SECURITY 2017

25. ročník konference o bezpečnosti v ICT

IQRF – reliable wireless mesh network for IoT

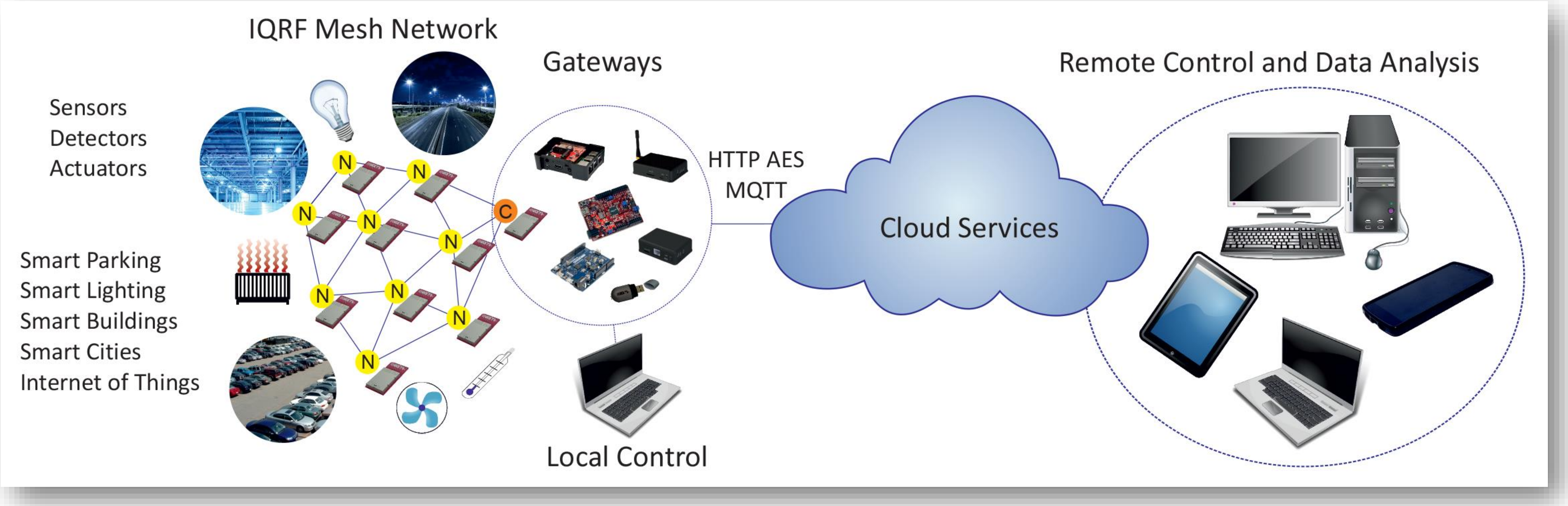
Mgr. Ivona Spurná

MICRORISC

IQRF technology

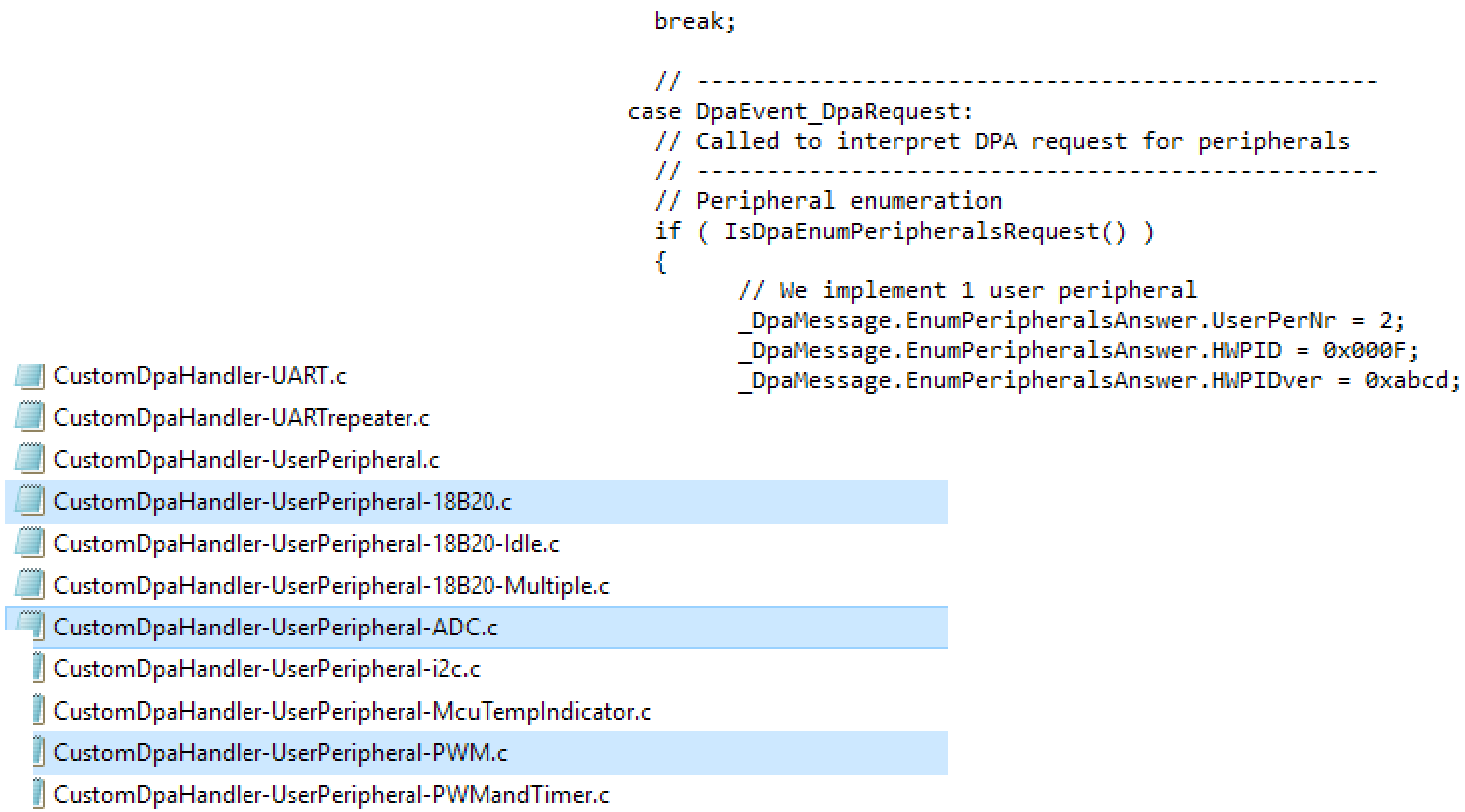
- Low power, low speed and low data volume wireless connectivity
- Transceivers with built-in operating system
- MICRORISC – IQRF development, manufacturing since 2004
- Frequency band: 868/916/433 MHz
- Topology: MESH (max. 240 hops) – reliable data transfer
- Routing method: synchronized directed flooding
- Range: tens of metres in buildings, hundreds metres in an open space (500 m)
- Low current consumption (<100 nA – 19 mA)
- The transmission speed suitable for controlling and data collecting (~19 kb/s)
- Transmission length: max 30 – 50 ms / packet
- Packet-oriented communication (max. 64 user bytes / RF packet).
- FRC – Fast Response Command – fast messaging
- No licence fees

IQRF Topology



3-layered design of IQRF

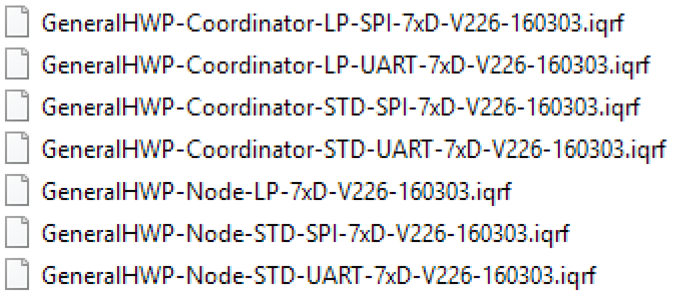
- Custom DPA Handler
- Hardware profile
- Operating system



```
  break;

  // -------------------------------------------------
case DpaEvent_DpaRequest:
  // Called to interpret DPA request for peripherals
  // -------------------------------------------------
  // Peripheral enumeration
  if ( IsDpaEnumPeripheralsRequest() )
  {
        // We implement 1 user peripheral
        _DpaMessage.EnumPeripheralsAnswer.UserPerNr = 2;
        _DpaMessage.EnumPeripheralsAnswer.HWPID = 0x000F;
        _DpaMessage.EnumPeripheralsAnswer.HWPIDver = 0xabcd;
```

```
CustomDpaHandler-UART.c
CustomDpaHandler-UARTrepeater.c
CustomDpaHandler-UserPeripheral.c
CustomDpaHandler-UserPeripheral-18B20.c
CustomDpaHandler-UserPeripheral-18B20-Idle.c
CustomDpaHandler-UserPeripheral-18B20-Multiple.c
CustomDpaHandler-UserPeripheral-ADC.c
CustomDpaHandler-UserPeripheral-i2c.c
CustomDpaHandler-UserPeripheral-McuTempIndicator.c
CustomDpaHandler-UserPeripheral-PWM.c
CustomDpaHandler-UserPeripheral-PWMandTimer.c
```

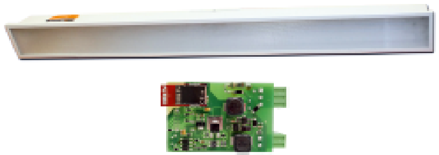


```
GeneralHWP-Coordinator-LP-SPI-7xD-V226-160303.iqrf
GeneralHWP-Coordinator-LP-UART-7xD-V226-160303.iqrf
GeneralHWP-Coordinator-STD-SPI-7xD-V226-160303.iqrf
GeneralHWP-Coordinator-STD-UART-7xD-V226-160303.iqrf
GeneralHWP-Node-LP-7xD-V226-160303.iqrf
GeneralHWP-Node-STD-SPI-7xD-V226-160303.iqrf
GeneralHWP-Node-STD-UART-7xD-V226-160303.iqrf
```

Communication with DPA protocol

- Direct Peripheral Access (DPA) is a simple byte oriented protocol used to control services and peripherals of IQMESH network devices by SPI or UART interfaces.

DATmoLUX
Indoor lighting



TECO
Switch

Status
Light: ON
Intensity: 5

DPA Message

NADR	PNUM	PCMD	HWPID	PData
0400	20	03	1106	

Request: switch (

PROTRONIX
CO_2, temperature and relative humidity sensor

Status
CO_2: 443 ppm
Temperature: 18,3 °C
Relative humidity: 43 %

DPA Message

NADR	PNUM	PCMD	HWPID	PData	
0100	0C	02	3201	0A 47 44 03	Request: sensor reading
0100	0C	82	3201	00 4A 01 B8 01 B0 00 B7 BF	Response: sensor reading

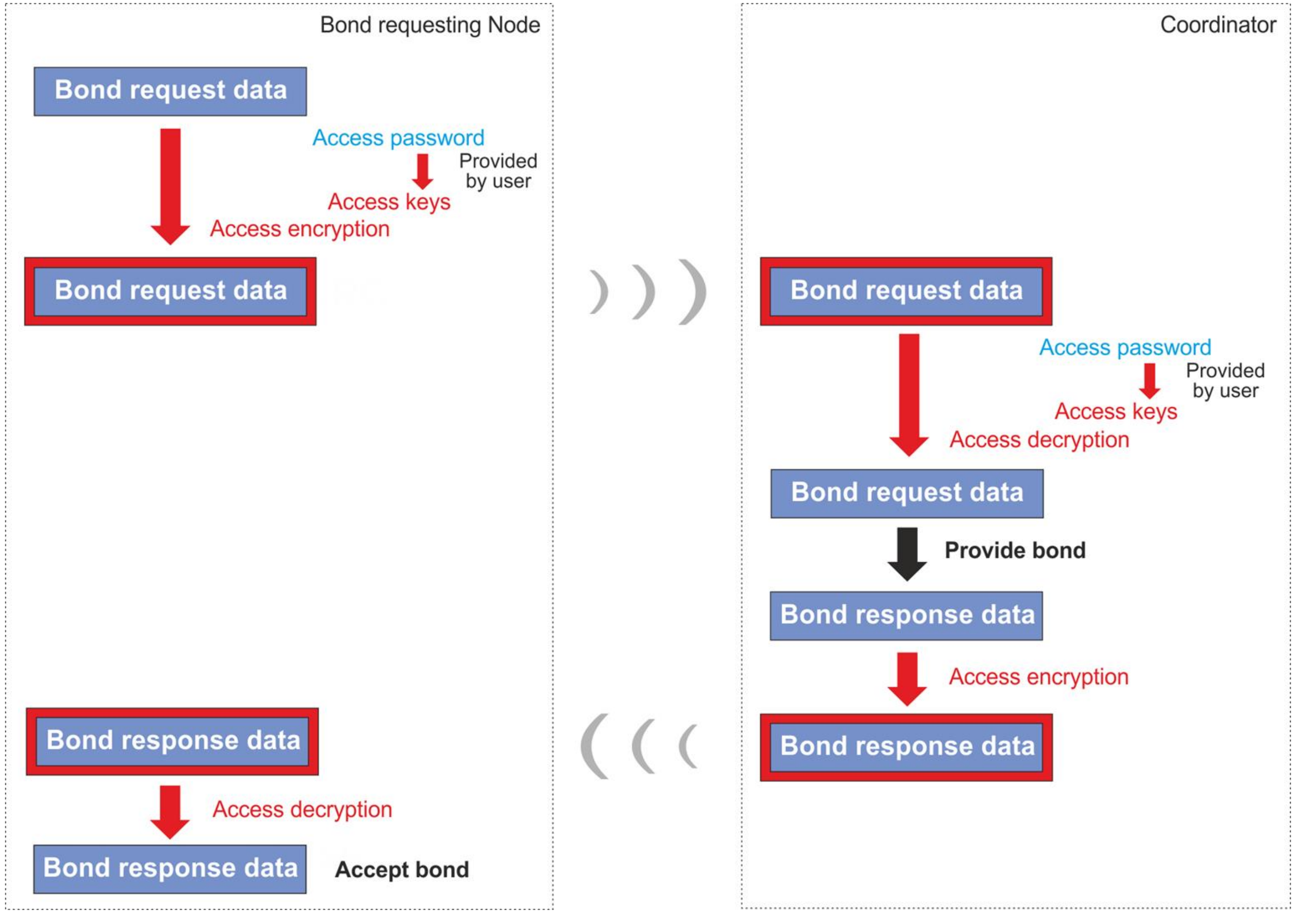
Security with IQRF

- OS 4.0 (release Q1 2017)
  - 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.
- Generated from respective passwords.
- Network password
  - randomly with high entropy
  - delivered encrypted to devices

Protection during bonding (simplified)



Keys vs. passwords

- 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.

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.

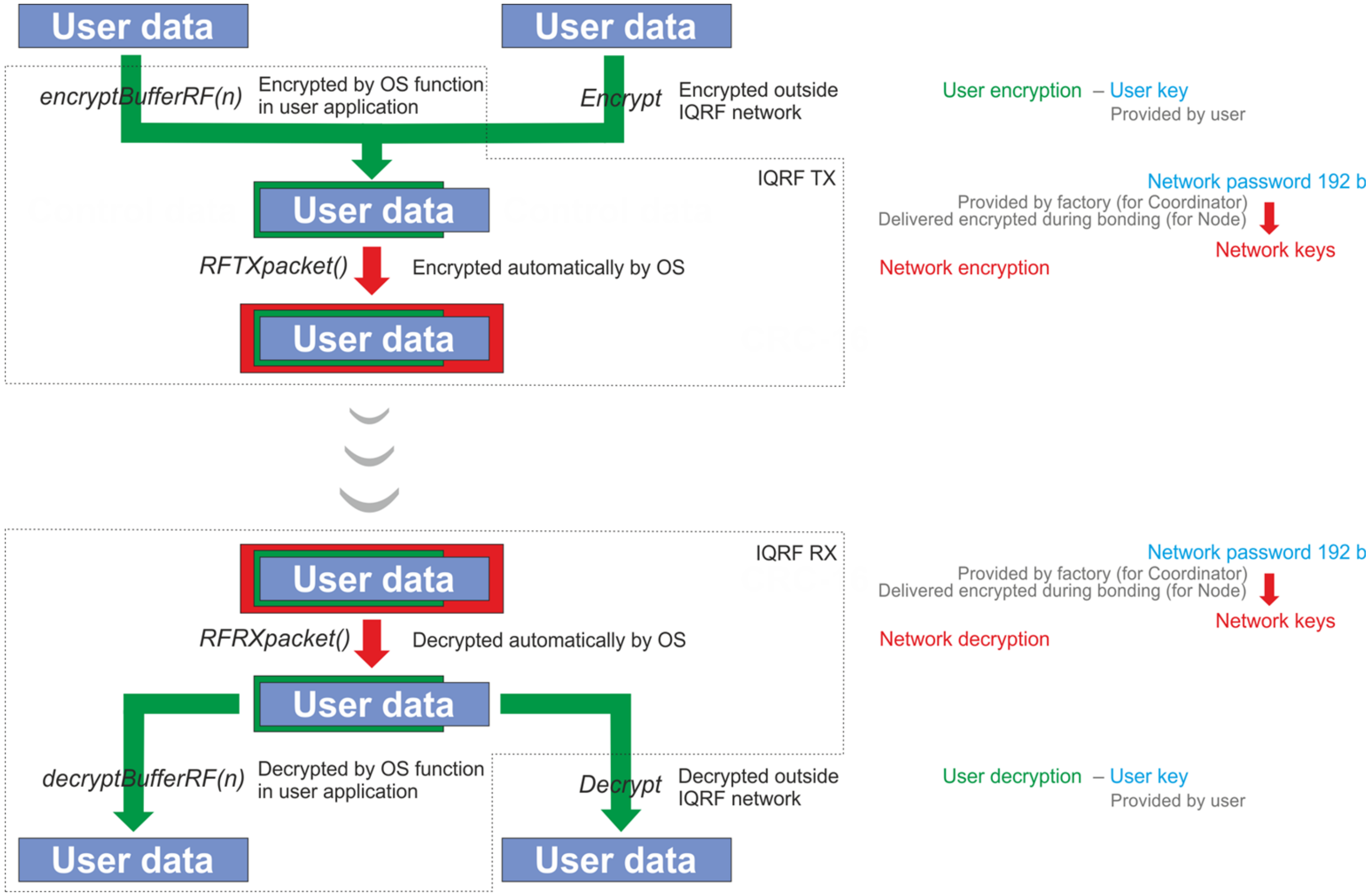
Networking encryption

- TR has a 192 b password.
- 128b network key derived from the coordinator password
- The password is passed to Nodes securely.
- User - no care about the Networking encryption + distribution.
- Integrity check.

User encryption

- Optional.
- Fully under user’s control.
- User key specified by the user.
- Only ciphertexts are transferred.
- User encryption/decryption can be performed outside TR.

Protection during networking communication



User data

User data

encryptBufferRF(n) Encrypted by OS function in user application

Encrypt Encrypted outside IQRF network

User encryption – User key
Provided by user

IQRF TX

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

User data

RFTXpacket() Encrypted automatically by OS

Network encryption

User data

IQRF RX

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

User data

RFRXpacket() Decrypted automatically by OS

Network decryption

User data

decryptBufferRF(n) Decrypted by OS function in user application

Decrypt Decrypted outside IQRF network

User decryption – User key
Provided by user

User data

User data

Děkuji za pozornost.

Mgr. Ivona Spurná
MICRORISC
ivona.spurna@microrisc.com