IQRF OS 4.0, security and some news

Vladimír Šulc, Ph.D.
MICRORISC s.r.o., CEO
Jičín, Czech Republic

IQRF® Alliance meeting
October 19, 2016, Warsaw

MICRORISC s.r.o.

MICRORISC

CZECH

TECHNOLOGICAL

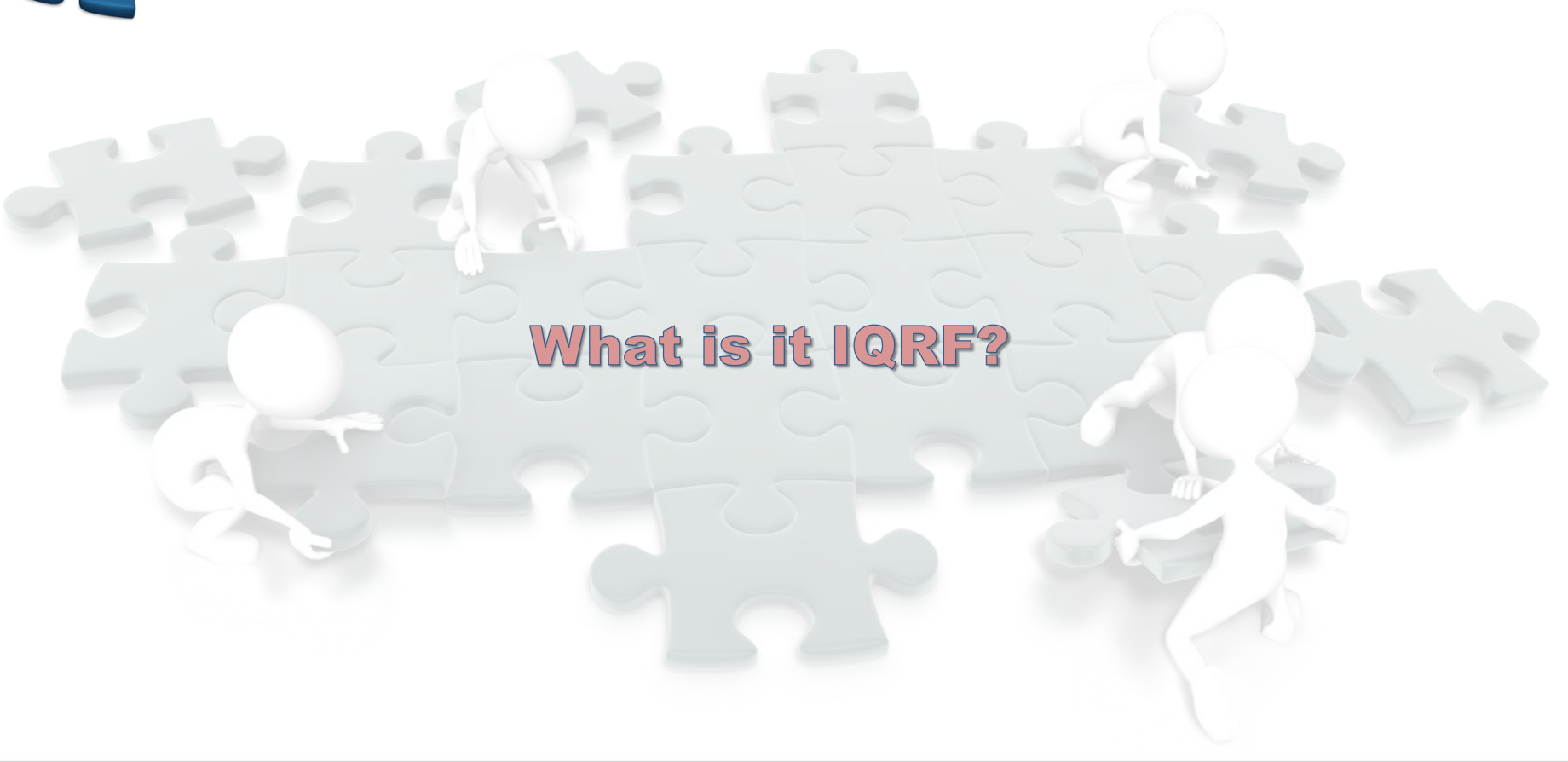
WITH CLEAR VISIONS

ORIENTED TO MANUFACTURES

INNOVATIVE

GLOBAL

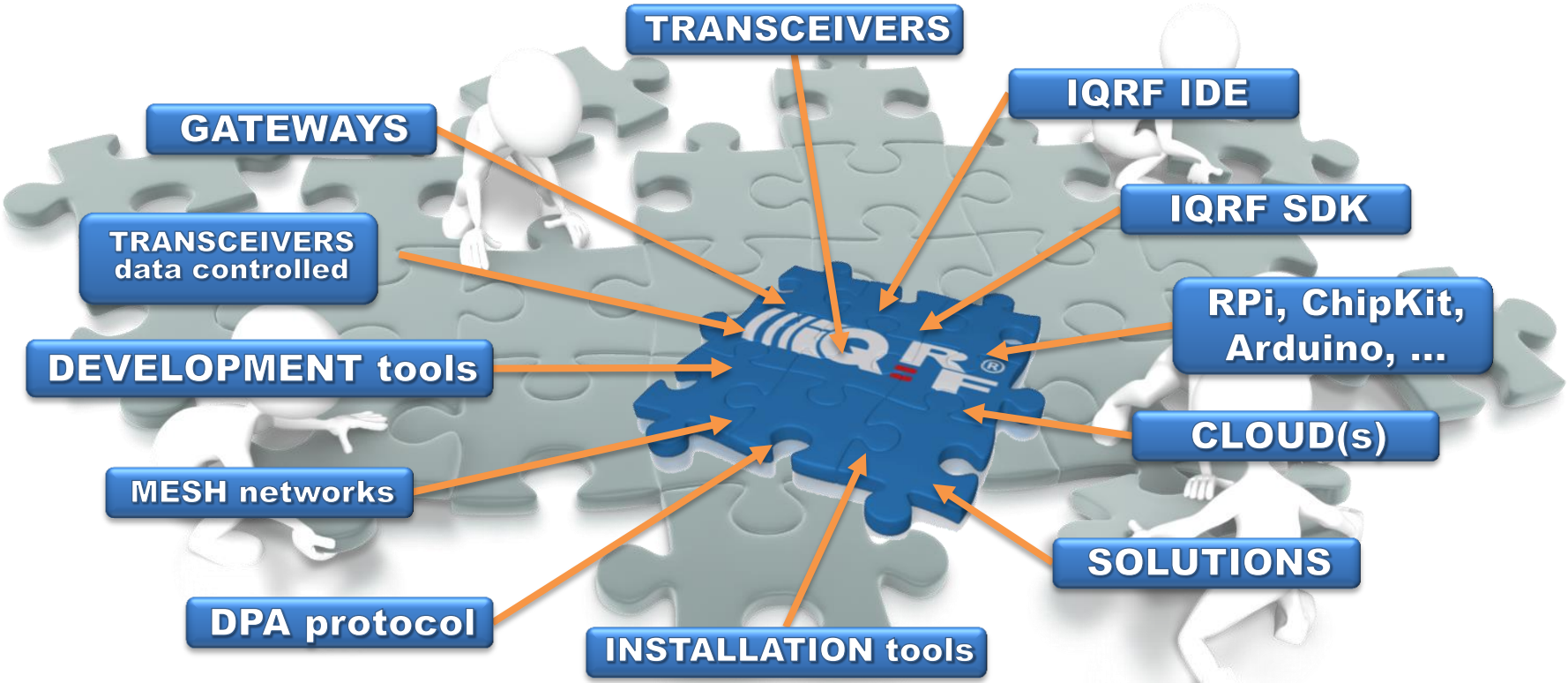
... ENABLING FUTURE INNOVATION®



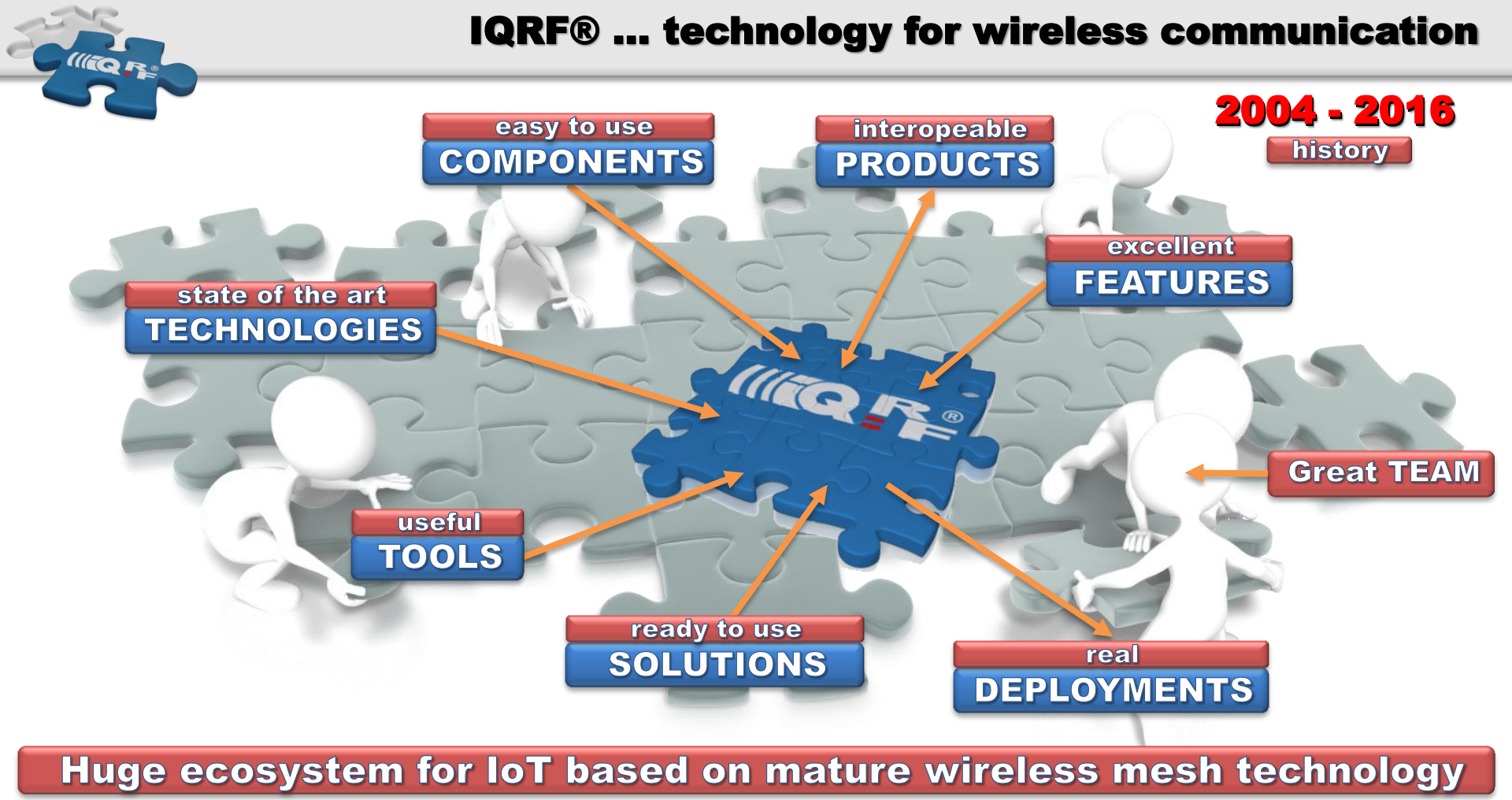
What is it IQRF?

IQRF® ... technology for wireless communication

2004 - 2016



IQRF® ... technology for wireless communication



Huge ecosystem for IoT based on mature wireless mesh technology

IQRF OS 4.00

IQRF OS 4.00

Complex security features

New bonding mechanism

System stability and performance

Deep system optimizations

Redesigned packets structure

Seamless migration

It is even easier to use

Higher performance and stability

New tools for system monitoring

Deep Sleep mode with consumption 35 nA

Security based on industrial standards (AES-128)

IQRF OS 4.00 security

Why we need more security?

It is wireless. *Everybody* can listen our data or fake packets!

No physical protection.

Security concept should consider more threats.

Security in previous versions of IQRF OS

Consistency protection

Automatic encryption of network communication

Networks communication isolation

Bonding security dependent on an application layer

COMPLEXITY

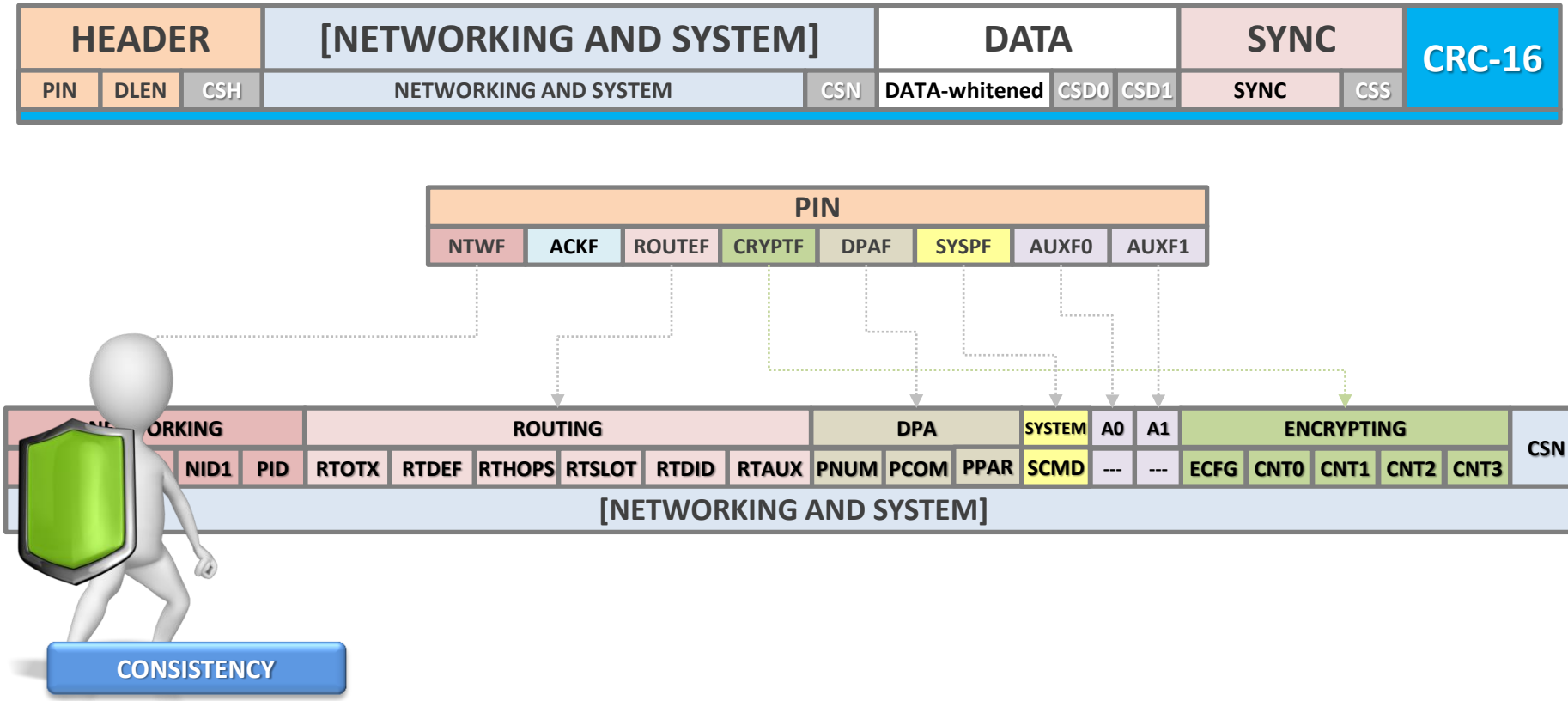
ADEQUACY

SIMPLICITY

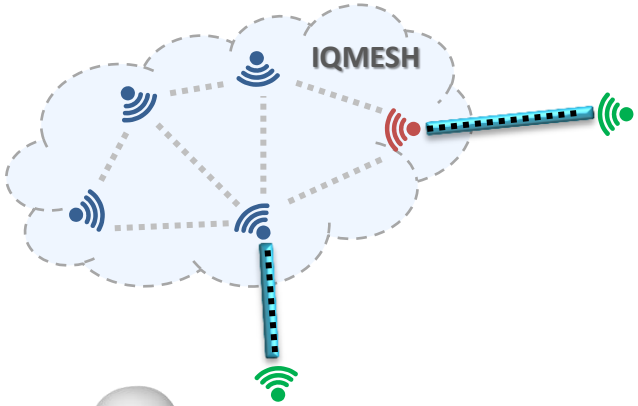
UNDERSTANDABILITY

PREDICTABILITY

Security starts at consistency protection



Protection of communication during network pairing



BONDING PROTECTION

WHY?

Bonding is a process during which devices exchange sensitive information (e.g. network passsword, addresses, …)

HOW?

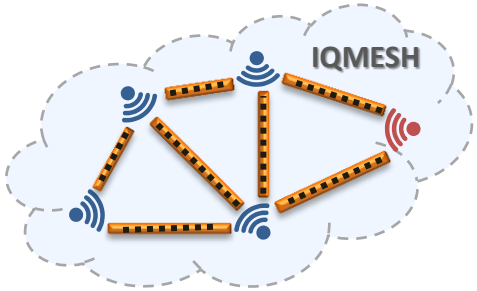
Bonding password (128 b)

Its knowledge entitles new device to join the network

Bonding keys + AES 128 b → **ENCRYPTION** → **BONDING DATA**

Packets consistency check

Automatic protection of network communication



WHY?

Network communication is continous process during which some sensitive data or commands may be transmitted.

HOW?

Network password (192 b)

Its knowledge entitles devices to decrypt and process packets

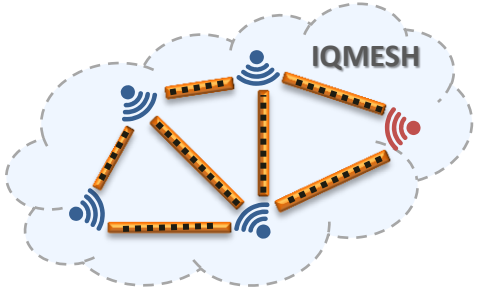
Network keys + AES 128 b → **ENCRYPTION** → **NETWORK PACKET**

+ Packets consistency check

+ Forged packets check / drop

+ Dynamic keys change

User's security layer to maximize data protection



WHY?

Users may use additional encryption shield for data. Thus, data not necessarily should be processed by the IQRF network.

HOW?

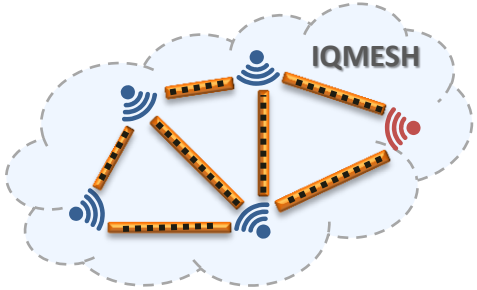
User's key (128 b)

Its knowledge entitles application to decrypt data

User's key + AES 128 b → **ENCRYPTION** → DATA

It enables data isolation from the IQRF platform.

Ready to fix potential problems in the future



WHY?

In the future, new vulnarabilities (e.g. in AES) may be found and running system should be patched.

HOW?

Application upgrade: SPIPGM, RFPGM, IQMESH OTA

HWP upgrade: SPIPGM, RFPGM, IQMESH OTA

Secure IQRF OS upgrade: SPIPGM, RFPGM, IQMESH OTA

Simplicity and understandability

encryptBufferRF(x)

decryptBufferRF(x)

setUserKey()

setBondingPassword()

WHY?

If security is not understandable or brings technical difficulties users will not usually use it.

HOW?

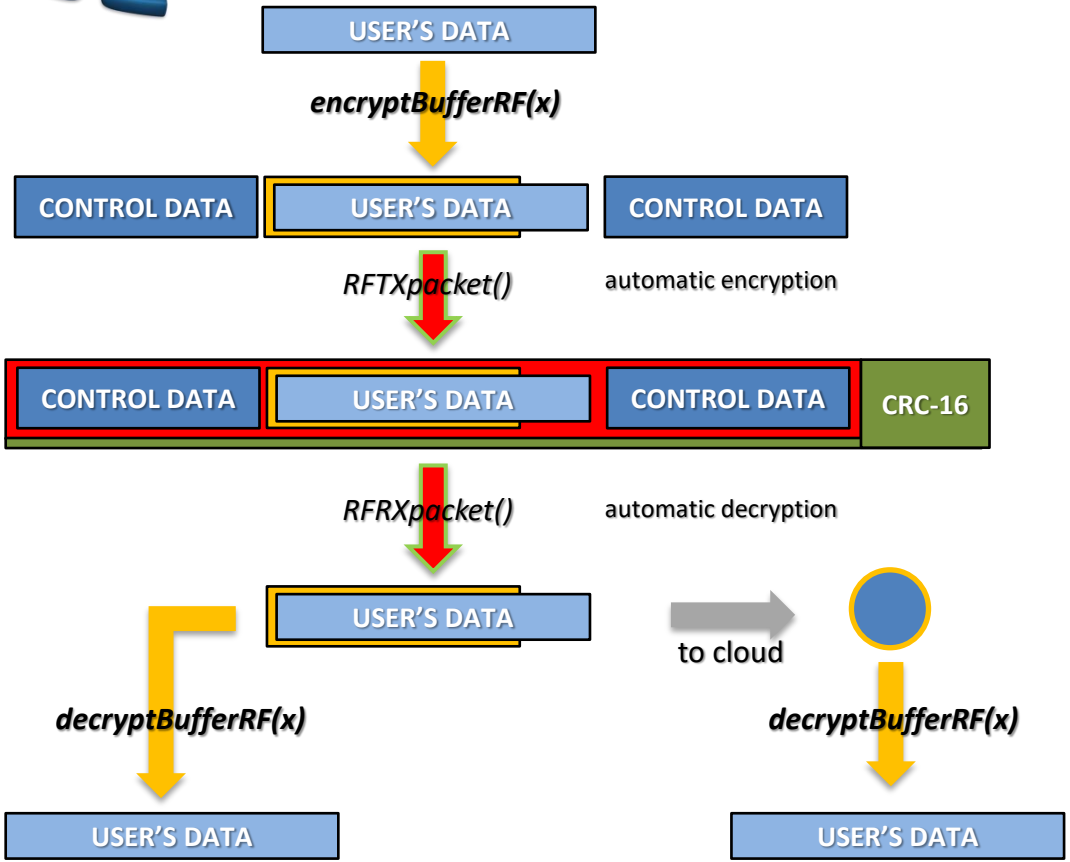
All discussed features related to network security are automatic.

Random Network password (192 b) is set during manufacturing.

Dynamic network keys exchange realized by the IQRF OS.

Easy to understand API.

Network communication - schematics



User's encryption AES 128 b CBC + user's key

network password 192 b

Network encryption AES 128 b + CDC + CP + network keys
Cipher Data Chaining + Consistency protection

network password 192 b

Network decryption AES 128 b + CDC + CP + network keys
Cipher Data Chaining + Consistency protection

User's decryption AES 128 b CBC + user's key

Security concept – features

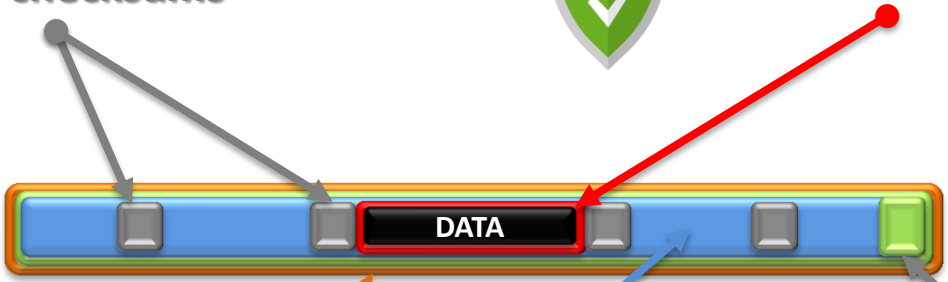
Keys + passwords management

SPIPGM
RFPGM
OTA

FUTURE PROTECTION

Block checksums

User's encryption shield



PACKET

CRC-16

Network encryption shield
Forged packets protection
Packet's consistency protection

Security concept – few security layers

Prevention is always better than elimination of the problem .