Radiocrafts
Embedded Wireless Solutions

Application Note AN013

Implementing ZigBee Smart Energy (SE) Devices with RC2400-ZNM

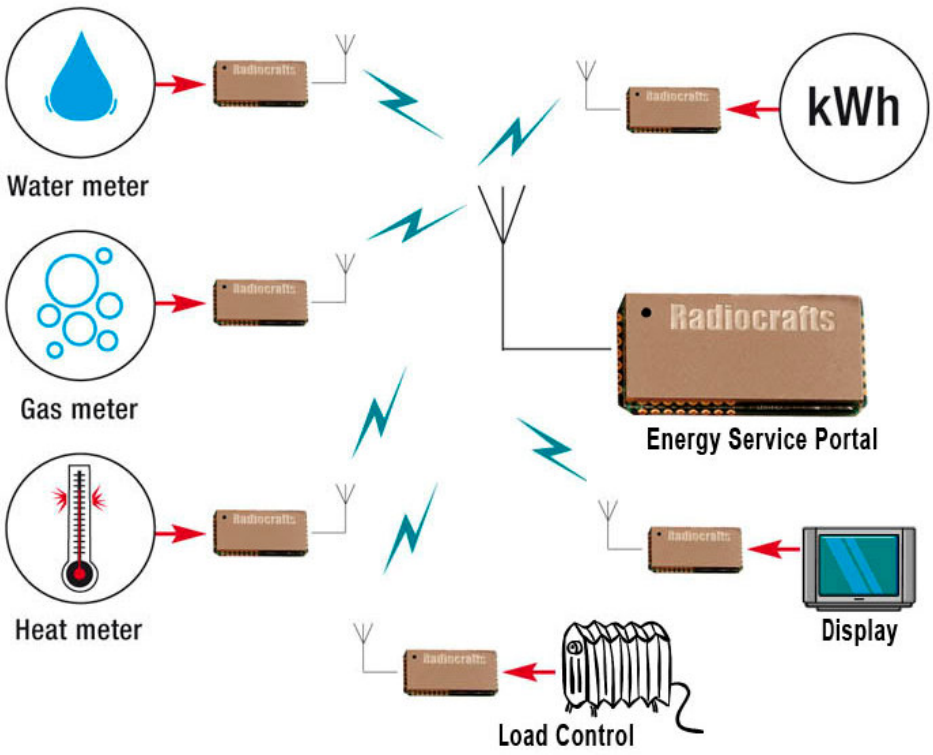
by Ø. Nottveit

Introduction

Radiocrafts offers two ZigBee Network Modules (ZNM, and ZNM-SE) with preloaded ZigBee PRO compliant stack. The ZigBee features are made available for an external application processor through an API via UART or SPI. See Figure 2.This document describes the basics of how such a module can be used to develop solutions compliant to the Smart Energy profile, see [1][2]. For more details on using the RC2400-ZNM, see [3][4].

The ZNM functionality is available for both RC2400 and RC2400HP (low and high RF output power platforms), but for the rest of the document such a module is only referred to as RC2400-ZNM.

There are two variants of the RC2400-ZNM firmware functionality. These are named RC2400-ZNM and RC2400-ZNM-SE. The difference is whether or not the module handles the application security (see page 9).



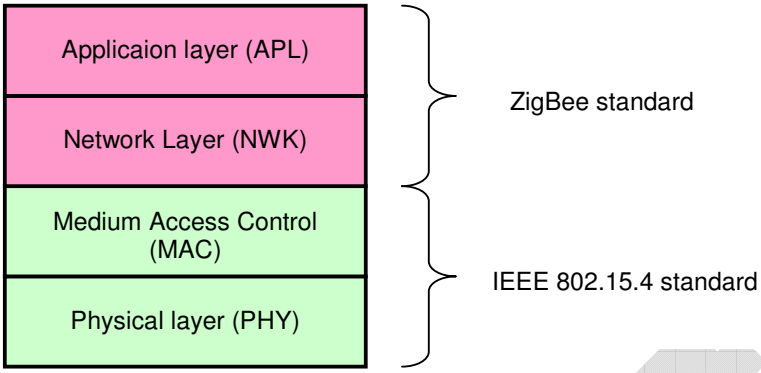


Figure 1. IEEE 802.15.4 and ZigBee protocol stack

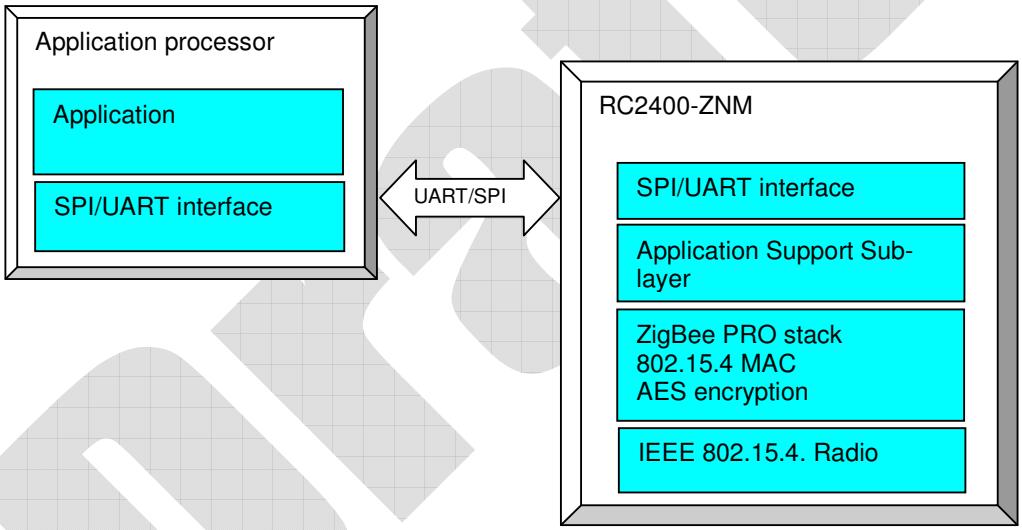


Figure 2. ZigBee Network Module concept

ZigBee Smart Energy Profile

The ZigBee Smart Energy profile is a public profile for metering Home Area Networks. It defines the behavior for devices used in wireless metering, load control and demand response. The profile specification also sets security requirements for such a network.

The current standard 1.0 defines the following devices

- Energy Service Interface (ESI), formerly known as Energy Service Portal (ESP)
- Metering Device
- In-Premise Display Device (IPD)
- Programmable Communication Thermostat (PCT)
- Load Control Device
- Range Extender
- Smart Appliance Device
- Prepayment Terminal Device

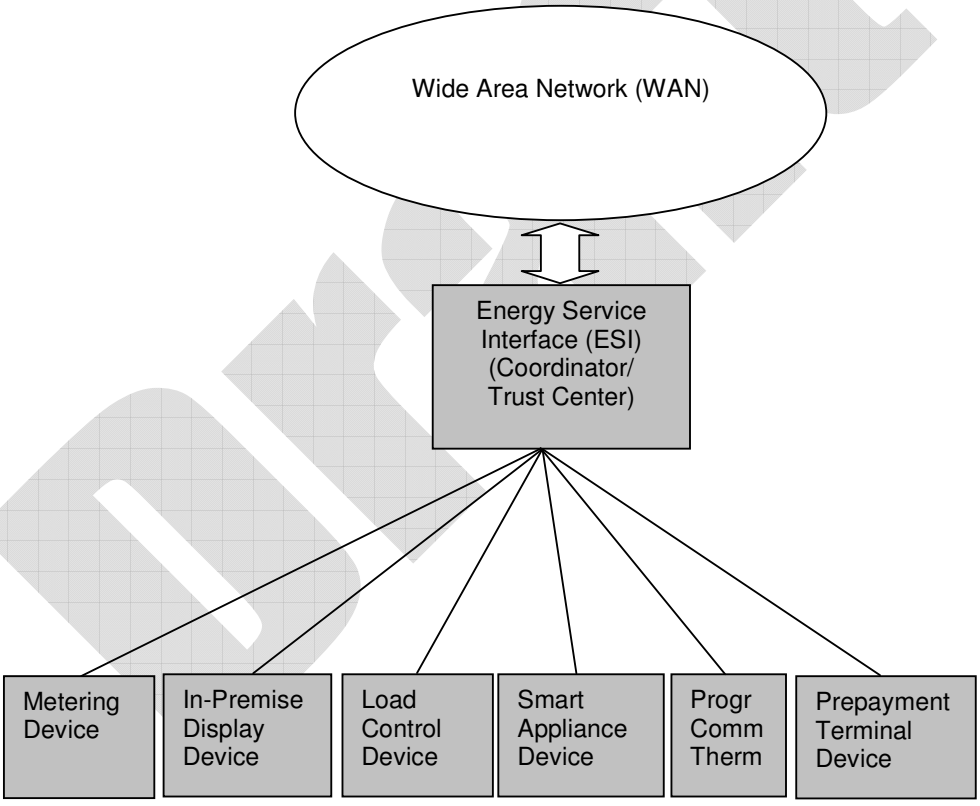


Figure 3 Logical smart metering network example

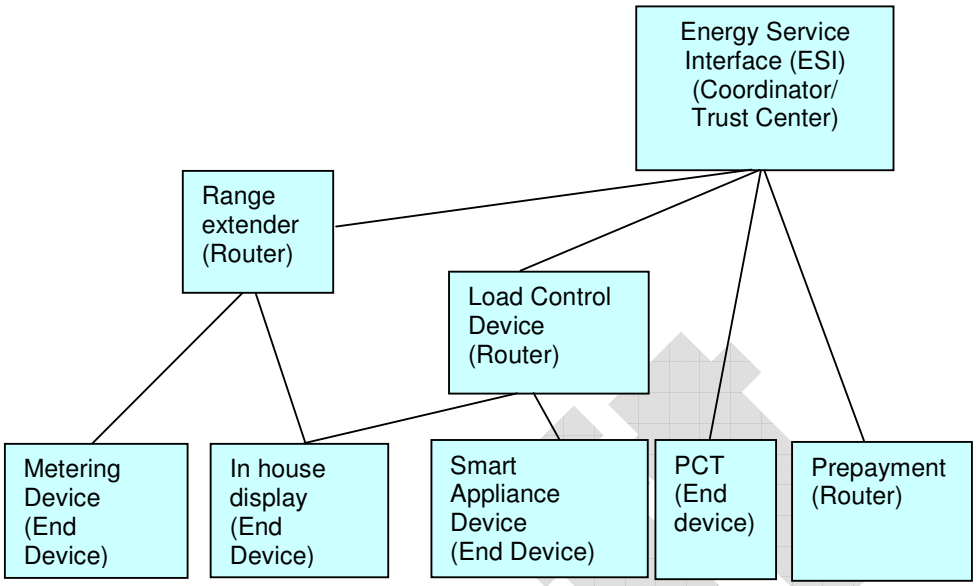


Figure 4 Physical Smart Energy network example

Table 1 shows the details of the services/cluster each device type shall and can support.

	Clusters															
Device	**Basic**	**Key Establishment**	**Cluster with Rep. Cap.**	**Power Configuration**	**Inter PAN Com**	**Alarm**	**Commissioning**	**Identify**	**Message**	**Price**	**Demand Response/Load Control**	**Time**	**Simple Metering**	**Tunneling (SEP 1.1)**	**Prepayment(SEP 1.1)**	**Over-The-Air Upgrade(OTA) (SEP 1.1)**
ESI(ESP)	S	S/C	s/c	s	s/c	s	s/c	s	S	S/c	S	S	s/c	s/c	s/c	
Metering	S	S/C	s/c	s	s/c	s	s/c	s	c	c		c	S	s	c	
IPD	S	S/C	s/c	s	s/c	s	s/c	s	c	c	c	c	c	c		
PCT	S	S/C	s/c	s	s/c	s	s/c	s	c	c	C	C	c		c	
Load Control	S	S/C	s/c	s	s/c	s	s/c	s		c	C	C				
Range Extender	S	S/C	s/c	s	s/c	s	s/c	s								
Smart Appliance	S	S/C	s/c	s	s/c	s	s/c	s	c	C	c	C				
Prepayment Terminal	S	S/C	s/c	s	s/c	s	s/c	s	c	C	c	C	c		S/C	

S = Mandatory **S**erver, s = Optional **s**erver, C = Mandatory **C**lient , c = Optional **c**lient

Table 1 Smart Energy Devices vs. Clusters

An implementation of SE 1.0 devices can be based on either the ZigBee 2007 Basic feature set or the PRO feature set. In addition it is required that Fragmentation and Application Link Keys are enabled, both which are optional in the stack profiles.
Application Link Keys are negotiated with the Key_Establishment Cluster, which utilize a Certificate based key exchange (CBKE) using Elliptical Curve Cryptography (ECC). Each device must also have a valid certificate in order for the Application Link Keys to be negotiated.

The security key scheme is shown in Table 2, and shows which key is required for each Cluster.

Functional Domain	Cluster Name	Security Key
General	Basic	Network Key
General	Identify	Network Key
General	Alarms	Network Key
General	Time	Application Link Key
General	Commissioning	Application Link Key
General	Power Configuration	Network Key
General	Key Establishment	Network Key
Smart Energy	Price	Application Link Key
Smart Energy	Demand Response and Load Control	Application Link Key
Smart Energy	Simple Metering	Application Link Key
Smart Energy	Message	Application Link Key
Smart Energy	Tunnelling	Application Link Key
Smart Energy	Pre-Payment	Application Link Key

Table 2 Security key usage (From [1])

Current released variant of the profile is 1.0. Revision 1.1 is in draft state and will include a definition of Tunneling, Prepayment and OTA Cluster in addition to upgrade of some of the other clusters. Rev. 1.1 will also support multiple ESIs in each network.

The work on Smart Energy 2.0 is started and includes a brand new IP-based stack including 6LoWPAN and ROLL.

RC2400-ZNM and RC2400-ZNM-SE presently handles SE profile 1.0, and is intended to also support SE 1.1 and 2.0, but a firmware upgrade is expected.

RC2400-ZNM Principle of Operation

To understand the basic operations of RC2400-ZNM please see [3] and [4]. Based on the serial interface described there, Figure 7 shows the flow chart for the communication between an external processor and the RC2400-ZNM. The communication is seen from the external processor point of view.

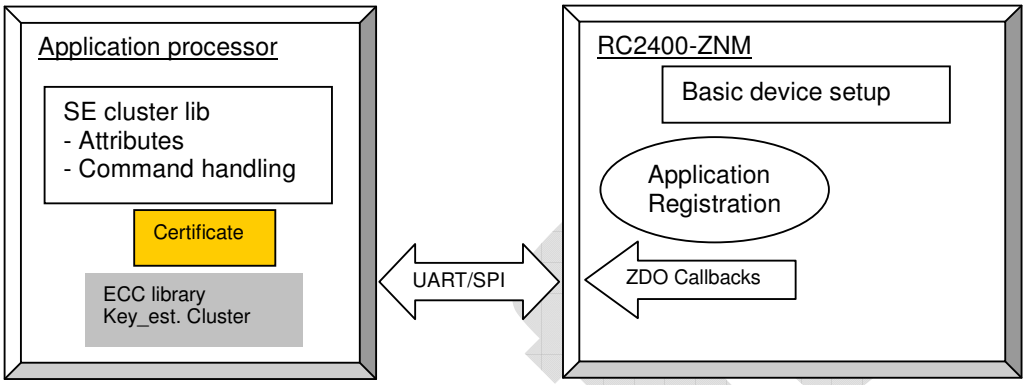


Figure 5. Conceptual view of the application processor and RC2400-ZNM

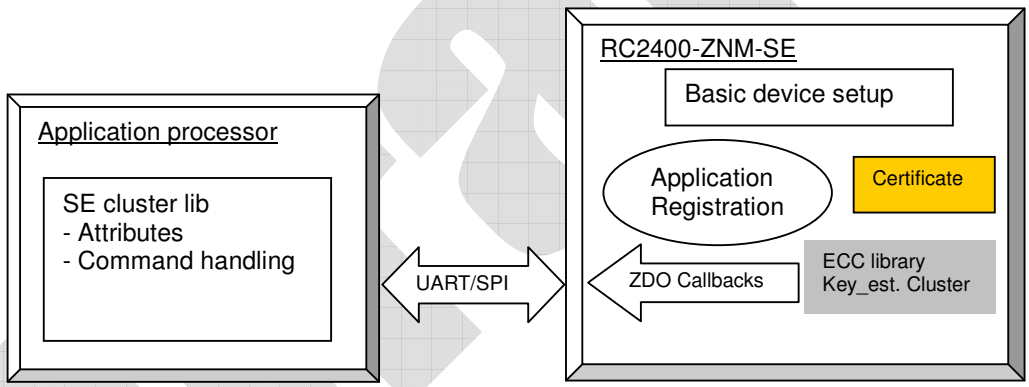


Figure 6. Conceptual view of the application processor and RC2400-ZNM-SE

First the external processor initiates the serial driver and the RC2400-ZNM will typically be held in reset during this time. When the external processor is ready the RC2400-ZNM is released (Reset line set high) and the external processor will get a *Reset_indication* message via the serial interface. The serial communication is now confirmed up and running, and the external processor can configure the RC2400-ZNM. The initialisation of the communication must be done every time the module power is switched on.

Basic Device Setup

Some of the setup will be fixed (e.g. for a gas meter to be an End Device) and such parameters can be configured during manufacturing of the SE device. Others parameter can de installation specific and will be set during installation. The configuration includes parameters like logical type (Coordinator, Router, End Device), PAN ID, channel selection etc.

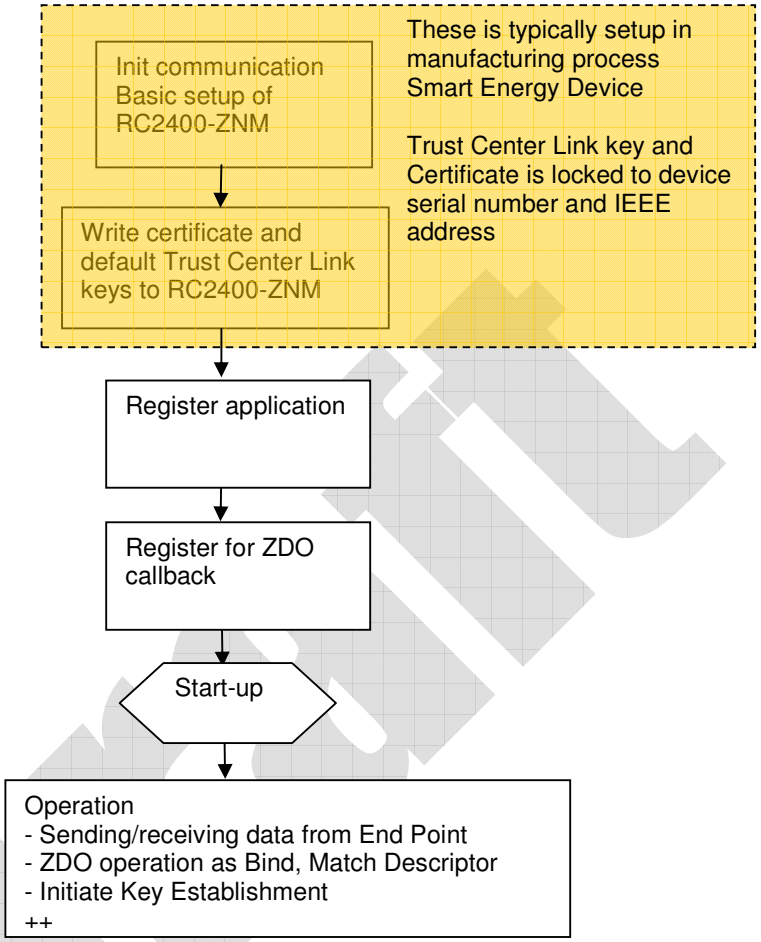


Figure 7. Flowchart for communication to RC2400ZNM

Certificate

All smart energy devices require a Certificate generated by an approved source like Certicom. These certificates are licensed, but test certificates are available for development and testing. Depending on the preferred solution (ZNM vs. ZNM-SE, se page 9) a Certificate can be written directly in the flash of the RC2400 module. This applies for the RC2400-ZNM-SE. Default Trust Centre Link keys must also be written to the module.

Both the Certificate and default link keys are linked to a specific device and its IEEE address and serial number. Hence the Certificate and default link keys can not be moved to another device.

Application registration

Application registration is defining the capability of the device and which End point it is located at. This is done with an *AF_Register* command.

The data registered can be summarized as
- End Point (logical address)
- Profile ID

- Device ID
- Version
- Latency requirement
- Input cluster supported
- Output cluster supported

The data registered is also known as the Simple Descriptor.

There can be several logical SE devices connected to one physical radio with different End Points.

Messages addressed to this EP will be sent via the serial interface.

ZDO callbacks

In addition to the application message the application processor sometime need to get notice on more network related messages received by the RC2400-ZNM. These are referred to as ZDO messages.

An example of this is the message ZDO_Device_Annonce that new devices generate to report their existence. This info is important for the ESI, but not for all other devices in the network. So the ESI must register for the ZDO_Device_Annonce message while other devices can skip this.

After all the above setup of the RC2400-ZNM, the module can start-up as a ZigBee device and activate RF. This is done with a specific *ZB_Start_Request* command.

Cluster libraries

The basic concept of the RC2400-ZNM requires the cluster library to be implemented in the external processor. This means that the attributes are stored there and the commands received must be handled there.

Application data is send and received from the RC2400-ZNM with the commands *AF_Data_Request* and *AF_Incoming_MSG* (see [4])

Example #1:
The ESI shall implement the Price server cluster hold the attribute Price. At certain intervals the price is updated from the WAN network. The ESP can then send the command *Publish_Price* to the SE devices with the Price Client Cluster. But the price is never stored within the RC2400-ZNM.

This means that if an SE device (e.g. In-Premises Display) later queries the price with the *Get_Current_Price* command, this command must be sent via UART/SPI to the application processor. The application processor will then generate a unicast *Publish_Price* command to the device that queried.

Example #2:
A metering device holds many attributes including type of meter (water, gas, and electricity), main index, meter status, data formatting, unit and optional historical data with time-of-use. The meter is required to report the main index every 15 minutes. But as a battery operated device it is an End Device and polls the network every 5 minutes.

The End Device polling is a part of the network layer and is handled by the module. The regular reporting is handled by the external processor. Each 15 minutes the external processor will wake-up, awake the RC2400-ZNM and send the required meter report.

Certicom ECC-libraries

Certicom security library for handling the Certificate based key exchange (CBKE) using Elliptical Curve Cryptography (ECC), can be located either inside the ZNM module or in the external processor. This algorithm takes 10- 20 kB of Flash memory, so to minimize complexity and cost of external processor the library should be located inside the module. The module will in this case be named RC2400-ZNM-SE.

The Key_Establishment_Cluster must be handled by the ECC library, and hence this will be handled inside the RC2400-ZNM-SE module. All that is needed from the application processor is an initiate call for key establishment.

TBD (The rest of the document is TBD)

Detailed setup of ESP/ESI
TBD (rest of document is TBD)

Cluster support

Mandatory

Server:
- Basic
- Key_establishment_cluster.
-Message
-Price
-Demand Response/Load Control
-Time

Client:
- Key_establishment_cluster.

Optional

Server:
-Cluster with reporting capabilities
-Power Configuration
-Inter-PAN Communication
-Alarms
-Commissioning
-Identify
- Manufacture-specific (If such exist it must be certified as Manf.Spes. in addition to SE certified)
-Smart Energy Tunnelling
-Simple Metering
-Prepayment

Client:
-Cluster with reporting capabilities
-Inter-PAN Communication
-Commissioning
- Manufacture-specific (If such clusters exists it must be certified as Manf.Spes. in addition to SE certified)
-Smart Energy Tunnelling
-Price
-Simple Metering
-Prepayment

Demand Response/Load Control

Commands sent from server:
-Load Control Event
-Cancel Load Control Event
-Cancel All Load Control Events

Attributes at Client
UtilityEnrolmentGroup
StartRandomizeMinutes
StopRandomizeMinutes
DeviceClassValue

Commands sent from Client

Report Event Status
Get Scheduled Events

Message

Commands sent from server:
Display Message
Cancel Message

Commands sent from Client
Get Last Message M
0x01 Message Confirmation

Price

Commands sent from server:
Publish Price

Key Establishment Cluster

Initiator is Client and Responder is Server
Normally SE device is Initiator and ESP is Responder, but it is recommended that ESP will also initiate is SE device fails.

Server/Client attributes:
Information
Contains info on capabilities

Server commands:
Initiate Key Establishment Request
Ephemeral Data Request
Confirm Key Data Request
Terminate Key Establishment

Client commands:
Initiate Key Establishment Response
Ephemeral Data Response
Confirm Key Data Response
Terminate Key Establishment

Simple Metering

Server Attributes

Reading Information Set
TOU Information Set
Meter Status
Formatting
ESP Historical Consumption
Load Profile Configuration
Supply Limit

References

[1] Smart Energy Profile Specification 1.0 075356r15ZB_SE_PTG-SE_Profile_Specification.pdf
[2] Smart Energy Profile Specification 1.0 addendum :SEP 1.0 Intermediate Release Profile Specification
[3] RC2400_RC2400HP_ZNM_User_Manual
[4] CC2530ZNP Interface Specification

Document Revision History

Document Revision	Changes
0.2	First draft

Trademarks

ZigBee® is a registered trademark of the ZigBee Alliance.

Contact Information

Web site: www.radiocrafts.com
Email: radiocrafts@radiocrafts.com
sales@radiocrafts.com
support@radiocrafts.com

Address:
Radiocrafts AS
Sandakerveien 64
NO-0484 OSLO
NORWAY

Tel: +47 4000 5195
Fax: +47 22 71 29 15