System Specification

enocean alliance
Building Smarter Connectivity

Secure Remote Management

V 3.1

San Ramon, CA, USA

Executive Summary

Ver.	Editor	Change	Date
3.0	AP, MKA	Major update to Secure Remote Management	2022
3.1	AP	Added Session establishment in section 2.2.1	30.04.2024

DISCLAIMER

This information within this document is the property of the EnOcean Alliance and its use and disclosure are restricted. Elements of the EnOcean Alliance specifications may also be subject to third party intellectual property rights, including without limitation, patent, copyright or trademark rights (such a third party may or may not be a member of the EnOcean Alliance.) The EnOcean Alliance is not responsible and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This document and the information contained herein are provided on an "as is" basis and the EnOcean Alliance disclaims all warranties express or implied, including but not limited to (1) any warranty that the use of the information herein will not infringe any rights of third parties (including any intellectual property rights, patent, copyright or trademark rights, or (2) any implied warranties of merchantability, fitness for a particular purpose, title or noninfringement.

In no event will the EnOcean Alliance be liable for any loss of profits, loss of business, loss of use of data, interruption of business, or for any other direct, indirect, special or exemplary, incidental, punitive or consequential damages of any kind, in contract or in tort, in connection with this document or the information contained herein, even if advised of the possibility of such loss or damage. All Company, brand and product names may be trademarks that are the sole property of their respective owners.

The above notice and this paragraph must be included on all copies of this document that are made.

The EnOcean Alliance Secure Remote Management (REMAN) Specification is available free of charge to companies, individuals and institutions for all non-commercial purposes (including educational research, technical evaluation and development of non-commercial tools or documentation.)

This specification includes intellectual property („IPR“) of the EnOcean Alliance and joint intellectual properties („joint IPR“) with contributing member companies. No part of this specification may be used in development of a product or service for sale without being a participant or promoter member of the EnOcean Alliance and/or joint owner of the appropriate joint IPR. EnOcean Alliance grants no rights to any third party IP, patents or trademarks.

These errata may not have been subjected to an Intellectual Property review, and as such, may contain undeclared Necessary Claims.

EnOcean Alliance Inc.
c/o Global Inventures
5000 Executive Parkway, Suite 302
San Ramon, CA 94583
USA
Graham Martin Chairman & CEO EnOcean Alliance

Table of Contents

1 Introduction

This document describes the functionality of Secure Remote Management.

Remote Management allows EnOcean devices to be configured and interrogated over the air (using radio telegrams) without the need to physically access the device. Remote Management also allows retrieving debug information from the device and requesting the device to execute pre-defined procedures.

Secure Remote Management provides Remote Management functionality using a secure radio communication channel. It is designed to be platform independent and to be extensible for future use cases.

1.1 Definitions

Command – is a Request from the Remote Manager to the Remote Device to perform a specified action.

Device Description File – is a product specific xml file that describes the configurable parameters of a device in a machine-readable way

EEP – is the abbreviation of **E**nOcean **E**quipment **P**rofile. EEP describe the data encoding used by EnOcean devices.

EURID – is a unique device address (similar to a MAC address) that is assigned to every EnOcean device during production. The EURID unambiguously identifies the sender of an EnOcean radio telegram; it might additionally be used to specify the intended receiver of an EnOcean radio telegram (as part of an addressed data telegram - ADT).

Function Number – is a unique number assigned to an RMCC or RPC function.

Message – is the information exchanged between sender and receiver using their radio interfaces. One message might be transmitted using one or several Telegrams (depending on the length of the message).

Product ID – is a 6-byte value that uniquely identifies the device type and the manufacturer of a device. The Product ID is split into a two byte Manufacturer ID (assigned by EnOcean Alliance) and a four byte Product ID (assigned by the manufacturer). The Product ID is for instance used to look up the Device Description File for a given device.

Remote Commissioning - the application of the EnOcean Remote Management functionality by defining new standardized RPCs. The process of commissioning target devices without requiring physical access to the device. This can be accomplished in an interoperable way with the Remote Commissioning interface and process defined in [1].

Remote Device – is the device that is configured or interrogated by a Remote Manager or requested by the Remote Manager to execute a pre-defined procedure.

Remote Management – is the process used by the Remote Manager to configure or interrogate a Remote Device over the air (using radio telegrams) without the need to physically access the Remote Device. Remote Management also allows the Remote Manager to retrieve information from the Remote Device or to request the Remote Device to execute pre-defined procedures.

Remote Manager – is the device that is configuring or interrogating a Remote Device or requesting the Remote Device to execute a pre-defined procedure.

SYS_EX Telegram – is the telegram type that is used for Remote Management

1.2 References

[1] EnOcean Remote Commissioning Specification
https://www.enocean-alliance.org/recom-spec/

[2] EnOcean Equipment Profiles Specification
http://www.enocean-alliance.org/eep/

[3] Security of EnOcean Radio Networks
https://www.enocean-alliance.org/sec/

[4] Device Description File and Documentation Structure – XSD and XML Example
https://www.enocean-alliance.org/ddf/

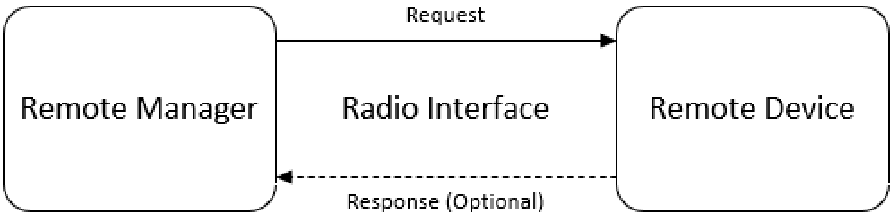
2 Remote Management Framework

Remote Management is the process used by a Remote Manager to configure or interrogate a Remote Device over the air (using radio telegrams) without the need to physically access the Remote Device. Remote Management also allows the Remote Manager to retrieve information from the Remote Device and to request the Remote Device to execute pre-defined procedures. The Remote Manager could for instance be a commissioning tool or a gateway while the Remote Device could for instance be an actuator or a sensor.

Using Remote Management, the Remote Manager issues one or several Requests to the Remote Device to perform a specific action such as setting a specific parameter to a certain value or interrogating the value of a specific parameter.

The Request can either be a Remote Management Common Command (RMCC) or a Remote Procedure Call (RPC). RMCC are basic functions defined by EnOcean Alliance which are supported by all devices. RPC provide more advanced functionality and their implementation can be manufacturer-specific.

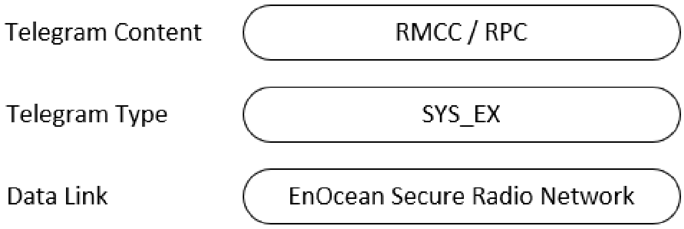
Depending on the Request type, the Remote Device might provide a Response to the Remote Manager. This basic communication flow is illustrated below.



Remote Management can be executed in a directed way (where a Remote Manager issues Requests to a specific Remote Device identified by its EURID) or as broadcast (where a Remote Manager issues Requests to all Remote Devices within its radio distance).

2.1 Remote Management within EnOcean Radio Protocol

Remote Management is executed within the framework of EnOcean Radio Protocol as shown below.



Specific information to the different layers is provided in the next chapters.

2.2 EnOcean Secure Radio Network

Data is exchanged as secure messages according to the Security of EnOcean Networks specification [3]. The security level format (SLF) shall be chosen according to the definition provided in chapter 8 of that specification.

For networks communicating using ERP1, SEC telegrams shall be used if the entire SYS_EX message fits into one ERP1 telegram. Otherwise, the SYS_EX message has to be split into a chain of secure chained data messages (SEC_CDM).

For networks communicating using ERP2, the entire SYS_EX message will be transmitted in one SEC telegram; this is possible because ERP2 permits a larger payload size.

2.2.1 Session Management

The previous Remote Management specification defined session commands for the communication between Remote Manager and Remote Device, like “unlock” and “lock”, or “start session” or “close session”.

These session commands ensured that at any given time only one Remote Manager could manage the Remote Device and were used to authenticate the Remote Manager. Attempts from a second Remote Manager to manage the device at the same time were discarded.

Session commands are no longer needed as the authentication of the Remote Manager is based on its possession of the security key used for secure communication with the Remote Device.

It is possible to have more than one Remote Manager (such as a PC gateway software or an embedded gateway) managing the Remote Device. In this case, each Remote Manager has to individually establish a secure connection with the Remote Device. The Remote Device must be able to handle one or more such secure connections. The maximum number of secure connections is product-specific.

A Secure Remote Management session can be initiated in the following ways:

1. Persistent Device Command:
Send a Secure Remote Management command (RMCC or RPC) directly to a device that is continuously powered.

2. Signal-Based Activation:
Initiate a Secure Remote Management session by sending a Secure Remote Management command (RMCC or RPC) following the receipt of a Signal 9 from an EnOcean device activating the receiver for a predetermined duration.

3. Bidirectional Energy-Constrained Devices:

For devices powered by batteries or energy harvesting, initiate a Secure Remote Management session by responding to an EEP data telegram (direction 1) with a Secure Remote Management command (RMCC or RPC) instead of a regular EEP reply (direction 2). Upon this response, the EnOcean device activates its receiver temporarily, allowing the managing device optional to send a Query Status RMCC (refer to Section 3.3). to confirm session establishment

2.3 SYS_EX Messages

The payload of the secure messages uses the SYS_EX message type (R-ORG 0xC5). The Endianness is Big-endian as usual in EnOcean communication. Two types of SYS_EX messages are defined depending on the type of transmitted telegram content.

EnOcean Alliance defined RMCC and RPC use the Manufacturer ID 0x7FF (EnOcean Alliance) which is omitted from the telegram payload for efficiency. The format of these messages is defined in chapter 2.3.1.

Manufacturer-defined RPCs use the Manufacturer ID of the manufacturer and the Manufacturer ID is transmitted as part of the telegram payload. The format of these messages is defined in chapter 2.3.2

2.3.1 SYS_EX Message for EnOcean Alliance-defined RMCCs or RPC

EnOcean Alliance-defined RMCC and RPC use the manufacturer ID 0x7FF which is omitted from the message payload. The resulting message structure is shown below.

	7	6	5	4	3	2	1	0
0	0	Unused = 0						
1	Function number							
2	Payload of RMCCs and RPCs							
…								
n								

The different fields within that message are listed Table 1 below.

Offset	Size	Data	Description
0	1	Manufacturer ID Present	Defines if the Header contains a Manufacturer ID 0b0: Manufacturer ID not present (Manufacturer ID 0x7FF will be used).
1	3	unused	Unused bits = 0
4	12	Function number	Function number of the RMCC/RPC
16	n	Payload	Payload of the RMCC/RPC

Table 1 SYS_EX fields for EnOcean Alliance-defined RMCC or RPC

2.3.2 SYS_EX Message for Manufacturer-specific RPC

Manufacturer-specific RPC provide the Manufacturer ID as part of the message payload. The resulting message structure is shown below.

<table>
<tr><th></th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>0</th></tr>
<tr><td>0</td><td>1</td><td colspan="7">Device Manufacturer ID</td></tr>
<tr><td>1</td><td colspan="4"></td><td colspan="4"></td></tr>
<tr><td>2</td><td colspan="8">Function number</td></tr>
<tr><td>3</td><td colspan="8" rowspan="3">Payload of Manufacturer specific RPCs</td></tr>
<tr><td>…</td></tr>
<tr><td>n</td></tr>
</table>

The different fields within that message are listed in Table 2 below.

Offset	Size	Data	Description
0	1	Manufacturer ID Present	Defines if the Header contains a Manufacturer ID 0b1: Manufacturer ID is present
1	11	Manufacturer ID	Device Manufacturer ID
12	12	Function number	Function number of the Manufacturer specific RPC
24	n	Payload	Payload of the Manufacturer specific RPC

Table 2 SYS_EX fields for manufacturer-specific RPC

2.4 RMCC, PRC and Responses

Secure Remote Management supports the following Requests and Responses:

- Request for EnOcean Alliance defined RMCC
- Request for EnOcean Alliance defined RPC
- Request for Manufacturer defined RPC
- Response to RMCC or RPC

2.4.1 Function Numbers

Requests and Responses are identified according to their function number as shown in Table 3 below.

Available function numbers	(0x000 – 0xFFF)	4096
Reserved	(0x000)	1
RMCC Request (EnOcean Alliance defined)	(0x001 – 0x1FF)	511
RPC Request (EnOcean Alliance or Manufacturer defined)	(0x200 – 0x5FF)	1024
RMCC Response or RPC Response	(0x600 – 0xFFF)	2560

Table 3 Function numbers for RMCC Requests, RPC Requests and their Responses

RMCC Requests and Responses are described in chapter 3 while RPC Requests and Responses are described in Chapter 4.

3 Remote Management Control Commands (RMCC)

Remote Management Control Commands - RMCC - are available in every product with Remote Management feature. They provide the basic functionality for Remote Management and have a common definition by EnOcean Alliance. Remote Devices therefore always react in the same way on the defined RMCC. The supported RMCC Requests are the following:

- Action
- Ping
- Query status

Table 4 below provides the Function Numbers for RMCC.

Function number	RMCC – Remote Management Control Commands
0x000…0x004, 0x007	RESERVED
0x005	Action
0x006	Ping
0x008	Query Status

Table 4 RMCC Function Numbers

3.1 Action Request

The Action RMCC requests the Remote Device to identify itself by means of performing an action. Typical examples include blinking a light, emitting a sound or switching a connected load ON or OFF.

Table 5 below provides the syntax of the Action RMCC. The Remote Device does not provide a Response to this RMCC, but it is possible to query its response status using the Query Status RMCC described in Chapter 3.3.

ACTION RMCC Request		
Function number		0x005
Payload data length		0 bytes
Unicast		yes
Broadcast		yes
Device responses to command		no
Status return code		
OK	0x00	
Wrong target Id	0x01	
Wrong manufacturer Id	0x04	

Table 5 Action Request Format

3.2 Ping

The Ping RMCC requests the Remote Device to report the radio quality of the received Request so that the Remote Manager can determine the reliability of the communication with the Remote Device. Table 6 below provides the syntax of the Ping RMCC.

The Remote Device does provide a Response to this RMCC as described in Chapter 3.2.1; additionally, it is possible to query its response status using the Query Status RMCC described in Chapter 3.3.

PING RMCC REQUEST		
Function number		0x006
Payload Data length		0 bytes
Unicast		yes
Broadcast		no
Device responses to command		yes
Status return code		
OK	0x00	
Wrong target Id	0x01	

Table 6 Ping RMCC Request Format

3.2.1 Ping Response

The Remote Device responds to the Ping Request from the Remote Manager with a Response using the format shown in Table 7 below.

PING RMCC RESPONSE	
Function number	0x606
Payload Data length	1 byte
Unicast	yes
Broadcast	no

Table 7 Ping RMCC Response Format

The Ping Response of the Remote Device includes 1 byte of payload shown in Table 8 which encodes the received signal strength (RSSI) of the received Ping Request.

Offset	Size	Data	Description	Valid Range	Scale	Unit
0	8	RSSI	RSSI-Level of received ping request.	0 … 255	0 … 255	-dBm

Table 8 Ping RMCC Response Payload

3.3 Query Status

The Query Status RMCC can be used by the Remote Manager to query debug information about the result of the most recent Remote Management Request on the Remote Device. Query Status can be used to query the following information:

- Most recent Request that was processed (identified by the Function Number)
- Result of that Request (identified by the Return Code)

Table 9 below provides the syntax of the Query Status RMCC.

QUERY STATUS RMCC REQUEST		
Function number		0x008
Manufacturer Id		0x7FF
Payload Data length		0 bytes
Unicast		yes
Broadcast		yes
Device responses to command		yes
Status return code		
	OK	0x00
	Wrong target Id	0x01
	Wrong manufacturer Id	0x04
	Not sent	0x07

Table 9 Query Status RMCC Request Format

3.3.1 Query Status Response

The Remote Device responds to the Query Status Request from the Remote Manager with a Response using the format shown in Table 10 below.

QUERY STATUS RMCC RESPONSE		
Function number		0x608
Payload Data length		3 bytes
Data content	Last Function number	12 bits
	Last function return code	8 bits
Unicast		yes
Broadcast		no

Table 10 Query Status RMCC Response Format

The Query Status Response of the Remote Device includes 3 byte of payload shown in Table 11 which encodes the Function Number and the resulting Return Code of the most recently processed Remote Manager Request.

Offset	Size	Data	Description
0	3	unused	Not used = 0
4	12	Function number	Last Function number of the RMCC/RPC
16	8	Return code	Last Function Return Code

Table 11 Query Status RMCC Response Payload

Table 12 provides a list of possible Return Codes.

Status name	Code number
OK	0x00
Wrong target ID	0x01
Wrong manufacturer ID	0x04
Wrong data size	0x05
Not sent	0x07
RPC failed	0x08
Address out of range	0x0D
Code data size exceeded	0x0E
Wrong data	0x0F

Table 12 Function Return Codes

3.4 Remote Device Response to RMCC Request

If a Remote Device received an RMCC from the Remote Manager that requires a Response to the Remote Manager then this Response will be send immediately using the syntax provided in the previous chapters.

If the Remote Device recognizes that the received Request was a broadcast Request, i.e. a Request from the Remote Manager to all Remote Devices within its radio range, and the Request requires a Response from the Remote Device, then the Response shall be sent with random delay to avoid collisions between the Responses from different Remote Devices. The random delay shall be randomly selected between 0 ms and 2000 ms.

4 Remote Procedure Calls (RPC)

RPCs functions strongly depended on the Remote Device. They provide additional functions like remote learn or remote clear of the learned IDs. Not every Remote Device provides the same RPCs. The manufacturer can also determine and implement RPC for his needs. These special RPCs are defined by the Function number and Manufacturer Id. The RPC are called with the call function command.

The benefit of extended options in Remote Management is that special and user defined remote device functions can be called remotely. The Remote Management offers ways to call those functions with appropriate commands and parameters. The following actions after the commands are specific for the remote device. The extended functions are specified by their Function number and manufacturer ID. Not every remote device supports every extended function. It is expected that some functions need to send data back to the actor. The length of the data can vary.

4.1 Remote Learn

The Remote Learn Request RPC can be used to start or stop the Learn Mode of a Remote Device.

Remote Learn RPC Request		
Function number		0x201
Payload Data length		1 byte
Unicast		yes
Broadcast		yes
Device responses to command		no
Status return code		
OK	0x00	
Wrong data size	0x05	
RPC failed	0x08	

Table 13 Remote Learn RPC Request Format

Offset	Size	Data	Description	Valid Range	Scale	Unit
0	8	Flag	learn flag, determines different behavior of the learn procedure	Enum: 0x00: RESERVED 0x01: Start learn 0x02: Next channel 0x03: Stop learn 0x04: SMART ACK – Start simple learn mode 0x05: SMART ACK – Start advanced learn mode 0x06: SMART ACK – Stop learn		

Table 14 Remote Learn RPC Request Payload

4.2 Remote Memory Write

The Remote Memory Write RPC can be used to write data to the memory of a Remote Device.

Remote Memory Write RPC Request		
Function number		0x203
Payload Data length		5+N bytes
Unicast		yes
Broadcast		yes
Device responses to command		no
Status return code		
OK	0x00	
Wrong data size	0x05	
RPC failed	0x08	
Code address out of range	0x0D	
Data size exceeded	0x0E	

Table 15 Remote Memory Write RPC Request Format

Offset	Size	Data	Description
0	32	Memory Address	Destination address where the data shall be written
32	8	Number of bytes	Number N of bytes to be transferred and written to the memory
40	N*8	Data	Data to be transferred and written to the memory

Table 16 Remote Memory Write RPC Request Payload

4.3 Remote Memory Read

The Remote Memory Read RPC can be used to read data from the memory of a Remote Device.

Remote Memory Read RPC Request		
Function number		0x204
Payload Data length		5 bytes
Unicast		yes
Broadcast		no
Device responses to command		yes
Status return code		
OK	0x00	
Wrong data size	0x05	
RPC failed	0x08	
Code address out of range	0x0D	
Data size exceeded	0x0E	

Table 17 Remote Memory Read RPC Request Format

Offset	Size	Data	Description
0	32	Memory Address	Start address where the data shall be read from the memory
32	8	Number of bytes	Number of bytes to be transferred and read from the memory

Table 18 Remote Memory Read RPC Request Payload

4.3.1 Remote Memory Read Response

The Remote Device sends the Remote Memory Read Response to the Remote Manager in response to a Remote Memory Read Request from the Remote Manager.

Remote Memory Read RPC Response	
Function number	0x804
Payload Data length	N bytes
Unicast	yes
Broadcast	no

Table 19 Remote Memory Read Response Format

Offset	Size	Data	Description
0	N*8	Data	Data read from the memory

Table 20 Remote Memory Read RPC Response Payload

4.4 SMART ACK Read Settings

The Remote Manager can use the SMART ACK Read Settings RPC to read the SMART ACK Mailbox Settings or the SMART ACK Learned Sensors from the Remote Device. The Setting Type field determines which of these two options is requested. The Remote Device responds to this request either an RPC Response with Function Number 0x805 (in response to Mailbox Settings Request) or Function Number 0x806 (in response to Learned Sensor Request).

SMART ACK Read Settings RPC Request		
Function number		0x205
Payload Data length		1 byte
Unicast		yes
Broadcast		no
Device responses to command		yes
Status return code		
OK	0x00	
Wrong data size	0x05	
RPC failed	0x08	
Data size exceeded	0x0E	

Table 21 SMART ACK Read Settings RPC Request Format

Offset	Size	Data	Description	Valid Range	Scale	Unit
0	8	Setting Type	Type of settings to read	Enum:		
				0x00: RESERVED		
				0x01: Mailbox Settings (Read number of mailboxes)		
				0x02: Learned Sensors (Read the ID table of sensors)		

Table 22 SMART ACK Read Settings RPC Request Payload

4.4.1 Response to Mailbox Settings Request

If the Remote Manager requests information about Mailbox Settings, then the Remote Device responds using Function Number 805.

SMART ACK Read Settings RPC: Mailbox Settings Response	
Function number	0x805
Payload Data length	6 bytes
Unicast	yes
Broadcast	no

Table 23 Format of Response to SMART ACK Read Settings – Mailbox Settings RPC

Offset	Size	Data	Description
0	32	SMART ACK flash address	Address where the SMART ACK settings are stored
32	16	SMART ACK mailbox count	Number of mailboxes stored in flash

Table 24 Payload of SMART ACK Read Settings – Mailbox Settings RPC Response

4.4.2 Response to Learned Sensors Request

If the Remote Manager requests information about Learned Sensors, then the Remote Device responds using Function Number 806. For each of the *N* entries in its ID table, it will provide information about the SensorID, the ControllerID and the Mailbox index.

SMART ACK Read Settings RPC: Learned Sensors Response	
Function number	0x806
Payload Data length	N*9 bytes
Unicast	yes
Broadcast	no

Table 25 Format of Response to SMART ACK Read Settings – Learned Sensors RPC Request

Offset	Size	Data	Description
N*0	32	SensorID	EURID of sensor
N*32	32	ControllerID	EURID of controller
N*64	8	Mailbox index	Index of mailbox

Table 26 Payload of Response to SMART ACK Read Settings – Learned Sensors RPC Request

4.5 SMART ACK Write Settings

The Remote Manager can use the SMART ACK Write Settings RPC to add a SMART ACK Mailbox, delete a SMART ACK Mailbox, Learn In a SMART ACK Mailbox or Learn Out a SMART ACK Mailbox. The requested operation is determined by the Operation Type field in the payload of this command.

SMART ACK Write Settings RPC Request		
Function number		0x206
Payload Data length		depending on operation type
Unicast		yes
Broadcast		no
Device responses to command		no
Status return code		
OK	0x00	
Wrong data size	0x05	
RPC failed	0x08	

Table 27 SMART ACK Write Settings RPC Request Format

4.5.1 Add Mailbox Request (only controller)

Offset	Size	Data	Value	Description
0	8	Operation Type	0x01	Add Mailbox (only controller)
8	8	Mailbox index		Index of mailbox
16	32	SensorID		EURID of sensor
48	32	PostmasterID		EURID of postmaster

Table 28 Payload for SMART ACK Write Settings - Add Mailbox RPC Request

4.5.2 Delete Mailbox Request

Offset	Size	Data	Value	Description
0	8	Operation Type	0x02	Delete mailbox
8	8	Mailbox index		Index of mailbox

Table 29 Payload for SMART ACK Write Settings - Delete Mailbox RPC Request

Offset	Size	Data	Value	Description
0	8	Operation Type	0x03	Learn In (only controller)
8	8	Mailbox index		Index of mailbox
16	32	SensorID		EURID of sensor
48	32	ControllerID		EURID of controller

Table 30 Payload for SMART ACK Write Settings – Learn In RPC Request

4.5.3 Learn Out Request (only controller)

Offset	Size	Data	Value	Description
0	8	Operation Type	0x04	LearnOut (only controller)
8	8	Mailbox index		Index of mailbox
16	32	SensorID		EURID of sensor
48	32	ControllerID		EURID of controller

Table 31 Payload for SMART ACK Write Settings – Learn Out RPC Request

4.6 RPC Remove Device

The Remote Manager can use the SMART ACK Remove Device RPC to remove a Remote Management connection from the Remote Device.

SMART ACK Remove Device RPC Request		
Function number		0x207
Payload Data length		0 byte
Unicast		yes
Broadcast		no
Device responses to command		no
Status return code OK Wrong data size RPC failed	 0x00 0x05 0x08	

Table 32 Remove Device RPC Request Format

4.7 Remote Device Response to RPC Request

If a Remote Device received an RPC Request from the Remote Manager that requires a Response to the Remote Manager, then this Response shall be sent using the syntax provided in the previous chapters.