

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

by Ø. Nottveit

Introduction

Radiocrafts' ZigBee network modules (ZNM) make powerful ZigBee features available for an external application processor through an API via UART or SPI. Figure 2 shows the concept of the ZigBee Network Module with preloaded ZigBee PRO compliant stack and ZNM application layer. The –ZNM is described in detail in [3] and [4].

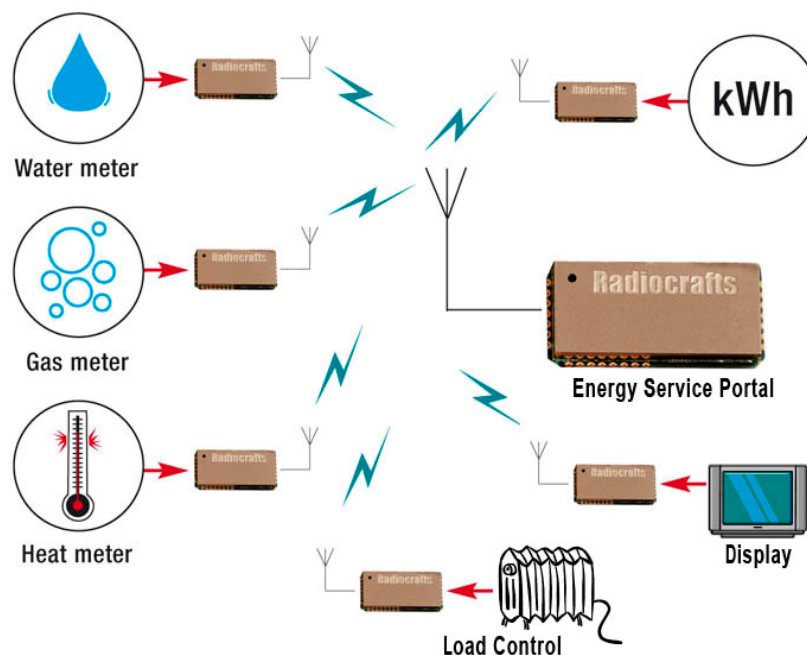
This document describes the basics of how such a module can be used to develop solutions compliant to the Smart Energy Profile (SEP) [1], [2].

The ZNM functionality is available for both RC2400 and RC2400HP. Since the API is the same for both, the rest of the document does not differentiate between HP and non-HP versions.

There are two variants of the RC2400-ZNM firmware with corresponding article numbers. These are named RC2400-ZNM and RC2400-ZNM-SE, with the only difference is whether or not the module handles the application security (See page 8). For applications requiring Smart Energy devices the –SE version of the module is recommended. Other ZigBee applications must use the standard –ZNM version. The API is the same for both –SE and standard –ZNM.

Prerequisite knowledge in order to get full value from reading this document:

- Knowledge of ZigBee including an understanding of Clusters, End points, Binding, Joining, Trust Center and Security
- Knowledge of Smart Energy Profile including CBKE Security Scheme and profile specific devices and clusters
- Understanding of the ZigBee Network Module concept



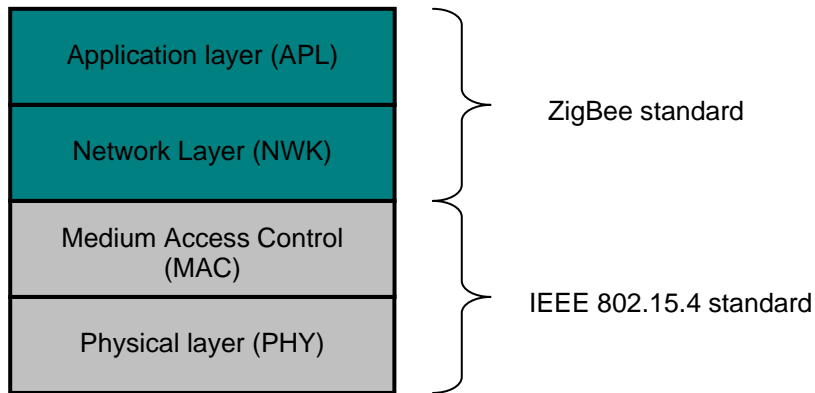


Figure 1. IEEE 802.15.4 and ZigBee standard protocol stack

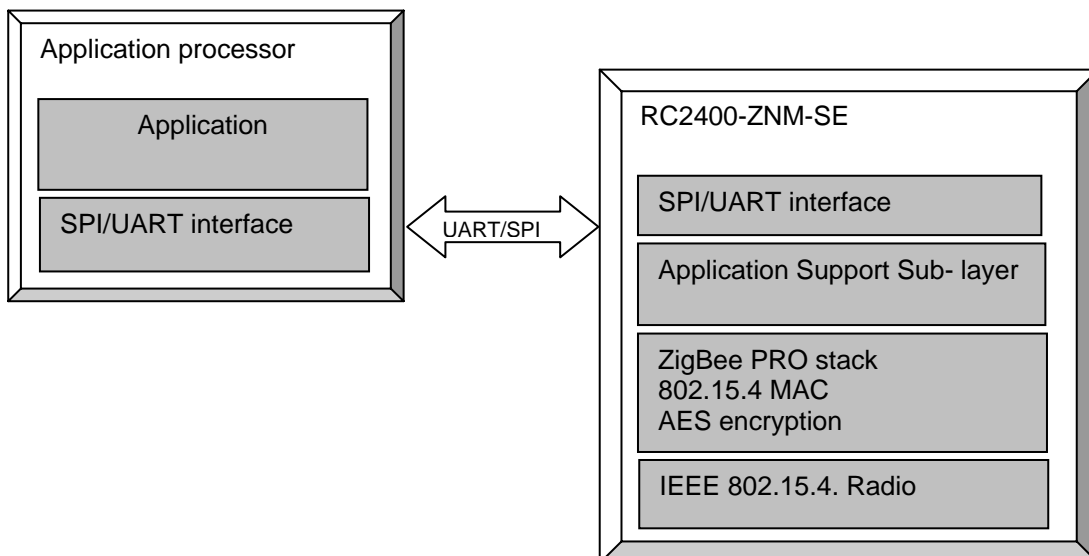


Figure 2. ZigBee network module concept

The application processor must configure the ZNM module and start the radio communication process. The following **minimum** message exchange must take place host <-> ZNM:

- Set up of logical type, device type, cluster support
- Loading of certificate and key
- Network startup-commands

ZigBee Smart Energy Profile

The ZigBee Smart Energy profile is a public profile for metering in Home Area Networks (HAN). It defines behavior for devices for metering, Load Control & Demand response. The profile also specifies security requirements for such networks.

Revision 1.0 of the standard 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

An example of a logical Smart Energy network is shown in Figure 3, while an example of a physical Smart Energy network with multihop is shown in Figure 4.

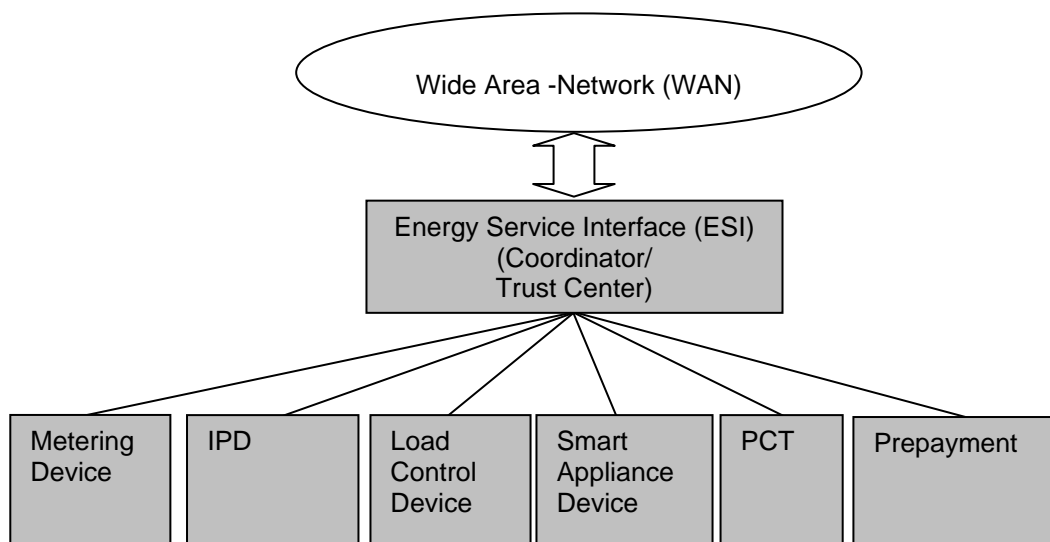


Figure 3 Logical smart metering network example

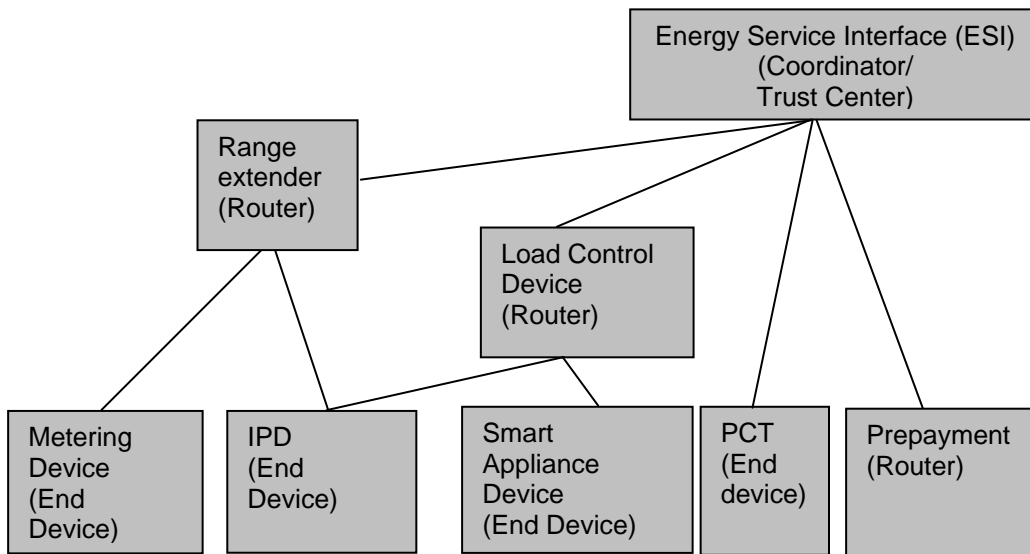


Figure 4. Physical Smart Energy network example

Table 1 shows which clusters are required and optional in each device.
 Cluster definition: A collection of attributes and commands for a given function/feature of a device.

Device	Clusters															
	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 Server, s = Optional server
 C = Mandatory Client, c = Optional client

Table 1. Smart Energy Devices vs. Clusters

An implementation of an SE 1.0 device can be based on either ZigBee 2007 Basic feature set or PRO feature set. In addition it is required that Fragmentation and Application Link Keys are enabled, both optional in stack profiles.

Application Link Keys (sometimes just called 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. All smart energy devices require a Certificate generated by a certificate agency (CA) like Certicom. These certificates are licensed, but test certificates are available for development and testing.

Current revision of SEP is 1.0, but revision 1.1 of SE is in draft version and will include definition of Tunneling, Prepayment and OTA Cluster in addition to upgrade some of the other clusters. Rev. 1.1 will also support multiple ESIs in each network.

Security

Security is handled at several levels in the SEP. A secure joining is required, where the network key is transferred with the Key Transport function. A preconfigured link encryption key, unique for each device, is used in the process. This key must be present at both trust center/ESI and joining device and must therefore be supplied to the trust center out of band. The network key will be used for control messages and some cluster messages, while the most critical clusters require an application link key.

The security key scheme in Current revision of SEP is 1.0, but Table 2 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	Tunneling	Application Link Key
Smart Energy	Pre-Payment	Application Link Key

Table 2. Security key usage

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 5 shows the flow chart for the communication between external processor and RC2400-ZNM. The communication is seen from the external processor point of view.

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-SE is released (reset high) and the external processor will get a *Reset_indication* message via serial interface. The serial communication over the interface is then confirmed up and running and the external processor can configure the RC2400-ZNM. The initialization of communication must be done every time the supply voltage is turned "on".

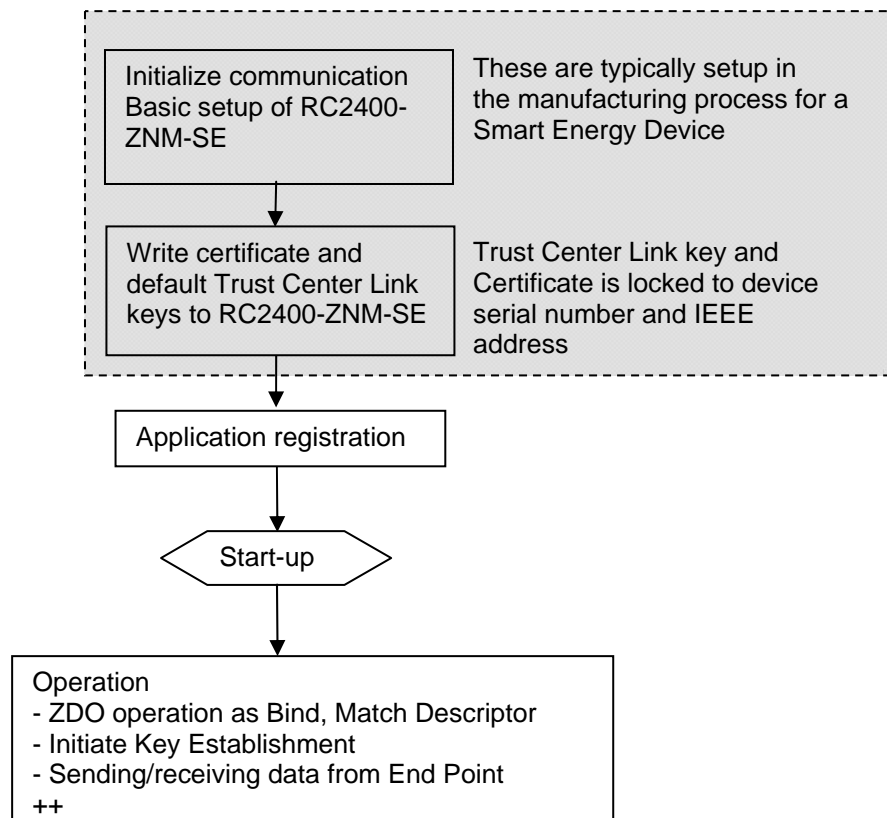


Figure 5 Flowchart for communication to RC2400-ZNM-SE

Below is described in more detail some of the steps described in the flowchart.

Basic device setup

Some of the setup will be fixed (e.g. for a gas meter to be an End Device) while other parameters can be installation specific and will be set during installation. The configuration includes parameters like logical type (Coordinator, Router, and End Device), PAN ID, channel selection etc. For complete list of parameters to set up see the SEP, and for a minimum setup see example at end of this document.

Certificate

When security is handled inside the module in ZNM-SE (see page **Error! Bookmark not defined.**) a certificate will be written directly in the flash of the RC2400 module. A 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 with multiple parameters.

The parameters registered with this one command 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/from this EP will be sent via the serial interface.

Clusters

The basic concept of the RC2400-ZNM-SE requires the cluster 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 sent and received from the RC2400-ZNM-SE with the commands *AF_Data_Request* and *AF_Incoming_MSG* (see [4])

Example #1:

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

This means that if a SE device (e.g. In-Premise Display) later queries the price, with the *Get_Current_Price* command, this command must be sent via UART/SPI to application processor at the ESI device. 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 or electricity), main index, meter status, data formatting, unit and optional historical data with time-of-use. The meter is required to report 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 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 must wake-up, awake the RC2400-ZNM and send the required meter report.

Security handling in RC2400-ZNM-SE

The Key_Establishment_Cluster must be handled by the ECC library, and this should be handled inside the RC2400-ZNM-SE module. All that is needed from application processor is an initiate call for key establishment. A security library for handling the Certificate based key exchange (CBKE) can optionally be located in the external processor (Figure 7). This algorithm takes 10- 20 kB of flash, so to minimize complexity and cost of external processor, the library should be located inside the module (Figure 6).

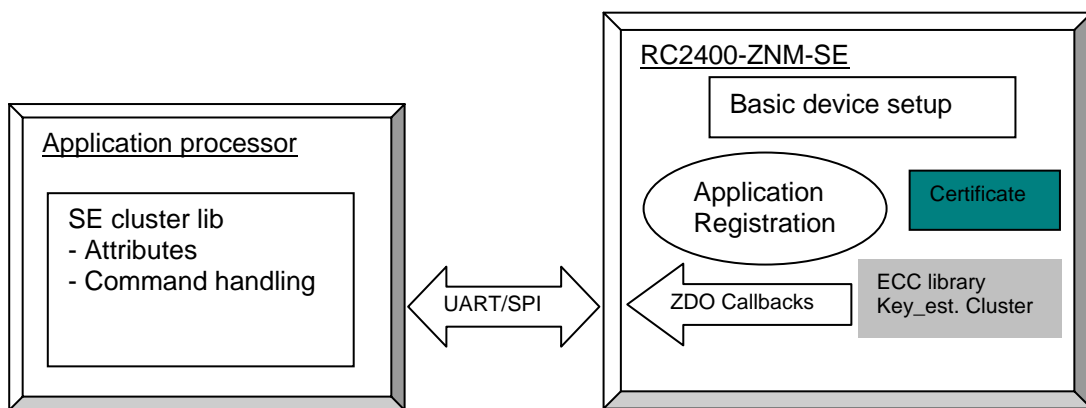


Figure 6 Conceptual view of application processor and RC2400-ZNM-SE

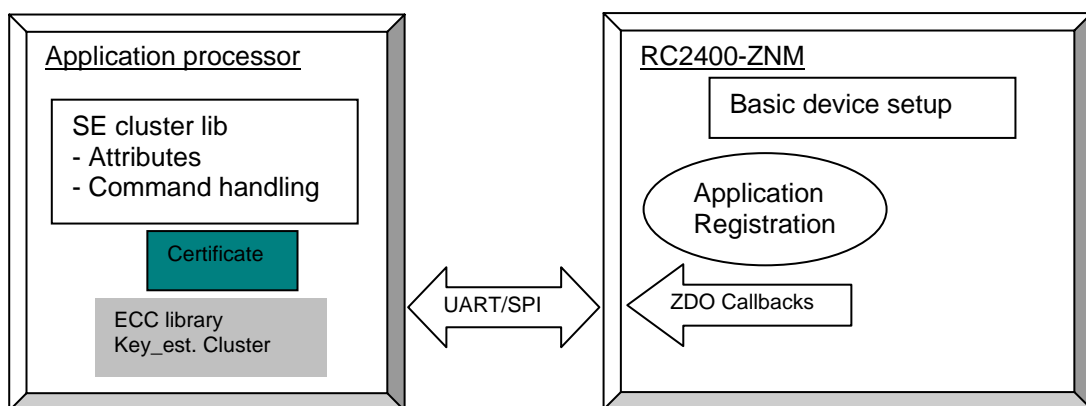


Figure 7. Conceptual view of application processor and RC2400-ZNM

To enable secure joining, the preconfigured link key must be written to the module. The RC2400HP-ZNM-SE module default use a single preconfigured trust center link key, but the module also supports multiple preconfigured trust center link keys. (One unique per device joining)

To enable multiple trust center link keys, write (with OSAL_NV_WRITE) 0x00 to address 0x006D. Maximum preconfigured trust center link keys are currently set to 10.

The unique preconfigured trust center link for each device might be written in locations 0x0101 to 0x010A with the following format (total 32 bytes)

IEEE address	Pre-configured link key	TX frame counter	RX frame counter
8 bytes	16 bytes	4 bytes	5 bytes

This modification must be done on all devices in the network.

Smart Energy Example

This example consists of the following subchapters:

- General part (this section)
- ESI setup
- HAN devices setup
- Operation

The example describes an SE compliant network with 3 devices.

- 1 ESI
- 1 Gas Meter
- 1 Display

and is supported with the RC2400HP-ZNM-SE Demo kit with 3 boards and the ZNM-CCT PC Tool.

The example network is drawn in Figure 8.

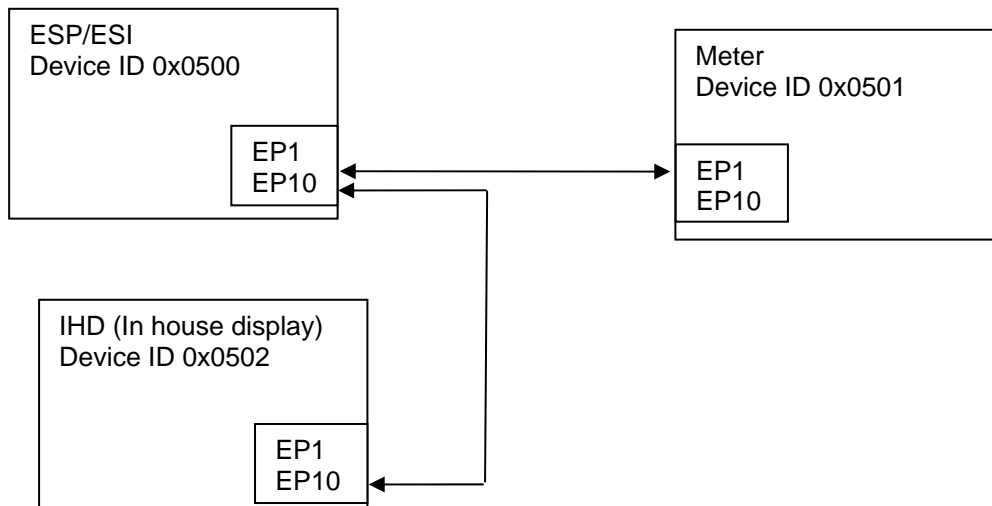


Figure 8. Smart Energy example network

In Table 3, Table 4 and Table 5 the cluster setup of each device can be seen. The devices include all the mandatory clusters in Smart Energy 1.0

Profile:	Smart Energy	Profile ID 0x0109
Device:	ESI	Device ID 0x0500
Server Clusters	Basic	Cluster ID 0x0000 Endpoint 0x01
	Time	Cluster ID 0x0A00 Endpoint 0x01
	Price	Cluster ID 0x0700 Endpoint 0x01
	Demand Response and Load Control	Cluster ID 0x0701 Endpoint 0x01
	Message	Cluster ID 0x0703 Endpoint 0x01
	Key Establishment	Cluster ID 0x0800 Endpoint 0x0A

Client Clusters	Simple Meter	Cluster ID 0x0703 Endpoint 0x01
	Key Establishment	Cluster ID 0x0800 Endpoint 0x0A

Table 3. Cluster setup of ESI

Profile:	Smart Energy	Profile ID 0x0109
Device:	Metering Device	Device ID 0x0501
Server Clusters	Basic	Cluster ID 0x0000 Endpoint 0x01
	Simple Meter	Cluster ID 0x0703 Endpoint 0x01
	Key Establishment	Cluster ID 0x0800 Endpoint 0x0A
Client Clusters	Key Establishment	Cluster ID 0x0800 Endpoint 0x0A

Table 4. Cluster setup of Metering device

Profile:	Smart Energy	Profile ID 0x0109
Device:	In-Premise Display	Device ID 0x0501
Server Clusters	Basic	Cluster ID 0x0000 Endpoint 0x01
	Key Establishment	Cluster ID 0x0800 Endpoint 0x0A
Client Clusters	Price	Cluster ID 0x0700 Endpoint 0x01
	Message	Cluster ID 0x0703 Endpoint 0x01
	Key Establishment	Cluster ID 0x0800 Endpoint 0x0A

Table 5. Cluster setup of Display device

Smart Energy Example - ESI setup

Normally the ESI will be set up first as coordinator to form the network. The sequence of API commands sent are shown in Figure 9. The API commands below are found in ZNM-CCT PCTool.

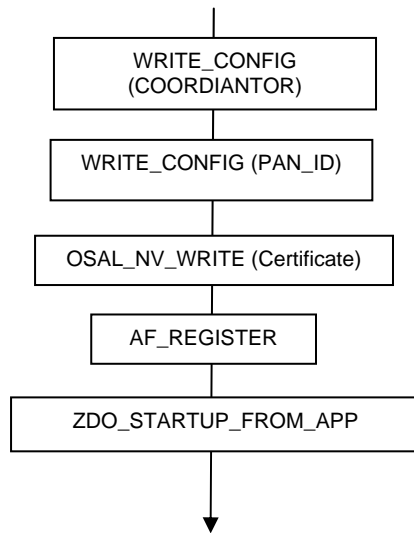


Figure 9. Initiate ESP/ESI

When writing the Certificate to the module the Device implicit Certificate, private key and CA public key must be written. See the RC24xx-ZNM User Manual. It is also important that the IEEE address of the module corresponds to the certificate written.

The certificate shown in ZNM-CCT is from SE Profile Specification. New test certificated or production certificates can be acquired from Certicom. (<http://www.certicom.com/device-authentication-service/smart-energy-device-certificate-service>)

The AF register command for ESI can be decoded as follows:

(Bytes are in same order as written to ZNP module. This means bytes within a field are written LSB first. E.g. Profile ID of SE profile is 0x0109, but written 0x0901,)

010901000501000500000A00000701070307010207

SOF + Length + CMD	End Point	Profile ID	Device ID	Version	Latency	Num In Cluster	List in Cluster	Num Out Cluster	List Out Cluster	CRC
FE152400	01	0901	0005	01	00	05	0000 0A00 0007 0107 0307	01	0107	32

After start-up the module will reply with a "change of state" = 0xFE0145C1098C, where the 09 indicate that the device is active as a coordinator in a network.

Smart Energy Example - HAN devices setup

When the network is formed the other devices can join in a secure manner. The setup sequence for joining meter and display is shown in. Sequences in dash are optional.

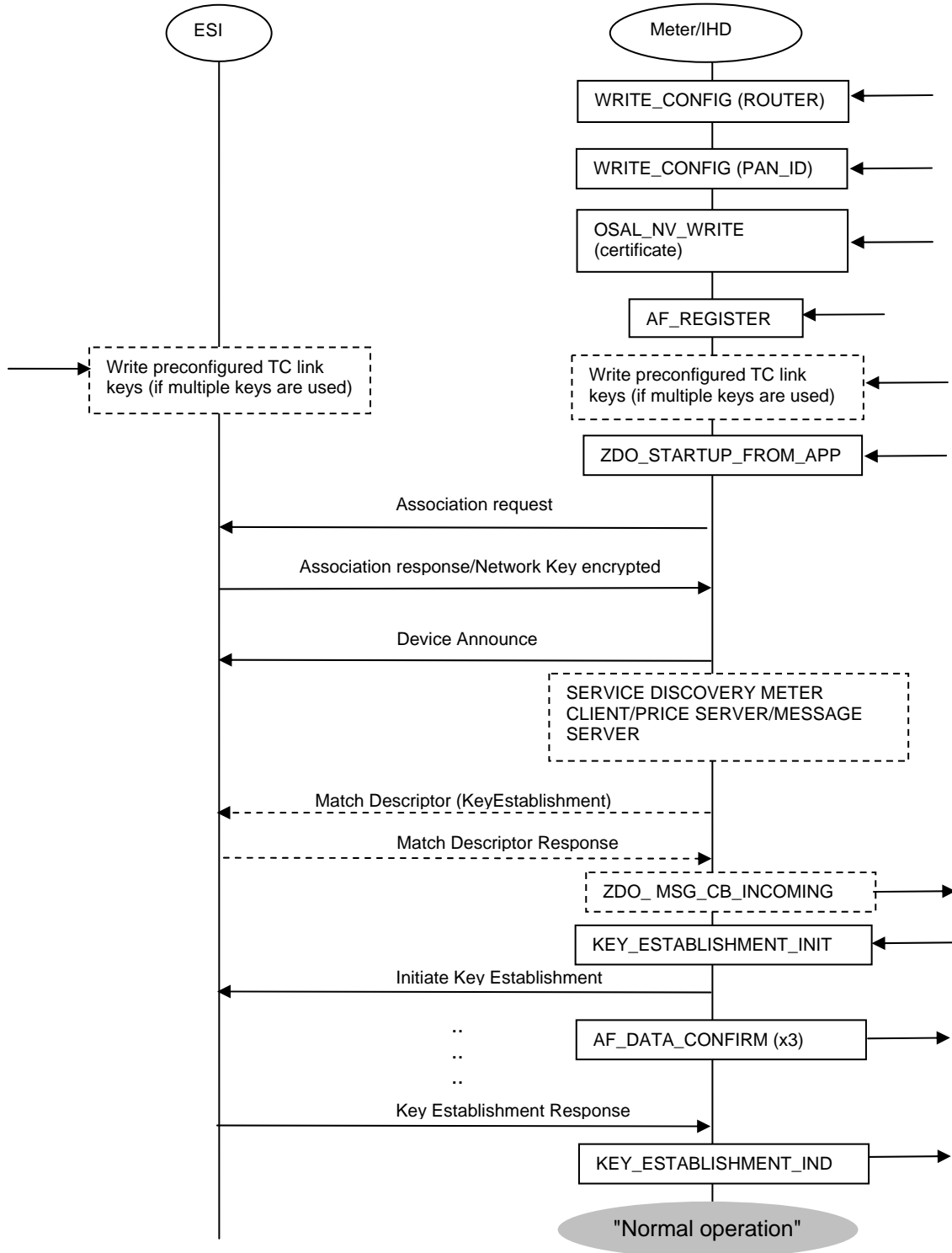


Figure 10. Setup sequence for joining devices

Smart Energy Example - operation

When device have performed a secure join of the network and Key Establishment procedure is finished the application processor can start sending application packages with application link security enabled.

There are some example application messages in the ZNM-CCT tool.

REPORT_METER_DATA (from meter to ESI) and PUBLISH PRICE (from ESI to display)

The AF_Data_request can be decoded as follows

	SOF	CMD	Dest addr	Dst End point	Src End Point	Cluster ID	Trans ID	Opt	Rad	Length	Data
Report meter data	FE	2401	0000	01	01	0207	00	40	03	0D	'13 bytes'
Publish price	FE	2401	FFFF*	01	01	0007	00	40	03	1F	'31 bytes'

*(must be replaced with short address of display)

The Data field can be decoded as follows (as specified in AFG ZigBee Cluster Library)

Report meter data:

Frame CTRL	Transaction sequence nb.	Cluster CMD	Attribute	Data type	Data
18	00	0A	0000	0D	0F0F0F0F0F0F
Not cluster specific command Not manf. specific Sent from Server Disable default response		Report attribute	Current Summation	48 bit data	dummy data

Publish Price:

Frame CTRL	Transaction sequence nb.	Cluster CMD	Provider ID	Rate Label	Issuer Event ID	Current time
58	00	00	0A0A0A0A	00	01010101	01010101
Cluster specific command Not manf. specific Sent from Server Disable default response		Publish Price	Dummy Provider ID		Dummy event ID	Dummy time

Unit of Measure	Currency	Price Trailing Digit & Price Tier	Num of Price Tiers & Register Tiers	Start time	Duration in minutes	Price
00	2400	A0	00	00000000	FFFF	008C0100
k	USD	10 digit trailing decimal point		Starting now	Until new notice	99,0

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
1.0	First release

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