kamstrup

Kamstrup South Africa (Pty) Ltd.

Suite 9, Southdowns Ridge Office Park Nellmapius & John Vorster Drive Centurion 0157 South Africa

T: +27 87 357 8659 F: +27 12 342 7620 E: pvh@kamstrup.com

ref: v3

18 July 2019

Decrypting and decoding Sigfox meter data

This is an example for decrypting and decoding data from the Kamstrup MULTICAL 21 ultrasonic water meter with radio module 11, communicating via Sigfox network.

For reference, please see these documents:

- Datasheet: http://products.kamstrup.com/download.php?uid=515d4ab700278
- Technical Description: http://products.kamstrup.com/download.php?uid=515d4b410de78

The meter specific XML based key file and the Sigfox Data file can be downloaded from your MyKamstrup account https://www.kamstrup.com/en-en/my-kamstrup-login, see https://www.kamstrup.com/en-en/my-kamstrup-guides for help.

XML file for example meter:

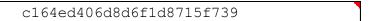
<?xml version="1.0" encoding="utf-8"?> <MetersInOrder orderid="" schemaVersion="2.0"> <Meter> <MeterNo>57722719</MeterNo> <SerialNo>57722719</SerialNo> <EncKeys> <DEK>C2E387277E39C9D821F3B05E1616F87C</DEK> </EncKeys> <MeterName>MC21</MeterName> <ConsumptionType>VolumeCold</ConsumptionType> <ConfigNo>0100200023133</ConfigNo> <ProgramNo> </ProgramNo> <TypeNo>02111C04894</TypeNo> <VendorId>KAM</VendorId> </Meter> </MetersInOrder>

Sigfox data file for example meter:

| Device | PAC | Meter Number |
|----------|------------------|--------------|
| 007D47BC | 1C2FEBF6D5837DAD | 57722719 |



Sigfox received message:



Structure of Sigfox message, showing fields, field lengths and content:

| PackID | AES Cnt | Encrypted Payload |
|------------|---------|----------------------|
| 1 | 1 | 10 |
| <u>c</u> 1 | 64 | ed406d8d6f1d8715f739 |

Message payload part (last 10 bytes) of the data is encrypted using AES-128 CTR. The input to decryption function is the **payload**, **DEK** (16 bytes key from XML file) and **IV** (constructed by repeating **AES Cnt** up to 16 bytes).

The following calculator can be used to verify decryption: www.cryptogrium.com/aes-ctr.html



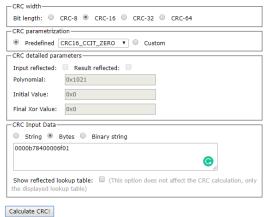
In this example, the encrypted payload is decrypted as

0000b78400006f010e93

Calculate and verify the **CRC** over the 8 data bytes of the **Decrypted Message**. The CRC-16 algorithm is CCIT_ZERO (0x1021) with start value 0x0000, no final XOR and no inversions.

| Decrypted Message | <u>CRC</u> |
|-------------------|------------|
| 8 | 2 |
| 0000b78400006f01 | 930e |

The following calculator is used as a check: www.sunshine2k.de/coding/javascript/crc/crc js.html



Result CRC value: 0x930E

kamstrup

PackID determines the structure and units of the message:

| PackID | | | | | | | | | | | |
|--------------------------|------------|---------|-----------------------------------|---------------------------|---|--------------------|---|--|--|--|--|
| | Bit | | | | | | | | | | |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | | | | |
| Decin | Units | | Log | PackageType | | ype | | | | | |
| 00b 01b 10b 11b | = 1 = 2 | 01b = f | m3 & L/hr t3 & GPM al & GPM | 0 = day 1 = hour | _ | 00b = 11b = | | | | | |

For this example, PackID is decoded as

| bin | |
|------|-----|
| | Dec |
| 8 | |
| hex | |
| text | |

| 11000001 | | | | | | | |
|----------|-------------|-----|-----|--|--|--|--|
| Decimals | PackageType | | | | | | |
| 2 | 2 | 1 | 3 | | | | |
| 03 | 00 | 0 | 001 | | | | |
| 3 | m3 & L/hr | Day | 1 | | | | |

From **PackID**, **PackageType** determines the content of the package:

| Package Content | | | | | | | | | | | |
|-----------------|---|--------|---------|-----------|----------|----------|---------------|--------------|-------------|--|-------|
| 0 | 0 | Packld | AES Cnt | InfoCode | ٧ | V1 | | Flow | CRC16 | | |
| U | 0 | - | 247 | 0061 | 14 | 146 0 | | 0 | 8f8f | | |
| 1 | 1 | Packld | AES Cnt | InfoCode | V1 | | V1 | | V1 Max Flow | | CRC16 |
| 1 | 1 | - | 247 | 0061 | 146 | | (| 0 | 8f8f | | |
| 2 | 2 | Packld | AES Cnt | InfoCode | ٧ | 1 | Min. water T. | Min. amb. T. | CRC16 | | |
| | 2 | - | 247 | 0061 | 14 | 146 | | 0 | 8f8f | | |
| 3 | 3 | Packld | AES Cnt | InfoCode | V1 | | Min. water T. | Max. amb. T. | CRC16 | | |
| 3 | 3 | - | 247 | 0061 | 146 | | 0 | 0 | 8f8f | | |
| 7 | 7 | Packld | AES Cnt | Infocodes | Min Flow | Max Flow | Min. amb. T. | Max. amb. T. | CRC16 | | |
| , | 7 | - | 247 | 0061 | 146 | 0 | 0 | 0 | 8f8f | | |

For this example, the content for **PackageType** = 1 is decoded as

| 0000b78400006f01 | | | | | | | |
|------------------|--------------------|-------|--|--|--|--|--|
| Info | V1 Max Flow | | | | | | |
| 2 | 4 2 | | | | | | |
| 0000 | 0000 000084b7 016f | | | | | | |
| | 33.975 | 0.367 | | | | | |

This shows that the total consumption volume, V1, on the meter is 33.975 m³, using the equation $Volume = V_1 \times 10^{-Decimals}$ [*Units*]

The maximum flow rate is 0.367 L/hr.

InfoCode identifies any active alarms and how long they have been active in the last 30 days. The LSB 4 bits indicate active alarms and represent DRY, REVERSE, LEAK and BURST. The hour counters are represented by the 12 MSB bits as 3 bits each.

| Burst | Leak | Reverse | Dry | Burst | Leak | Reverse | Dry |
|-------|------|---------|-----|-------|------|---------|-----|
| 3 | 3 | 3 | 3 | 1 | 1 | 1 | 1 |

kamstrup

The values for the hour counters are decoded as

| Interva | al Hours |
|---------|--------------------------------------|
| 0 | 0 hours |
| 1 | 1-8 hours |
| 2 | 9-24 hours = 1 day and night |
| 3 | 25-72 hours= 2-3 days and nights |
| 4 | 73-168 hours= 4-7 days and nights |
| 5 | 169-336 hours= 8-14 days and nights |
| 6 | 337-504 hours= 15-21 days and nights |
| 7 | > 505 hours= 22-31 days and nights |

For example InfoCode = 0x71 = 113 would decode to the following:

| | 00000001110001 | | | | | | | | |
|---------|---|---------|---|-------|-------|-------|------|--|--|
| Burst | Burst Leak Reverse Dry Burst Leak Reverse D | | | | | | | | |
| 3 | 3 | 3 | 3 | 1 | 1 | 1 | 1 | | |
| 000 | 000 | 000 | 111 | 0 | 0 | 0 | 1 | | |
| 0 hours | 0 hours | 0 hours | > 505 hours = 22-31 days and nights | FALSE | FALSE | FALSE | TRUE | | |

This shows that meter is dry now, and has been dry for more than 22 days in the last 30 days.

Yours sincerely,

Kamstrup South Africa (Pty) Ltd.

Marthinus Botha Technical Manager, South Africa Electricity

T: +27 87 357 8659

M: +27 82 826 1915 E: mjb@kamstrup.com