

48 FIGURE 46: FRC COMMUNICATION FLOW BETWEEN COORDINATOR AND ADDRESSED RON 149

49 FIGURE 47: RTPAR FRAME ELEMENT IN F-FB FRAMES IS USED FOR FRC CONFIGURATION 150

50 FIGURE 48: LFRC TIMING 151

51 FIGURE 49: MULTICHANNEL TRANSMISSION FOR ROUTED COMMUNICATION 153

52 FIGURE 50: TIQBC(1,4) COMPRESSION 154

1 **18. TABLE OF CONTENTS**

2

1.	Document.....	3	4.4.2.	Discovery of routing devices topology	17
1.1.	history and revisions	3	4.5.	Network communication.....	17
1.2.	Authors and Chapters supervisors	3	4.5.1.	Data and system communication	18
1.3.	Scope.....	3	4.5.2.	Communication security.....	18
1.4.	Purpose	3	4.6.	Addressing.....	18
1.5.	Design Architecture.....	3	4.7.	IQMESH® ROUTING protocol	18
1.6.	Acronyms.....	5	4.8.	FRC® data aggregation protocol	18
2.	General requirements and conventions.....	8	4.9.	IQRF DPA protocol	19
2.1.	PHY layer requirements.....	8	4.10.	IQRF security	19
2.1.1.	Regional requirements.....	8	5.	Application layer	20
2.1.2.	Data rates.....	8	5.1.	DPA communication services sublayer.....	20
2.1.3.	Modulation	8	5.1.1.	ALDPACS-DPA.request.....	20
2.1.4.	Timing.....	8	5.1.2.	ALDPACS-DPA.confirm.....	22
2.2.	Data link layer requirements	8	5.1.3.	ALDPACS-DATA.indication	23
2.2.1.	Multi-channel transmission	8	5.2.	Application layer common part services	24
2.3.	Network layer requirements.....	8	5.2.1.	ALCPS-SET.request	24
2.4.	Security	8	5.2.2.	ALCPS-SET.confirm	25
2.5.	Timings.....	9	5.2.3.	ALCPS-GET.request	25
3.	Conventions	10	5.2.4.	ALCPS-GET.confirm	26
3.1.	Flow diagrams.....	10	5.2.5.	ALCPS-RESET.request	26
3.2.	Data structures and elements.....	10	5.2.6.	ALCPS-RESET.confirm.....	27
3.2.1.	System Setup and Configuration (SSC)	11	5.2.7.	ALCPS-DATA.request.....	27
3.3.	IQRF Terminology and definitions.....	11	5.2.8.	ALCPS-DATA.confirm	30
3.4.	numbers and values	13	5.2.9.	ALCPS-DATA.indication.....	30
3.5.	Frames and transmission.....	13	5.3.	Application layer management services sublayer	32
3.6.	Data blocks in frames.....	13	5.3.1.	ALMS-DATA.indication.....	32
3.7.	Reserved fields and values.....	13	5.4.	Application layer management services (coordinator)	33
3.8.	Concept of primitives	14	5.4.1.	ALCMS-ASSOCIATE.request	33
3.8.1.	Processing of primitive requests.....	14	5.4.2.	ALCMS-ASSOCIATE.confirm.....	34
3.8.2.	Parameters of primitives	15	5.4.3.	ALCMS-DISASSOCIATE.request	35
4.	IQRF brief overview.....	16	5.4.4.	ALCMS-DISASSOCIATE.confirm	35
4.1.	General wireless mesh networks	16	5.4.5.	ALCMS-DISCOVER.request	36
4.2.	IQRF mesh network.....	16	5.4.6.	ALCMS-DISCOVER.confirm	37
4.3.	Network devices	17	5.4.7.	ALCMS-FRC.request	37
4.3.1.	Coordinator.....	17	5.4.8.	ALCMS-FRC.confirm	38
4.3.2.	Node.....	17	5.4.9.	NLMS-NSSCSET.request.....	39
4.4.	Creating the network	17	5.4.10.	NLMS-NSSCSET.confirm.....	39
4.4.1.	Association of joining devices	17	5.5.	Application layer management services (node)	41
			5.5.1.	ALNMS-JOIN.request	41
			5.5.2.	ALNMS-JOIN.confirm	42
			5.5.3.	ALNMS-LEAVE.request.....	42
			5.5.4.	ALNMS-LEAVE.confirm	43

5.5.5.	ALNMS-REFRC.request.....	43	7.4.6.	FRC frame collection (F-FC)	81
5.5.6.	ALNMS-REFRC.confirm.....	44	7.4.7.	DISASSOCIATE frame (F-DIS)	82
5.5.7.	ALNMS-LFRC.request	45	7.5.	Data link layer SSC	83
5.5.8.	ALNMS-LFRC.confirm	46	8.	PHY layer.....	85
5.6.	Application layer SSC.....	47	8.1.	Physical layer common part services (PLCPS)	85
6.	Network layer.....	50	8.1.1.	PLCPS-SET.request	85
6.1.	Network layer common part Services (NLCPS).....	50	8.1.2.	PLCPS-SET.confirm	86
6.1.1.	NLCPS-SET.request	50	8.1.3.	PLCPS-GET.request.....	87
6.1.2.	NLCPS-SET.confirm.....	51	8.1.4.	PLCPS-GET.confirm	87
6.1.3.	NLCPS-GET.request	52	8.1.5.	PLCPS-RESET.request	88
6.1.4.	NLCPS-GET.confirm	52	8.1.6.	PLCPS-RESET.confirm.....	88
6.1.5.	NLCPS-RESET.request.....	53	8.1.7.	PLCPS-DATA.request	89
6.1.6.	NLCPS-RESET.confirm.....	53	8.1.8.	PLCPS-DATA.confirm.....	90
6.1.7.	NLCPS-DATA.request.....	54	8.1.9.	PLCPS-DATA.indication	90
6.1.8.	NLCPS-DATA.confirm	55	8.1.10.	PLCPS-DATA.indication	91
6.1.9.	NLCPS-DATA.indication.....	56	8.1.11.	PLCPS-INFO.indication	91
6.2.	Network layer management services (NLMS)	57	8.2.	Bitstream and its transmission	93
6.3.	Network layer SSC.....	58	8.3.	PHY layer SSC.....	94
7.	Data link layer	62	9.	Security services layer	98
7.1.	Data link common part services.....	62	9.1.	Security services	98
7.1.1.	DLCPS-SET.request	62	9.1.1.	SES-SET.request.....	99
7.1.2.	DLCPS-SET.confirm	63	9.1.2.	SES-SET.confirm	99
7.1.3.	DLCPS-GET.request	64	9.1.3.	SES-GET.request	100
7.1.4.	DLCPS-GET.confirm	64	9.1.4.	SES-GET.confirm.....	100
7.1.5.	DLCPS-RESET.request.....	65	9.1.5.	SES-RESET.request	101
7.1.6.	DLCPS-RESET.confirm.....	65	9.1.6.	SES-RESET.confirm	101
7.1.7.	DLCPS-DATA.request.....	66	9.1.7.	SES-ENCRYPT.request	102
7.1.8.	DLCPS-DATA.confirm.....	67	9.1.8.	SES-ENCRYPT.confirm	103
7.1.9.	DLCPS-DATA.indication.....	67	9.1.9.	SES-DECRYPT.request	103
7.2.	Data link layer management services sublayer	70	9.1.10.	SES-DECRYPT.confirm	104
7.2.1.	DLMS-ROUTE.request	70	9.1.11.	SES-ENCRYPTDL.request	105
7.2.2.	DLMS-ROUTE.confirm	71	9.1.12.	SES-ENCRYPTDL.confirm.....	105
7.3.	Frames.....	72	9.1.13.	SES-DECRYPTDL.request	106
7.3.1.	Frame control elements.....	72	9.1.14.	SES-DECRYPTDL.confirm.....	106
7.3.2.	Standard non-network frame (SNNF)	74	9.2.	SES layer SSC.....	108
7.3.3.	Standard network frame (SNF).....	74	10.	Security specification	110
7.3.4.	Standard network frame for routing (SNFR)	75	10.1.	Security concept	110
7.3.5.	Fixed network frame.....	76	10.2.	Integrity.....	110
7.4.	Specific frames.....	77	10.2.1.	Time Quanta Bit coding method (TIQBC)	110
7.4.1.	JOIN-REQUEST frame (F-JR)	77	10.2.2.	Frame Integrity Tag for SNNF	110
7.4.2.	ACTIVE ASSOCIATION frame (F-ASA)	78	10.2.3.	Routing Integrity Tag (RIT).....	112
7.4.3.	PASSIVE ASSOCIATION frame (F-ASP)	79	10.3.	Authentication.....	112
7.4.4.	FRC frame broadcast (F-FB)	80	10.3.1.	Frame Integrity Tag.....	112
7.4.5.	FRC frame singles (F-FS)	81	10.4.	Encryption, DECRYPTION.....	116

10.4.1.	Data link layer encryption.....	116	11.5.10.	FRC special setups and recommended use cases.....	148
10.4.2.	Data link layer decryption.....	117	11.6.	Local FRC (LFRC).....	149
10.4.3.	Application layer encryption.....	117	11.6.1.	LFRC configuration parameters.....	149
10.4.4.	Application layer decryption.....	119	11.6.2.	Supported data collection modes.....	150
10.5.	Keys management.....	120	11.6.3.	Supported addressing modes.....	150
10.5.1.	Keys overview.....	120	11.6.4.	LFRC timing.....	151
10.6.	Keys derivations.....	121	11.6.5.	Virtual mode.....	151
10.6.1.	Network Communication Key (NCK).....	121	11.6.6.	LFRC and DLEN specification.....	152
10.6.2.	Beaming Communication Key (BCK).....	122	11.6.7.	Processing of incoming data during the LFRC-SINGLE phase	152
10.6.3.	Data Link Key (DLK).....	123	11.7.	Multichannel transmissions.....	153
10.7.	Replay protection.....	124	11.8.	Time quanta bit coding (TIOBC).....	154
10.7.1.	Non-networking frames (SNNF).....	124	11.8.1.	TIOBC coding schemes used in TISS.....	154
10.7.2.	Networking frames.....	124	12.	Device Classes specifications.....	156
11.	Functional DESCRIPTION.....	128	12.1.	Coordinator (C).....	156
11.1.	Association of new devices to the network.....	128	12.2.	Router (ROR).....	156
11.1.1.	Association based on the request to join (active).....	128	12.3.	Aggregating router (RORA).....	156
11.1.2.	Passive association of the nodes.....	129	12.4.	Beaming device (BED).....	156
11.2.	Addressing.....	131	13.	Network roles.....	157
11.2.1.	Supported addressing modes.....	131	13.1.	Coordinator.....	157
11.2.2.	Broadcast.....	132	13.2.	Node.....	157
11.2.3.	Unicast.....	132	13.2.1.	routing node (RON).....	157
11.2.4.	Multicast (FRC protocol only, FRCF = 1).....	133	13.2.2.	routing node with the aggregation (RONA).....	157
11.2.5.	Selectivecast (FRC protocol only, FRCF = 1).....	133	13.2.3.	Non-routing node (NRN).....	157
11.2.6.	Multicast (LFRC protocol only, FRCF = 1).....	133	13.2.4.	Beaming node (BEN).....	157
11.2.7.	Dedicated addressing space.....	134	14.	Devices working modes.....	158
11.3.	Discovery.....	135	14.1.	Online mode (RXMO).....	158
11.3.1.	PPS_FRC_DISCO.....	136	14.1.1.	XLPRX mode.....	158
11.3.2.	FTXE_FRC_DISCO.....	136	14.1.2.	LPRX mode.....	158
11.3.3.	PPS_DATA_SETVRN.....	136	14.1.3.	STDRX mode.....	158
11.4.	Routing.....	138	14.1.4.	JOIN mode.....	158
11.4.1.	Timing and synchronization between devices.....	138	14.1.5.	SYS mode.....	158
11.4.2.	Frame elements behavior during routing.....	140	14.2.	Offline mode (OFMO).....	158
11.4.3.	Timeslot length definition.....	140	14.2.1.	SLEEP mode.....	158
11.5.	FRC.....	142	14.2.2.	Beaming mode.....	158
11.5.1.	FRC configuration parameters.....	142	14.3.	Transmitting mode (TXMO).....	158
11.5.2.	Supported data collection modes.....	143	14.3.1.	XLPTX mode.....	159
11.5.3.	Supported addressing modes.....	143	14.3.2.	LPTX mode.....	159
11.5.4.	Processing delay.....	143	14.3.3.	STDTX mode.....	159
11.5.5.	FRC timing.....	143	15.	Constants.....	160
11.5.6.	Virtual mode.....	144	16.	Primitive parameters setup.....	162
11.5.7.	FRC and DLEN specification.....	145	16.1.	ALCPS-DATA.request.....	162
11.5.8.	Processing of incoming data during the FRC-SINGLE phase	145	16.1.1.	General data structure.....	162
11.5.9.	Processing of incoming data during the FRC-COLLECT phase	146	16.1.2.	PPS_DATA_FRC.....	162

16.1.3.	PPS_DATA_REFRC.....	162	19.1.	EU	170
16.1.4.	PPS_DATA_LFRC	163	19.2.	USA	171
16.1.5.	PPS_DATA_SETVRN	163	19.3.	Israel	172
16.2.	ALCMS-FRC.request.....	164	20.	Annex B - IQRF networks profiles	173
16.2.1.	PPS_FRC_DISCO	164	21.	Annex C - Requests.....	174
17.	List of figures.....	165			
18.	Table of contents.....	166			
19.	Annex A - Region related PHY setup (RRPS)	170			