IQRF OS 4.0 Webinar

Šimon Chudoba
IQRF Alliance, CEO

January 23rd , 2017

OS 4.0 – other features

- Deep sleep for TR-76D modules – consumption < 100 nA
- Longer RF range of LP mode – the same like for STD mode
- Improved FRC
  - 1B FRC downloads data from 63 Nodes
  - 2B FRC downloads data from 31 Nodes
- Device cloning canceled – access password used
- DPA demo canceled, Coordinator/Node as a one device canceled
- IQMESH examples removed from Startup Package – The only way for IQMESH is DPA.
- Basic IQRF header file template-basic.h renamed to IQRF.h
- OS 4.00D is not interoperable with OS 3.08D
- User OS upgrade to version 4.00D is possible, downgrade back to OS 3.08D is not possible
- IQRF IDE 4.40 and DPA 3.00 required

Security layers

Three different protections based on AES-128:

- Access encryption
  - Bonding
  - CATS services
  - Network backup and restore
- Networking encryption
- User encryption

Passwords and keys

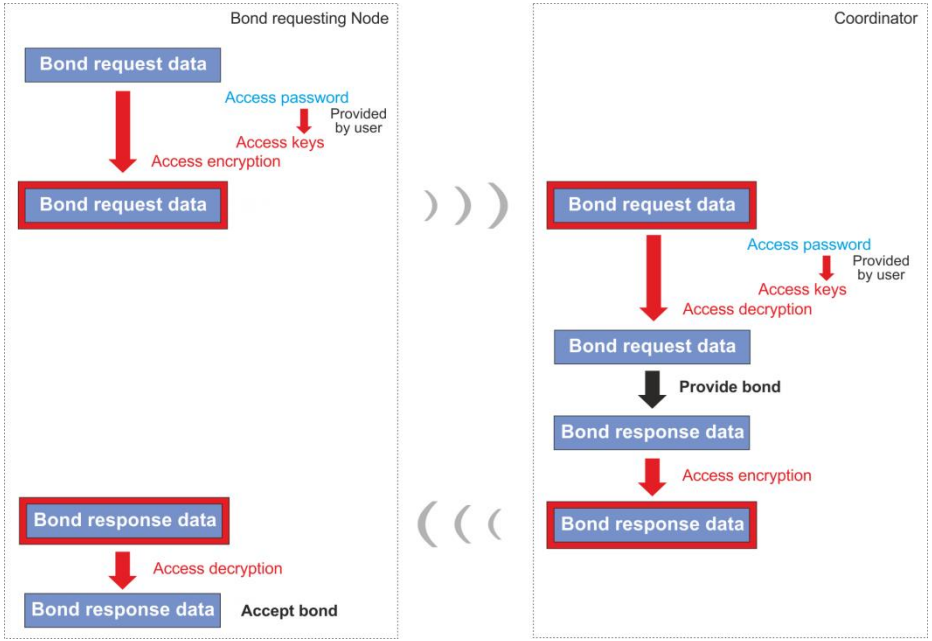
- Compromising of keys - security problems.
  - IQRF OS minimizes manipulation with network and access keys.
  - Keys are generated from respective passwords.
- Network password
  - generated randomly with high entropy
  - delivered encrypted to devices

Passwords and keys

Advantages

- User takes care about the passwords, not about keys.
- The keys are modified by embedded hash functions.
- No simple direct relationship between passwords and keys increases the security.
- The keys are generated dynamically, varying in time.
- The relationship between passwords and keys are different in different networks.
- Breaking the keys in one network has no impact on other networks

Access Encryption



- Access encryption
  - Bonding
  - CATS services
  - Network backup and restore
- Data exchanged during bonding are encrypted!
- AES-128 with 16 B key and standard CBC mode
- Access Password can be set by:
  - TR Configuration
  - new OS function: setAccessPassword()

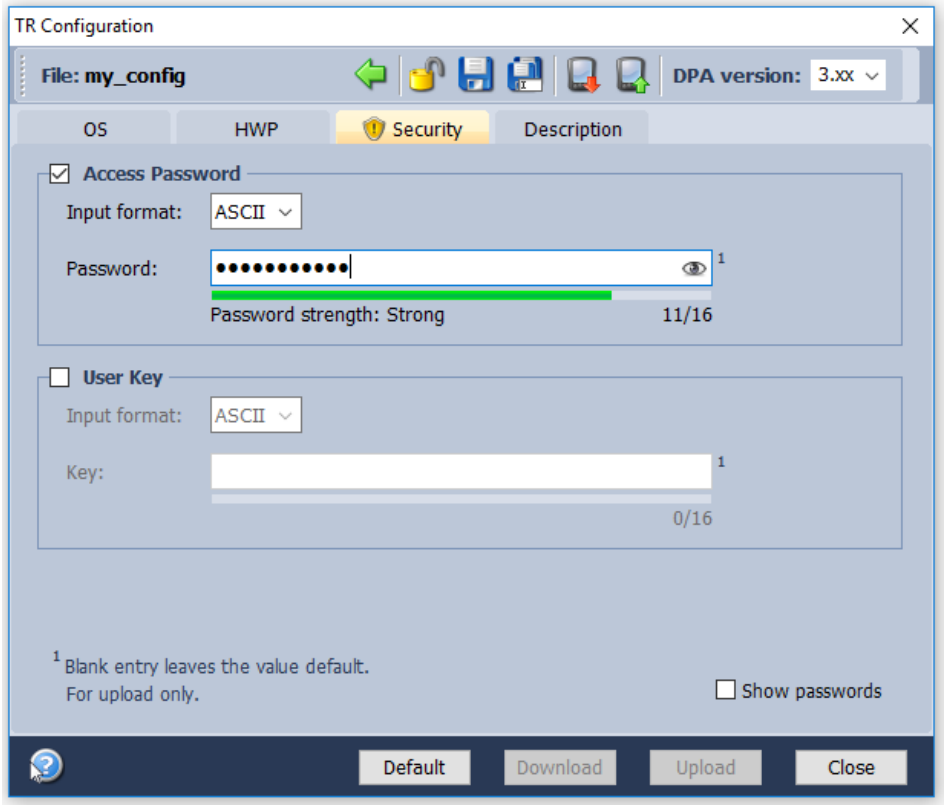
Networking encryption

- IQRF networks – encryption done by OS.
- Only systems with valid Network password are allowed.
- AES-128 with 16 B long keys + proprietary CDC algorithm.

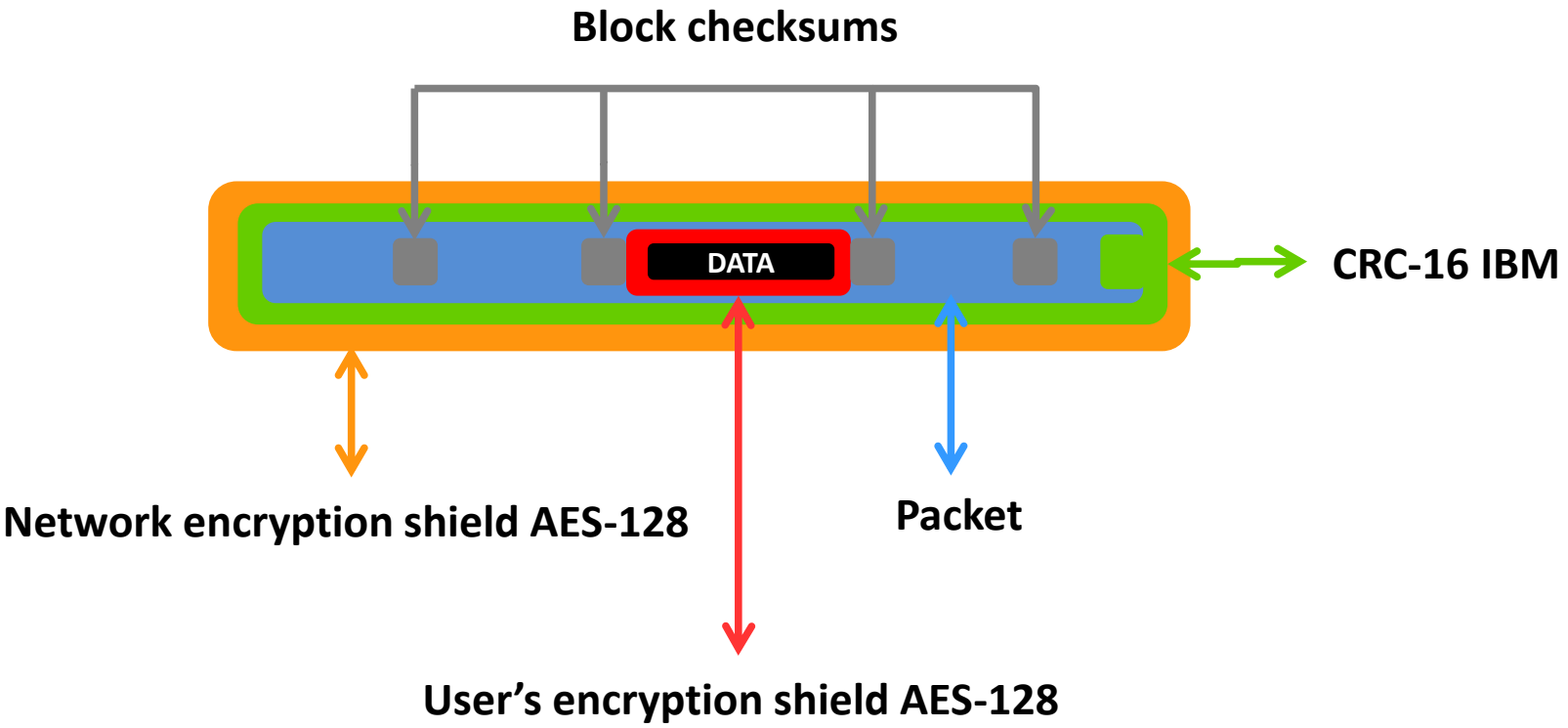
- Every TR has a unique random 192 b password
- 128b network key derived from the coordinator 192 b password
- The network password is passed to Nodes encrypted by Access encryption
- User - no care about the Networking encryption and password distribution
- Integrity check.

User encryption

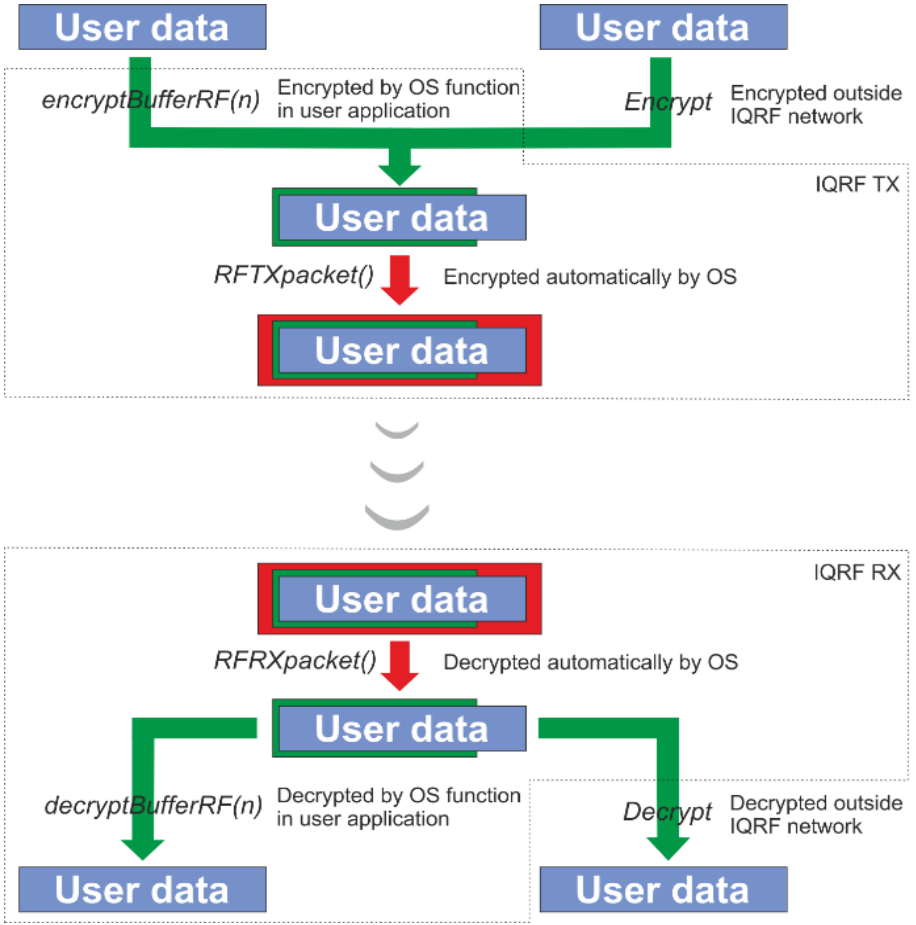
- Optional encryption of payload data (either networking or non-networking)
- Fully under user's control
- User key specified by the user
- Only cipher texts are transferred – information content not readable without user key
- User encryption/decryption can be performed outside TR.
- New OS functions:
  - setUserKey()
  - encryptBufferRF(blocks)
  - decryptBufferRF(blocks)



User encryption



Security



User encryption – User key
Provided by user

Network password 192 b
Provided by factory (for Coordinator)
Delivered encrypted during bonding (for Node)
Network keys

Network encryption

Network password 192 b
Provided by factory (for Coordinator)
Delivered encrypted during bonding (for Node)
Network keys

Network decryption

User decryption – User key
Provided by user

Summary

Access Encryption

- Access Password 128b - set by TR configuration or by setAccessPassword function in the C code
  - bonding
  - device restore - Coordinator/Node exchange in the network
  - DPA Service Mode authorization

Networking Encryption

- automatic encryption of networking packets by AES-128 with 16 B long keys and additional proprietary CDC (Cipher Data chaining) algorithm
- Every IQRF transceiver is equipped with a 192 b long unique fully random password individually generated at the factory. The 128 b networking keys are derived from the password of the Coordinator.

User Encryption

- possibility of user encrypting by AES-128 (set by TR configuration or by setUserKey function in the C code)
- new OS functions: encryptBufferRF and decryptBufferRF

www.iqrf.org/summit2017

IQRF Summit 2017

Prague, June 7th – 8th 2017

300 participants

30+ speakers

10+ workshops

Market Place

MICRORISC

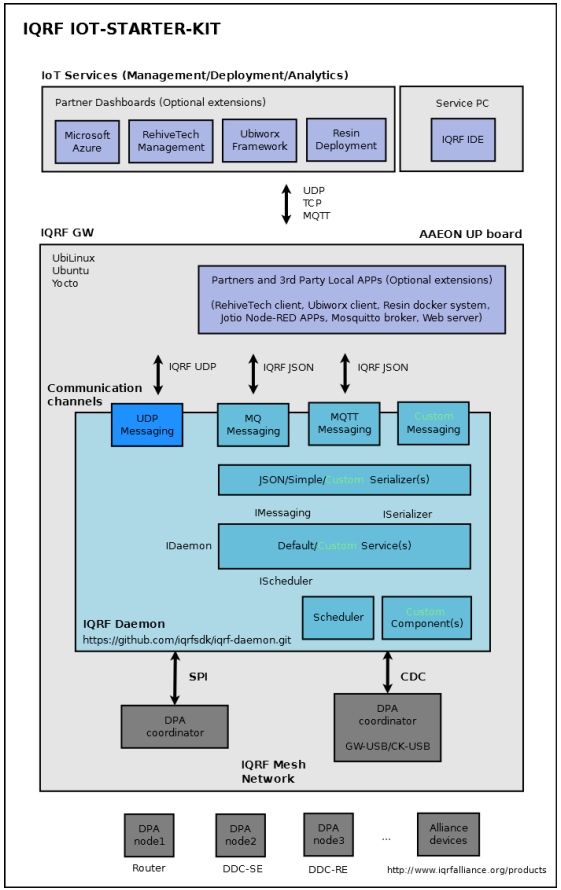
Microsoft

AAEON an ASUS assoc. co.

O2

IoT Starter Kit

https://github.com/iqrfsdk/iot-starter-kit



Useful links

- Start-up package
- OS 4.0 Security white paper
- IQRF SDK (github)
- New videos:
  - How to upgrade IQRF OS
  - How to make a network with IQRF OS 4.0
  - Custom DPA Handlers for IoT Starter Kit
- Standard websites:
  - www.iqrf.org
  - www.iqrfalliance.org
  - IQRF Summit 2017

Demonstration

- OS upgrade
- Configuration: Access Password (+ User Key)
- Bonding with Access Password
- Back up & Restore with Access Password
- IoT Starter Kit macros
- CATS
  - Scanner
  - OTA Connectivity with Access Password
  - OTA Restore


Thank you