Engineering
2232 Northmont Parkway
Duluth, Georgia 30096
USA

Onity
A UTC Fire & Security Company

Original Date:	12/16/2009	Document:	ORP_OAdoc
Project Number:	1071/2036	Page:	1 of 107
DWG/Part Number:			

ONITY READER PROTOCOL

DISTRIBUTION: Per document OPDP00003

ORIGINAL APPROVAL:

Prepared by (Last, First Initial)	Signature & Date (Use Italics)	Approved by (Last, First Initial)	Signature & Date (Use Italics)
Vahalia, Ketki	*Vahalia, K 12/16/2009*	Bacellar, Luiz	*Bacellar, L 12/16/2009*

REVISION APPROVAL RECORD (Revision history on next page):

Revision Number	Revision Date (yyyy/mm/dd)	Prepared by (Last, First Initial)	Approved by (Last, First Initial)	Signature & Date (Use Italics)
B	2010/02/25	Vahalia, K	Leyva, S.	Silvia B Leyva (2010/02/30)
C	2010/11/11	Leyva, S.	Vahalia, K	Ketki Vahalia (201011/12)

REVISION HISTORY:

Revision Number	Revision Date (yyyy/mm/dd)	Prepared by (Last, First Initial)	Description of Changes (reference section or page numbers)
B	2010/02/25	Vahalia, K	Updated ACU, reader and WLM firmware upgrade procedure Removed all command specific NACK tables and consolidated NACK error codes in one table. Added Firmware Upgrade Success command Updated the Test Key command (renamed to Test LMS Communication command) Update payload format for Add/Update Users and Delete users command. Describe a NACK scenario for Add/Update Users command. Added some clarification and a NACK condition for Update Lock command Update payload description for Send Events to OGACS command. Added sub command IDs for ACK command Added NACK_SUBCMD_INVALID_PAYLOAD Added event MECHANICAL_KEY_OVERRIDE_REVERTED
C	2010/11/10	Leyva, S	Added WLM serial number details in Read Lock Info command. Removed “Clear Audit Trail” command (Section 3.2.2) and AUDIT_TRAIL_CLEARED event (Section 5.2) Added clarification for ACU/LMS parameters (Section 4.1.1) Added following NACK codes – NETWORK_JOIN_FAILED, TEST_KEY_FAILED and INVALID_FIRMWARE_FILE Added details about battery life check during reader firmware upgrade (Section 4.49) Corrected payload length for Hello command (Section 4.1) Added details regarding ACU/CM being busy after the Update SCF command. (Section 4.40)

C (cont.)	2010/11/10	Leyva, S	Added new command for range verification in factory configuration (Modified Section 3.2.2 and added section 4.41) Added a date time format example (Appendix, Section 6.1) Modified Update SCF for Mifare support. (Section 4.40)

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose of this document

This document describes the Onity Reader Protocol used for communication between the Control Module/Translation Board and the Reader Module. The ORP is independent of the RFID technology used for reading the card, i.e. MIFARE, NFC, HID iCLASS, etc…

This document can serve as a basis for:-.

- HLD documents for the firmware to be developed between the Control Module OR Encoder and Reader Module.
- As a reference document for integration and testing of the ORP.

1.2 Scope of this document

This Document explains the different ORP commands.

1.3 Definitions, Abbreviation and Acronyms

Acronym	Description
ACK	Acknowledge
ACU	Access Control Unit – often used interchangeably with CM This term is also used to describe the complete lock
CM	Control Module – ACU is often used instead of CM
HB	Heart Beat
HLD	High Level Design
LMS	Lock Management System
NACK	No Acknowledge
NFC	Near Field Communication
ORP	Onity Reader Protocol
PDA	Personal Digital Assistant
PP	Portable Programmer
RM	Reader Module
SPI	Serial Peripheral Interface
UART	Universal Asynchronous Receiver Transmitter
WLM	Wireless Lock Module

Access Information → User, System and Time Parameters which define the access or denial of the user to the lock.

CM_Wakeup → Interrupt signal from the WLM to the Control Module

Device Data → Source ID (1 Byte) + Destination ID (1 Byte)

TARJ → Interrupt signal from the Reader Module to the Control Module

WLM_Wakeup → Interrupt signal from the Control Module to the WLM

Reader_Wakeup -> Interrupt signal from the Control Module to Reader

2 Overview

2.1 What is ORP

The ORP is Onity defined and Onity Proprietary Protocol.

The aim for ORP is to define the interface between the Control Module and Reader Module or WLM or PDA or LMS and Encoder to LMS. This in turn makes the Control Module independent of the different RFID technology used in Readers. Hence, any Reader Module (supporting a wide variety of technology from MIFARE to NFC to HID iCLASS, etc…) can be plugged into the Control Module without the need to modify the firmware on the Control Module. The PDA, WLM and the readers are physically connected to the Control Module over either UART or API. For these entities ORP is used for communication over the serial link and includes flow control signals. The Control Module can connect to the LMS through WLM through a virtual link. Between LMS and the Control Module, the ORP is used as an application protocol. The flow control in this case is between WLM and CM since WLM provides the connection between LMS and the CM.

The below Fig explains the concept of the same.

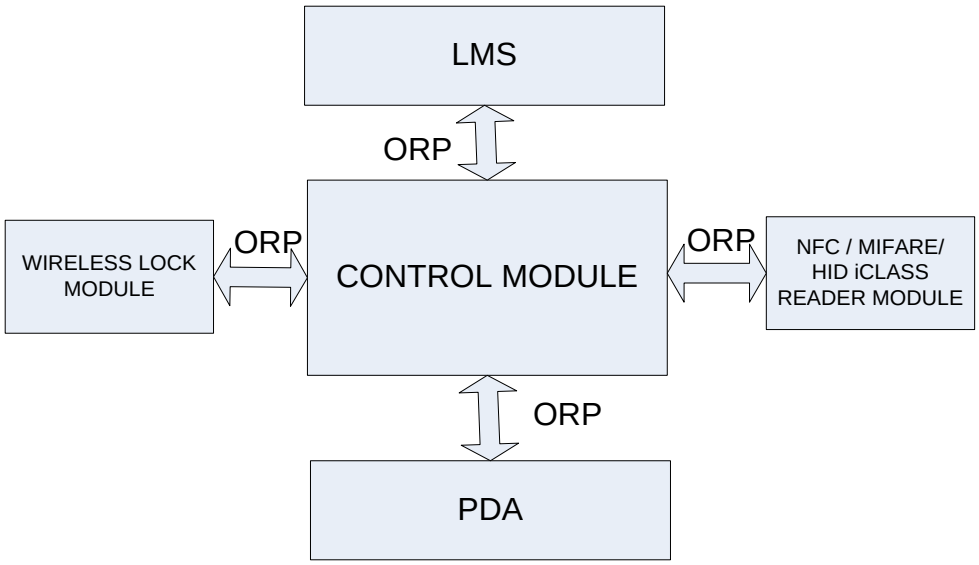

Figure 2-1 ORP Communications

2.1.1 Signals between Control Module and Radio Module (WLM)

The Control Module communicates with the WLM over UART (Rx and Tx) and two additional pins (WLM_Wakeup & *CM_Wakeup*) for flow control. The *WLM_Wakeup & CM_Wakeup* in steady state are pulled low.

When the WLM needs to send data to the Control Module, the *CM_Wakeup* signal shall be pulled high. The Control Module shall respond with an ACK. After an ACK is received the *CM_Wakeup* signal shall be pulled low and data transmitted.

When the Control Module needs to send data to the WLM, the *WLM_Wakeup* signal shall be pulled high. The WLM shall respond with an ACK. After an ACK is received the *WLM_Wakeup* signal shall be pulled low and data shall be transmitted.

The *CM Wakeup and WLM Wakeup* signals shall be used only to wake the CM or the WLM respectively. These signals shall have no impact on the ORP command processing. The same signals are used for the communication between LMS and the CM. Note that WLM send wake-up signal to Control Module every time it has a packet to be sent to Control Module.

2.2 Intended Audience

This document is intended for the ILS development team and leadership team from Onity and OEMS.

3 ORP Description

ORP is a request / response based protocol. A request always has a response in form of an acknowledgement. If the response has some data, it is acknowledged in turn. The following section describe the packet structure and the supported commands, along with sequence of successful ORP transaction or cases where ORP transaction fails.

3.1 Packet Structure

The packet structure for the ORP is as shown below:

Packet Length	Command ID	Sub Command ID	Packet Sequence Number	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Max 128 Bytes	2 Bytes

Table 3-1 ORP Packet Structure

The packet is sent out MSB first and the data in the packet is arranged in little endian format.

3.1.1 Packet Length

This is the length in bytes of the entire packet including the payload and checksum. When a payload is not present, then the packet length is 9.

3.1.2 Command ID

The command ID describes either the command to be executed or the event sent from the lock.

3.1.3 Sub Command ID

The sub command ID is used along with command ID to further describe a command or an event. Not all command IDs have an associated sub command ID.

3.1.4 Packet Sequence Number

The packet sequence number is used when an ORP command spans over multiple ORP packets. An ORP command always starts with sequence number 0 and is incremented for each new packet. Note that the sequence number is not incremented for ORP acknowledgements. The acknowledgements have the same sequence number as the packet it is acknowledging. The maximum sequence number is 65535. After an End Of Transmit packet, the sequence number rolls back to zero.

3.1.5 Source ID

The source ID identifies the source of the ORP packet. The valid source IDs are enumerated in **Error! Reference source not found.**.

Source ID	Value
ACU	0x00
Mifare Reader	0x01
iClass Reader	0x02
AWID Reader	0x03

Source ID	Value
eProx Reader	0x04
PDA	0x10
WLM	0x11
LMS	0x12
PTE	0x13

Table 3-2 ORP Source IDs

3.1.6 Destination ID

The destination ID identifies the destination of the ORP packet. The valid destination IDs follow the same enumeration as the source IDs and are enumerated in **Error! Reference source not found.**. Note: The "Source ID + Destination ID" is referred as "Device Data", in some of the ORP sequences. These naming differences will be corrected as part of ORP document re-structuring.

3.1.7 Payload

The payload may or may not be present, depending on the command ID and sub command ID. The maximum payload length is 128 bytes for LMS, WLM, PDA packets. For reader packets, the max payload length is 72 bytes.

3.1.8 Checksum

The checksum is used to validate the ORP packet. The checksum is calculated as follows:

The packet is considered as a set of 16-bit words. If packet length without the checksum is an odd number of bytes, a 0x00 byte is padded to the end of the packet. Then the 16-bit words are added. If their sum is a 32 bit number, the Result MSB word is added to the Result LSB word. The carry, if any is again added to the Result LSB and it is encoded as Checksum.

Example: Byte Array – 0x09 0x08 0x01 0xFF 0xFF 0xFF 0xFF **0x0A 0x08**

0x0809 +

0xFF01+

0xFFFF+

0x00FF

Result –32 bit number - 0x00020808

Result MSB – 0x0002 +

Result LSB – 0x0808

---

16 bit Checksum - **0x080A**

3.2 ORP Commands

3.2.1 Commands Categories

ORP commands can be classified into four categories:

- Control commands – These command require certain action at the lock, that can change the lock functional mode, its state or its configuration. These commands do not have any payload.
- Send Data commands – These commands change the configuration of the lock. These commands always have an associated payload, which can span across multiple packets.
- Get Data commands – These commands request data from the lock. The response to these commands always have an associated payload, which may span across multiple packets.
- Events – These are asynchronous events that the lock sends to LMS when certain conditions occur and LMS needs to be notified about the condition. The events have a payload that is limited to a single packet.

There are a few commands that do not fall into any one of the above categories. These commands are specifically identified later in the document, along with details of command execution.

3.2.1.1 Control Command

Control commands are single packet commands without any payload. Few examples of control commands are - Open door, Change mode, Flash Green/Red LED.

The initiator sends the ORP command and on successful execution, the responder responds with an ORP ACK packet. This is shown in Figure 3-1.

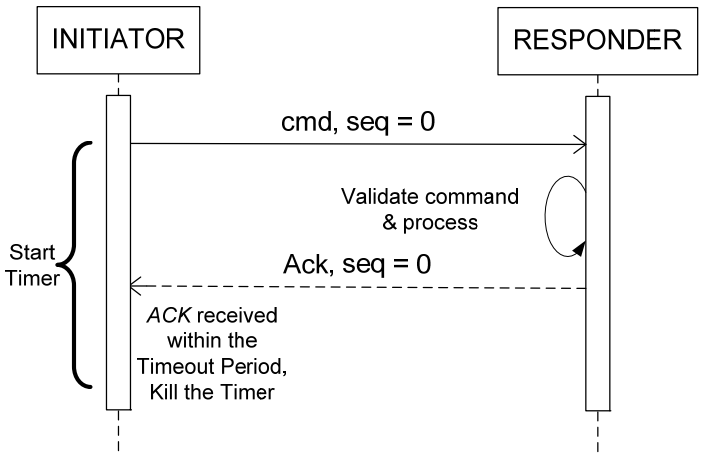

Figure 3-1 Control Command - Successful Execution

If an ACK is not received within the timeout period the command is retried. This is shown in Figure 3-2. The numbers of retries are configurable from 1-10.

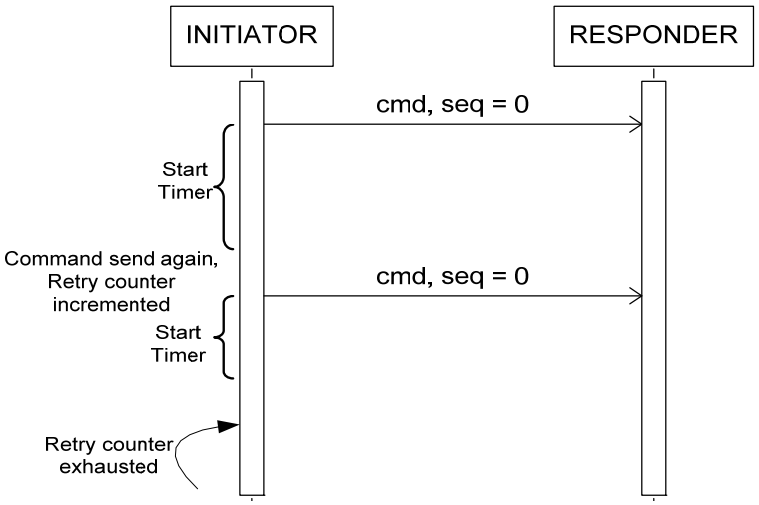

Figure 3-2 Timeout waiting for *ACK*

The responder sends a NACK packet in response to a command that is either invalid or not executed for some reason. The sub command in the NACK packet provides further details about the NACK reason. Some NACK packets may also have associated payload. These are detailed in specific commands.

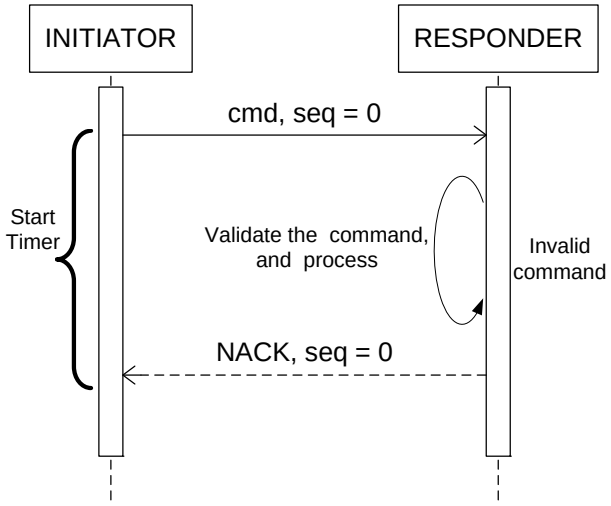

Figure 3-3 *NACK* response to a command

3.2.1.2 Request data Command

For request data commands, the responder sends an ACK with payload. This ACK is acknowledged with an ACK by the initiator. Few examples of request data commands are - Get Battery Level, Read ACU Lock Info, Get Dead Bolt Status.

Figure 3-4 and Figure 3-5 show the sequence of successful execution of a request data type command, with single and multiple packets respectively.

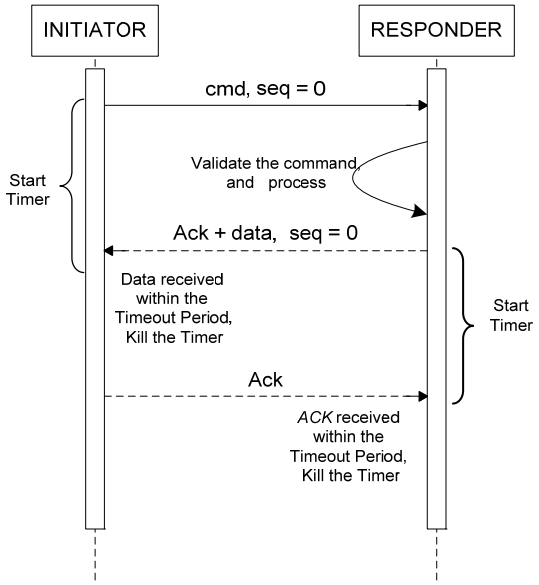

Figure 3-4 Request Data - Successful Execution

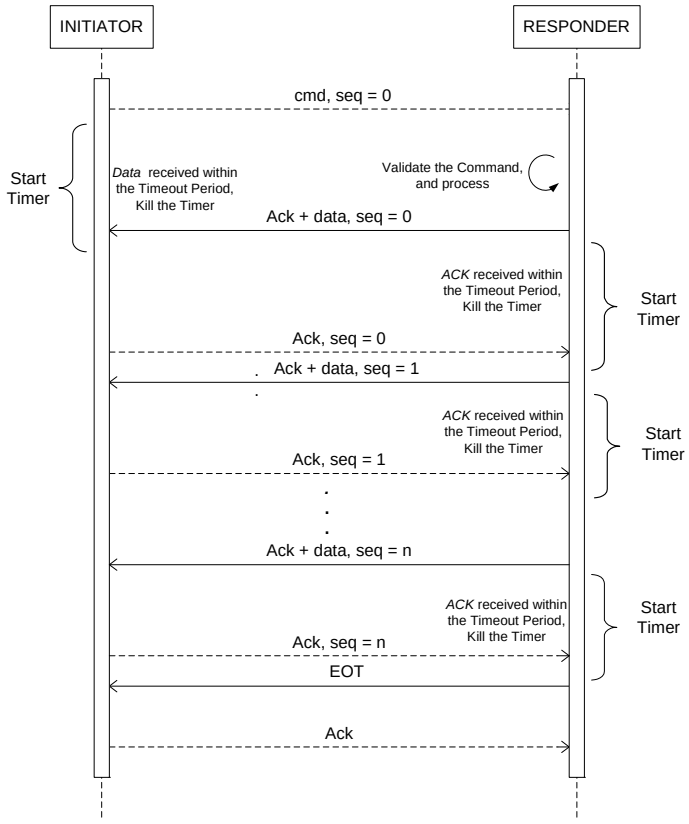

Figure 3-5 Request Data - Multi-packet successful Execution

If the ACK containing data from the responder is not received within the timeout period, the command is retried. This is shown in Figure 3-2. If the ACK to the ACK+data is not received within the timeout period, then the ACK + data is retried, as shown in Figure 3-6

If the command is not valid, or not executed for some reason, the responder sends a NACK with sub command ID set appropriately to indicate the reason for NACK, as shown in Figure 3-3. The sub command IDs for NACK are described in Table 5-1.

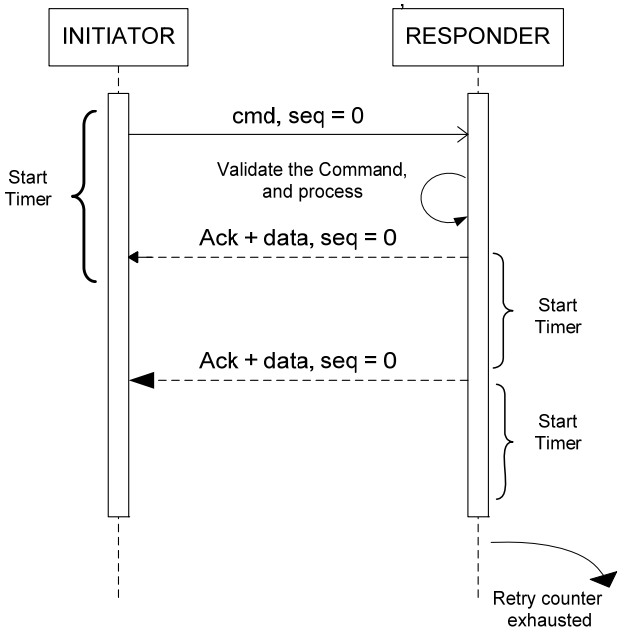

Figure 3-6 No ACK to ACK containing Data

3.2.1.3 Send Data Commands

For a Send Data command, the requestor sends data along with the command packet and waits for an ACK. If the data is more than the maximum ORP data size, it is sent in multiple ORP command packets. The successful execution flow is depicted in Figure 3-6 and Figure 3-7.

Some examples of Send Data commands are – Update Lock, Modify Timezone, Add User etc.

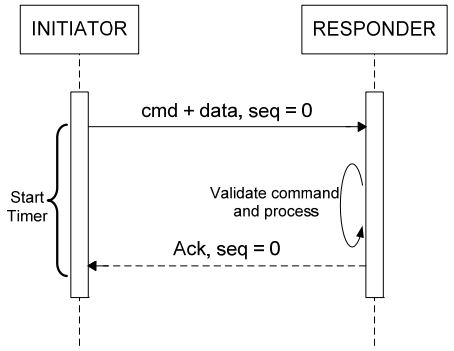

Figure 3-7 Send Data - Successful Execution

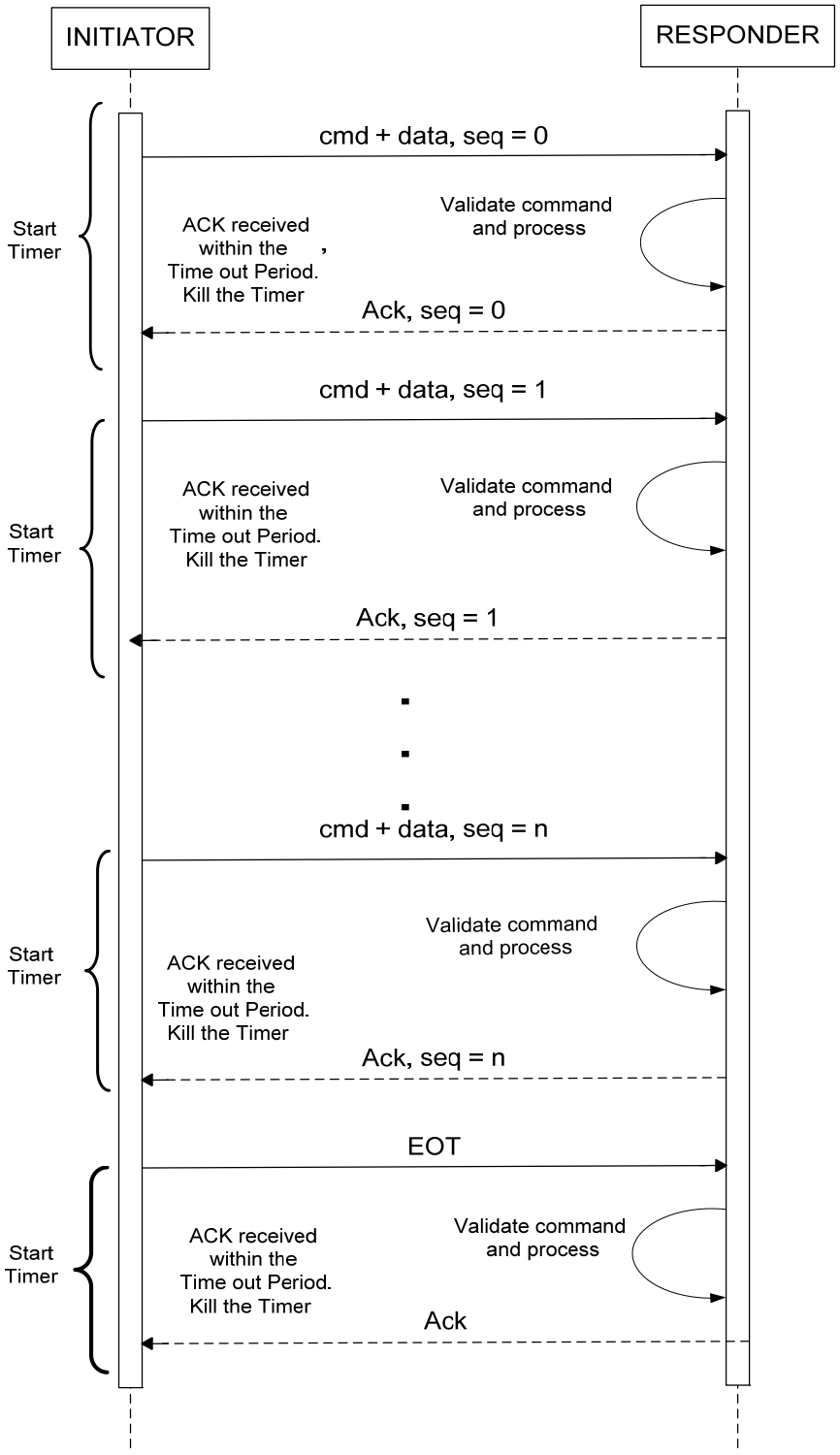

Figure 3-8 Send Data - Multiple Packets Successful Execution

If the ACK from the responder is not received within the timeout period, the initiator retries the command as shown in Figure 3-2 and Figure 3-9.

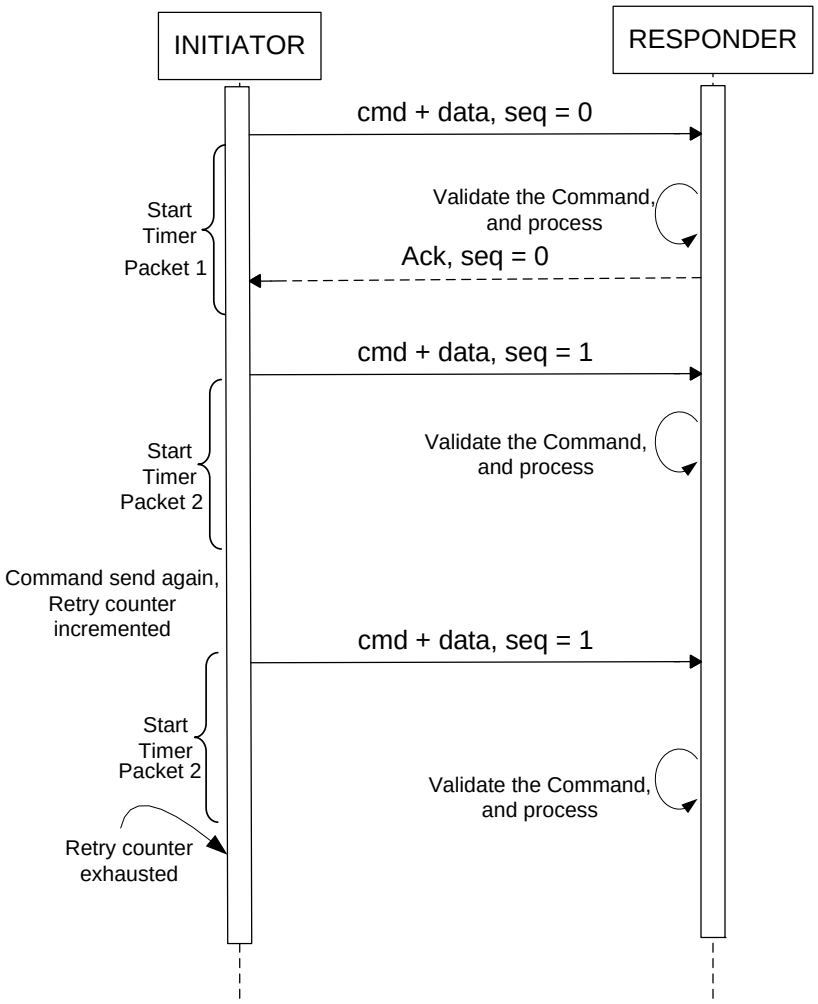

Figure 3-9 Send Data - ACK missing

3.2.1.4 Events

Events are sent from the lock to LMS. There are no events between lock, reader and PDA. They follow the same flow as the Send Data commands. Some examples of events are - Door Status Change Event, Dead Bolt status Change Event, Access Denied Event, Audit Write Event etc.

3.2.2 Commands List

Command	Command ID	Sub Command	Type	Reader	WLM	LMS	PDA	PTE	Encoder
Identification	0x01	0x00	Special	x	x		x		
Operational Parameters	0x02	0x00	Special	x	x		x		
Read Audit Trail	0x03	0x02	Request Data	x		x	x		x
Data	0x05	0x00 - Valid Data 0x58 - SCF, Invalid Data 0x59 - SCF, Invalid Authentication 0x5A - SCF, Invalid Location 0x5B - SCF, Invalid Card 0x5C - SCF Not Found	Special	x					
Acknowledge (ACK)	0x08	0x01 - Command Executed 0x02 - Data Received	Acknowledgement	x	x	x	x	x	x
No Acknowledge (NACK)	0x09	Refer Section 5.1	Negative Acknowledgement	x	x	x	x	x	x
End Of Transmission	0x0B	0x00	Control	x	x	x	x	x	x
Firmware Upgrade	0x0C	0x00 – ACU 0x01 – MiFARE 0x02 – iClass 0x03 – AWID	Send Data	x		x	x		
Open Door	0x0E	0x00	Control			x	x		
Change Mode	0x0F	0x01 - Office 0x02 - Office First 0x04 - Standard 0x07 - Blocked 0x08 - Emergency Lock 0x09 - Emergency Unlock 0x0A - Facility / Foyer	Control			x	x		
Get Battery Level	0x10	0x00	Request Data			x	x		
Read Lock Info	0x11	0x00	Request Data			x	x		
Configure Wireless Operational Parameters	0x12	0x00	Send Data		x				
LED & Buzzer Diagnostic	0x13	0x00	Request Data				x		
Write NWK Data to EEPROM	0x16	0x00	Send Data		x				

Command	Command ID	Sub Command	Type	Reader	WLM	LMS	PDA	PTE	Encoder
Flash Green/Red LED	0x17	0x00 - Red 0x01 - Green	Control		x		x		
Update Lock	0x19	0x00 – Door & Site Configuration 0x01 – User Data 0x02 – DST Information 0x03 – Holidays 0x04 – Time Zones 0x05 – Automatic Changes 0x06 – SCF 0x07 – ACF	Send Data			x	x		
Update ACU Clock(RTC)	0x1A	0x00	Send Data				x		
Read From EEPROM	0x1D	0x00	Request Data						
Read RTC Info	0x1E	0x00	Request Data				x		
Add / Update Users	0x1F	0x00	Send Data			x			
Delete Users	0x20	0x00	Send Data			x			
Update DST	0x21	0x00	Send Data			x			
Modify Time Zones	0x22	0x00 – Modify Entire Time Zone Table 0x01 – Modify Time Zone Table with Index	Send Data			x			
Write Door CFG	0x24	0x00	Send Data			x			
Change Automatic Changes	0x25	0x00	Send Data			x			
Modify Holiday Table	0x28	0x00	Send Data			x			
Read Lock Type	0x2B	0x00	Request Data						
Sleep	0x33	0x00	Control		x				
Sound Buzzer (High/Low)	0x34	0x01 –High 0x00 – Low	Control				x		
Network Join	0x38	0x00	Send Data		x		x		
Test LMS Communication	0x39	0x00	Send Data		x		x		
Get Door Status	0x44	0x00	Request Data						
Get Dead Bolt Status	0x45	0x00	Request Data						
Open Door For Certain Time	0x46	0x00	Control						

Command	Command ID	Sub Command	Type	Reader	WLM	LMS	PDA	PTE	Encoder
Get Num of User, FW Version, RTC	0x47	0x00	Request Data						
Hello	0x48	0x00	Send Data	x	x		x	x	
Check Lock Mode	0x4A	0x00	Request Data				x		
Switch Test	0x4B	0x00	Request Data				x		
Send System Code	0x4C	0x00	Send Data				x		
Send Lock ID	0x4D	0x00	Send Data				x		
Get Lock Status	0x4E	0x00	Request Data						
Reset	0x4F	0x00	Control	x	x				
Activate All	0x50	0x00	Control					x	
VANA	0x51	0x00	Control					x	
End of Test	0x52	0x00	Send Data					x	
Update ACF	0x60	0x00	Send Data			x			
Update SCF	0x61	0x00	Send Data	x		x			
Read Lock Operational Cycles	0x62	0x00	Request Data				x		
Send Events to OGACS	0x64	0x00	Send Data			x			
Request Clock (RTC) Command	0x65	0x00	Send Data			x			
Enable/Disable Communication of Events Command	0x66	0x00	Send Data			x			
WLM Firmware Upgrade	0x67	0x02 – FW_UPGRADE_INIT 0x03 – W_UPGRADE_ FRAME	Send Data				x		
Firmware Upgrade Success	0x68	0x00 – WLM FW 0x01 – ACU FW 0x02 – Reader FW	Send Data			x	x		
Start range verification	0x69	0x00	Control		x				

Table 3-3 ORP Command ID and Sub Command ID

4 Command Descriptions

4.1 Identification

The "Identification" process is a validation point. Without the Identification being successful, the WLM/Reader/PDA/PTE devices can not execute any commands with ACU/CM.

The identification command will be triggered when there is a Reset in any of the following devices: Control Module, WLM, or Reader.

Reset in the devices can happen in the following scenarios:

- On power up (Power on reset)
- Hardware Reset
- Software Reset due to Watchdog/exception in the code.

If Control Module reset happens, the ORP supported peripheral devices (WLM or Reader) have to be identified by the Control Module. To initiate the identification sequence, the control module shall send *Reset* command to the peripheral devices.

If reset happens in the WLM or Reader, these devices will send the Hello command (refer section 3.5) requesting for the identification to Control Module.

Control Module Identification with PDA will happen on specific command request from PDA,.

4.1.1 Identification: CM - WLM

To Initiate Identification with the WLM, the CM/ACU shall send *Reset* command (refer section 4.7) to WLM to induce forced reset. After sending ACK as response to Control Module, WLM shall undergo a reset and shall send the Hello command (refer section 4.5) requesting the identification.

On receiving the Hello command requesting the identification, Control Module shall send ACK response to the WLM followed by an identification sequence.

The Control Module shall send the *Identification* command along with additional information (interim data as payload) to the WLM. The payload of Identification packet shall contain the device ID for the control module.

After successfully validating the command, WLM shall act upon interim data and send response with the additional information (response interim data as payload) to ACU. The payload of the response packet contains the WLM information, including its device ID, firmware version and hardware version.

The response interim data shall be evaluated by the Control Module. If it matches, the Control Module sends the *Operational Parameters* to the WLM. The *Operational Parameters payload* consists of the number of Retries and Timeout. On receiving the *Operational Parameters,* the WLM validates the payload and sends an ACK to Control Module; else it sends a NACK with the appropriate error code. Please refer to section 5.1 for Error Codes.

After the ACK for the *Operational Parameters* is received, the Control Module sends the *Wireless operational parameter*s to WLM. The *Wireless operational parameter*s consist of Site Code, Lock Id, HB Rate, RF O/P Power, Channel ID, and FA Mode. On receiving the *Wireless operational parameters,* the WLM validates the parameters and sends an ACK to Control module.

Then the WLM initiates the process to join the WAP Network, NWK Join Process. If the join is successful, WLM initiates a "Write NWK Data to EEPROM" command to write the NWK Code to the ACU EEPROM. On receiving the Write NWK Data to EEPROM command*,* CM validates the data and sends an ACK to WLM.

Then the WLM then sends a Heart Beat (HB) to WAP. If WLM receives an HB_ACK for the first Heart Beat, it sends "Flash Red/Green LED" command to the ACU to flash Green LED. If HB_ACK for the first Heart Beat is not received before timeout, WLM sends "Flash Red/Green LED" command to the ACU to flash RED LED

indicating the failure of the network join process. Figure 4-1 shows the sequence of the initialization between WLM and lock control module.

If ACK is not received or NACK is received for wakeup signal or any of the intermediate commands (reset, operational parameters, hello, identification), then the wakeup signal or the command is retried until the retries are exhausted. If any failure in the NWK Join Process (indicated by ACU RED LED), NWK_Join command can be issued from PDA to re-initiate the join process, via Control Module.

After a soft reset, the WLM sends the Hello command to the CM to start the identification sequence. After a power on reset, the WLM waits for the CM to send the Reset command. If WLM times out waiting for the Reset command, it sends the Hello command to initiate the identification.

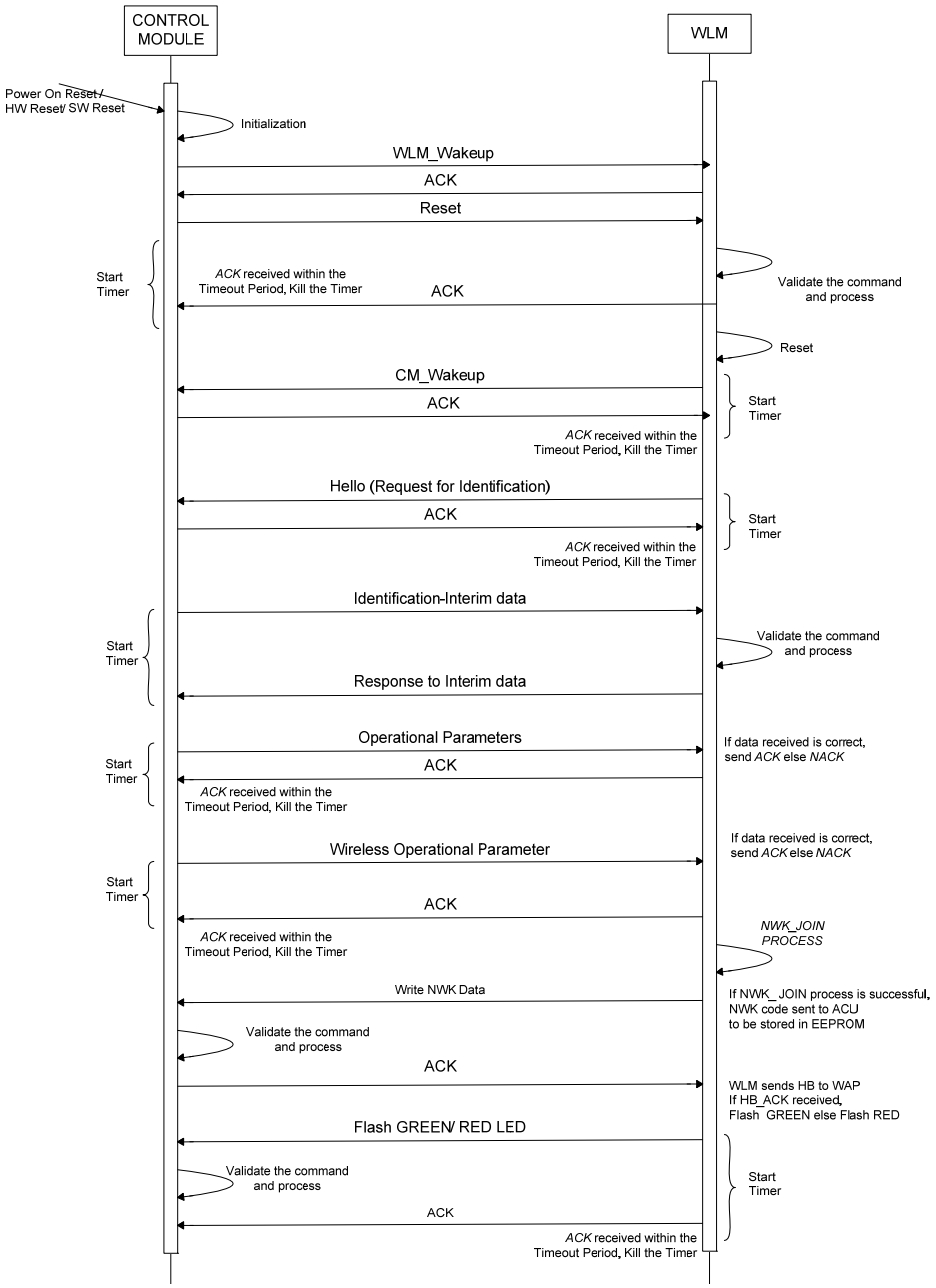

Figure 4-1 Identification: CM - WLM

Initiator (Identification Command for WLM Sent from CM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload: ACU Device ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	1 Byte	2 Bytes
0x0A	0x01	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer **Error! Reference source not found.**	Refer ORP Packet Structure

Responder (ACK from WLM - Command Executed – Response to Identification Command)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	17 Bytes	2 Bytes
0x0A	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload

WLM Device ID	Firmware Version	Hardware Version
1 Byte	6 Bytes	10 bytes
Refer **Error! Reference source not found.**		

Operational Parameters Packet (Sent from CM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes	2 Bytes
0x0B	0x02	0x00	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Please Refer below	Refer ORP Packet Structure

Payload

No. Of Retries	Timeout(sec)
1 Byte	1 Byte

Responder (ACK from WLM - Received Data)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Wireless Operational Parameters Packet (Sent from CM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	15 Bytes	2 Bytes
0x18	0x12	0x00	0x0002	Refer ORP Packet Structure	Refer ORP Packet Structure	Please Refer below	Refer ORP Packet Structure

Payload

Site Code	Lock Id	HB Rate	RF O/P Power	Channel ID	FA Mode
4 Bytes	4 Bytes	4 Bytes	1 Bytes	1 Bytes	1 Bytes

Responder (ACK from WLM - Received Data)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0002	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Write NWK Data to EEPROM (Sent from WLM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	8 Bytes	2 Bytes
0x11	0x16	0x00	0x0000	Refer ORP	Refer ORP Packet	NWK Data	Refer ORP Packet

				Packet Structure	Structure		Structure

Responder (ACK from CM - Command Executed Write NWK Data to EEPROM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Flash Green/RED LED (Sent from WLM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x17	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-1 Identification Command Packet & Response of WLM

If no ACK is received for the identification command or the operational parameters, within the timeout period or no operational parameter command is received from CM in response to interim data, then the respective commands are retried, until the retry count is exhausted.

4.1.2 Identification of Reader

When it is desired to initiate identification with the Reader, Control Module shall send *Reset* command (section 4.6) to Reader to induce forced reset. After sending ACK as response to Control Module, Reader shall undergo a reset and shall send the Tarj signal. After getting the ACK for Tarj signal, Reader shall send Hello command (section 4.5) requesting the identification.

On receiving the Hello command requesting for the identification, Control Module shall send ACK response to the Reader followed by an identification sequence.

The Control Module shall send the *Identification* command along with additional information (interim data as payload) to the Reader. The payload of Identification packet shall contain the device ID of the ACU.

After successfully validating the command, Reader shall act upon interim data and send response with the additional information (response interim data as payload) to ACU. The payload of the response packet contains

the reader information including the device ID, manufacturing timestamp, serial number, firmware version and hardware version.

The response interim data shall be evaluated by the Control Module. If it matches, the Control Module sends the *Operational Parameters* to the Reader. The *Operational Parameters payloads* consists of number of Retries and Timeout. On receiving the *Operational Parameters,* the Reader validates the payload and sends an ACK to Control module, else it sends a NACK with the appropriate error code. Please refer to section 5.1 for Error Codes.

Figure 4-2 shows the sequence of commands executed during identification of reader and ACU.

The retry logic is similar to that the identification logic between ACU and WLM. If ACK is not received for any commands, the command is retried until the retry count is exhausted.

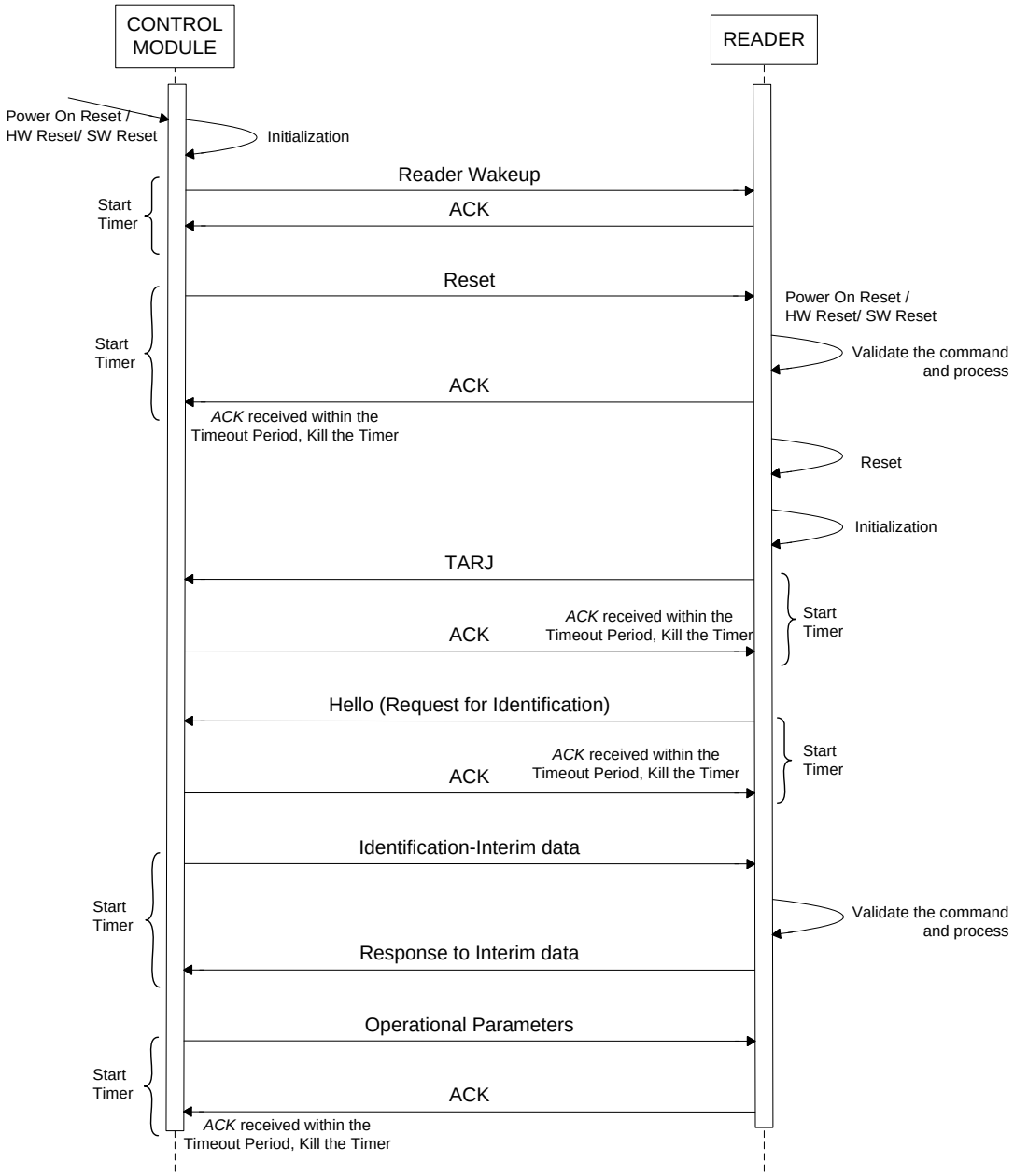

Figure 4-2 Identification Command: ACU - Reader

Initiator (Identification Command for reader sent from CM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload: ACU Device ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	1 Byte	2 Bytes
0x0C	0x01	0x00	0x0000	Refer ORP Packet	Refer ORP Packet	Refer **Error!**	Refer ORP Packet

				Structure	Structure	**Reference source not found.**	Structure

Responder (ACK from WLM - Command Executed – Response to Identification Command)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload–Interim Data	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	36 Bytes	2 Bytes
0x0C	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please Refer Below	Refer ORP Packet Structure

Payload

Reader Device ID	Manufacturing Timestamp	Firmware Version	Hardware Version	Reader Board Serial Number
1 Byte	5 Bytes	4 Bytes	10 bytes	16 Bytes
Refer **Error! Reference source not found.**				

Operational Parameters Packet (Sent from CM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes	2 Bytes
0x0B	0x02	0x00	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Please Refer below	Refer ORP Packet Structure

Payload

No. Of Retries	Timeout(sec)
1 Byte	1 Byte

Responder (ACK from WLM - Received Data)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum

1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-2 Identification Command: ACU – Reader (Packet & Response of Reader)

4.2 Acknowledge (ACK)

An ACK is sent upon successful reception of data/command OR upon successful execution of command. The sub command IDs for the ACK command are described in table below.

Sub Command ID	Description
0x01	Command Executed
0x02	Data Received

4.3 No Acknowledge (NACK)

An NACK is sent upon no reception of data/command OR upon unsuccessful execution of command.

Note: If an ACK/NACK is not received within the specified timeout period, the command shall be sent again. The number of retries are configurable from 1-10.

4.4 End of Transmission

This packet is sent at the end of command/response whenever payload of command/response is more than one packet length. If payload of a command/response is not more than one packet, “End of Transfer” packet will not be sent.

4.5 WLM / Reader Hello Command

Hello command will be sent from Reader or WLM to ACU requesting to initiate a command (e.g. identification command). Also this command can be used to wakeup ACU before peripherals initiates any command in the absence of wakeup signal. If an ACK is not received within the specified timeout period, the command shall be retried by Reader or WLM until the retry count is exhausted.

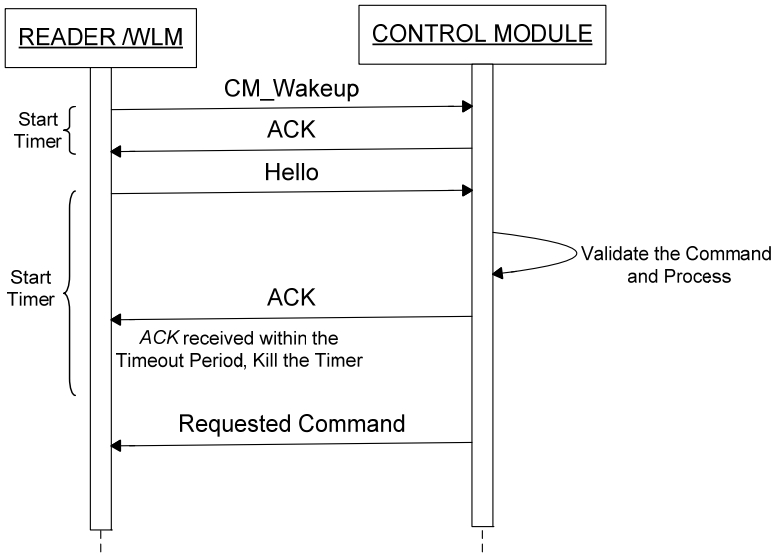

Figure 4-3 Hello Command – Reader / WLM (Successful Execution)

(Hello Command Sent from Peripheral device)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes	2 Bytes
0x0B	0x48	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload

Requested Cmd ID	Sub Cmd ID
1 Byte	1 Byte 0 – Normal reboot 1 – FW Upgrade from LMS 2 – FW Upgrade from PDA

ACK for Hello Command Sent by CM to WLM/Reader

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-3 Hello Command Packet Format

If the ACU does not respond to the wake-up signal (TARJ or CM_Wakeup), or the Hello command, the command is retired until the retry count is exhausted. If the Hello command is not valid, or if the ACU cannot execute the command for any reason, the ACU will respond with a NACK.

4.6 Reset Command

Control Module Reset can happen during one of the following:

- On power up (Power on reset)
- Hardware Reset
- Software Reset due to Watchdog/exception in the code.

Any of the above Control Module reset trigger or NWK_Join command received from PDA (only for WLM), shall reset the other ORP devices like WLM or Reader.

When it is desired to send Reset command from Control Module to ORP devices like WLM or Reader, the WLM *Wakeup / Reader Wakeup* signal is pulled high. The Control Module receives acknowledges to signal. After the *ACK* is received within the timeout period the control module shall pull the WLM *Wakeup / Reader Wakeup* signal low.

Reset command shall be initiated from Control Module to ORP supporting devices to induce a forced reset on that device. After sending ACK as response, corresponding device shall undergo a reset and shall send the *Hello* command to Control Module. On receiving the *Hello* command, Control Module shall send ACK response to the WLM/Reader followed by further steps of identification sequence. (refer section 3.1).

Reset command from CM

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x4F	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

ACK from WLM/Reader

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-4 Reset Packet Format

4.7 Data

This command is sent from the Reader Module to the Control Module. When a valid card is detected in the proximity of the reader and is read successfully OR a successful *read* operation is executed, the Reader Module shall forward the data to the Control Module.

When a card is detected by the Reader Module it shall try to read the card and validate the data. If reader module is unable to read the card or validate the data, it will send Data command to Control Module with appropriate sub command ID to indicate the failure.

If the card is validated, the Reader Module shall read the data contained in the card. The Reader Module shall then interrupt the Control Module using the *TARJ* signal. After an ACK is received the Reader Module shall then send the *Data* packet to the Control Module/Encoder. If the ACK from the Control Module/ Encoder is not received within the timeout period the *TARJ* signal is sent again. The number of retries is configurable from 1-10.

The Control Module/Encoder acknowledges the Reader Module after receipt of the *Data* packet. If the Reader Module doesn't receive the ACK from the Control Module/Encoder within timeout, it sends out the *Data* packet once again [
Figure 4-5]. The number of retries is configurable from 1-10. The data transfer is terminated by sending the End of Transmission packet.

Sub command ID	Details
0x00	Valid Data
0x58	SCF – Invalid Data
0x59	SCF – Invalid Authentication
0x5A	SCF – Invalid Location
0x5B	SCF – Invalid Card
0x5C	SCF Not found

Table 4-5 Sub Command IDs for Data command

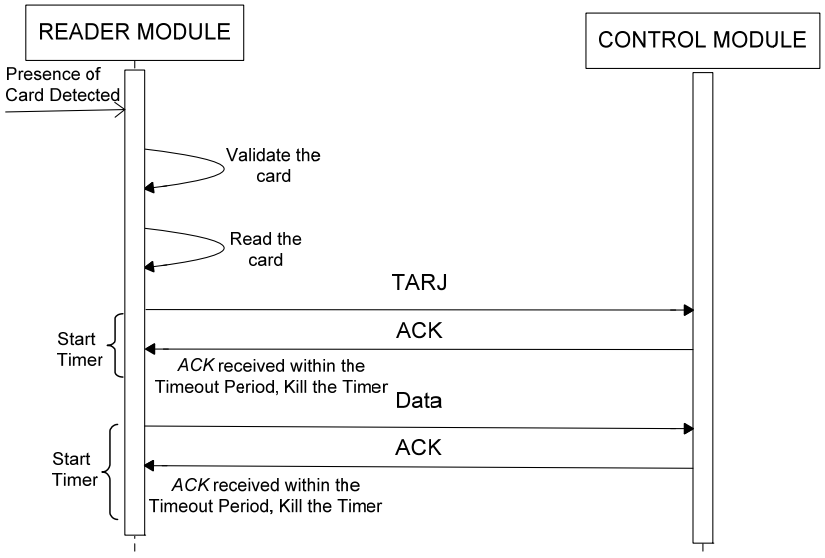

Figure 4-4 Data Command (Successful Execution)

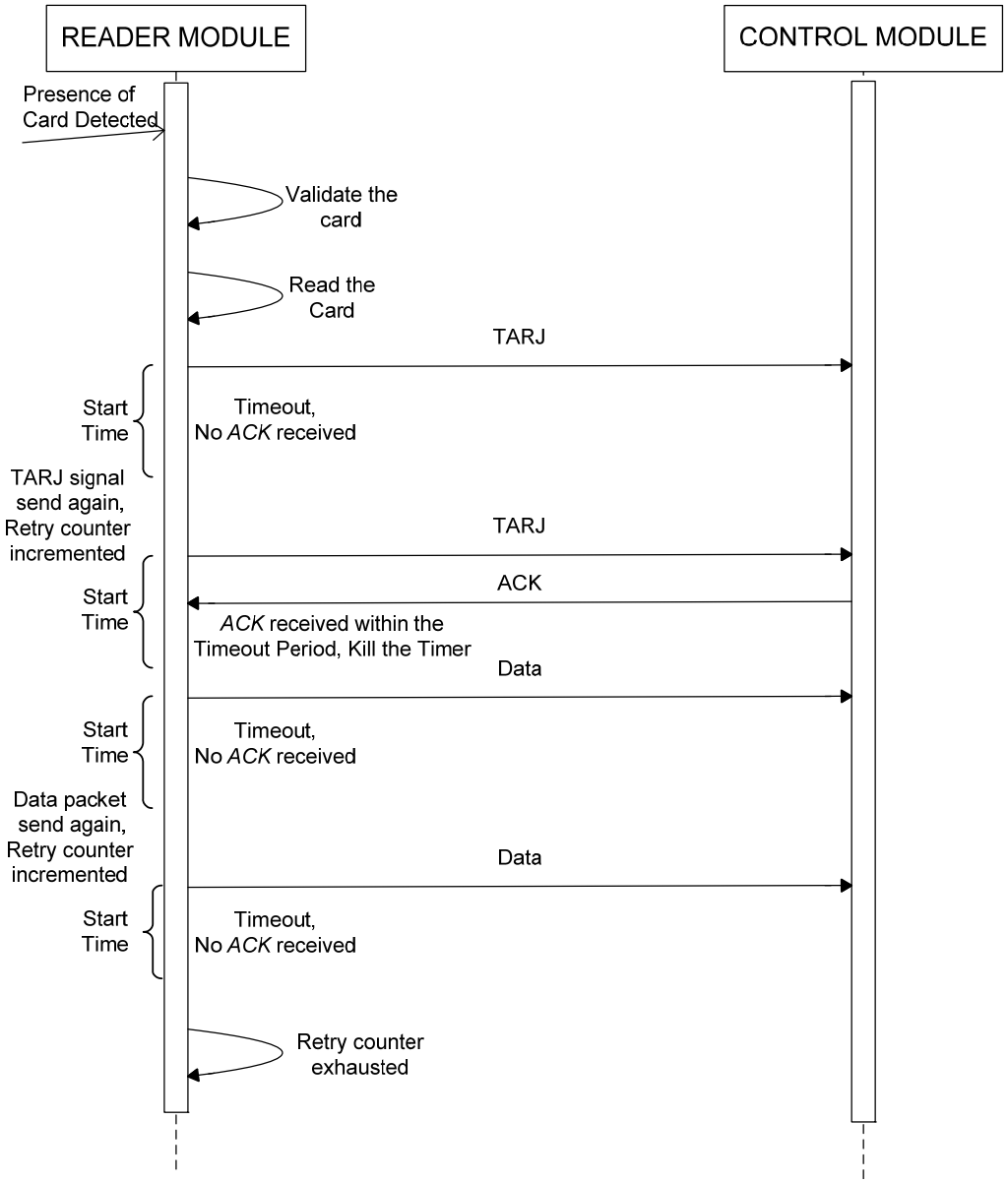

Figure 4-5 Data Command (Missing ACK for TARJ and Data)

4.8 Open Door

This command can be used from LMS or PDA to unlock the lock.

Initiator (Open Door Command Sent from LMS through WLM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x0E	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	TBD

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-6 Open Door Packet format

4.9 Change Mode

This command can be used from LMS or PDA to change the lock operation mode.

When lock is in blocked mode, LMS or PDA can issue a forced office sub command to enter in to office mode.

Initiator (Change Mode Command Sent from LMS through WLM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x0F	Refer Below	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-7 Change Mode Packet format

Sub command id	Modes
0x01	Change to Office
0x02	Office First
0x04	Change to Standard
0x07	Change to Blocked
0x08	Emergency Lock
0x09	Emergency Unlock
0x0A	Facility Code/ Foyer Mode

Table 4-8 Sub Command IDs

4.10 Flash Green/Red LED

This command can be used from WLM to flash LEDs to indicate a successful or failed join attempt.

Initiator (Flash Green/Red Command Sent from WLM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x17	0x00 - Red 0x01 - Green	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-9 Flash Green/Red Command format

4.11 Sound Buzzer (High/Low)

Initiator (Sound Buzzer (High/Low) Command Sent from LMS*)*

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x34	0x01 –High 0x00 – Low	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-10 Sound Buzzer (High/Low) Command format

4.12 Open Door for Certain Time

*Initiator (*Open Door for Certain Time *Command Sent from LMS)*

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Byte	2 Bytes
0x0B	0x46	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Period in sec	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	TBD

Table 4-11 Lock or Unlock Packet format

4.13 LED & Buzzer Diagnostic

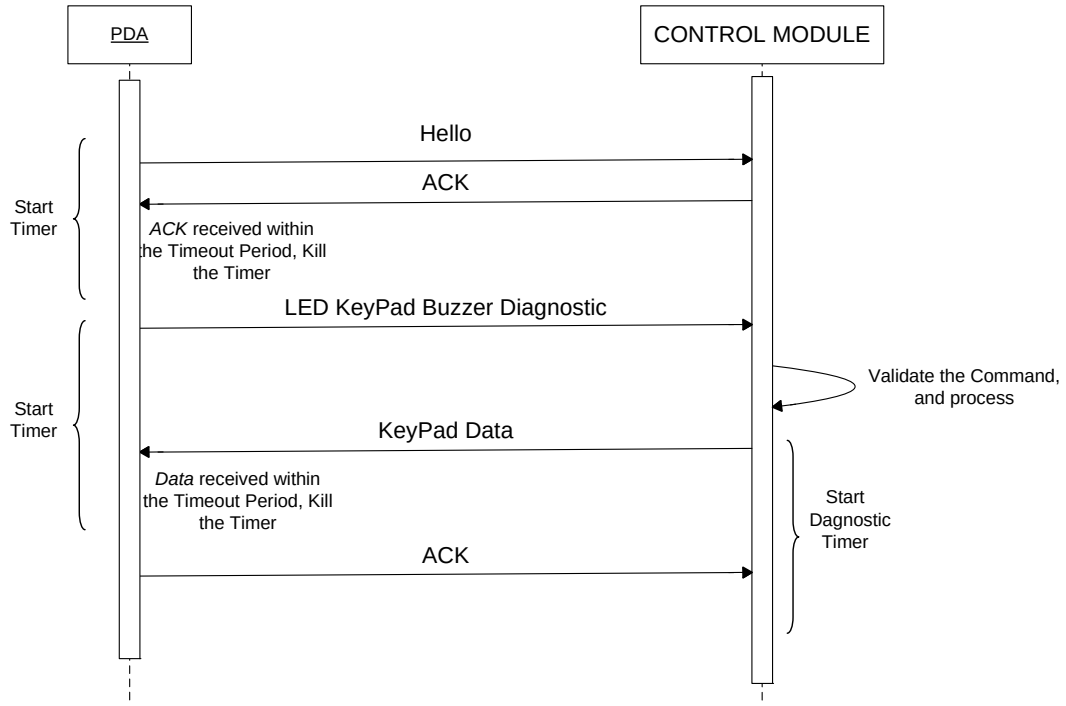

Figure 4-6 LED & Buzzer Diagnostic (Successful Execution)

Initiator (LED Buzzer & Keypad Diagnostics Command Sent from PDA)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x13	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Stop (LED Buzzer & Keypad Diagnostics Stop Command Sent from PDA in between the command)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x13	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed Keypad Data Sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload Keypad Data	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	1 Byte	2 Bytes
0x0A	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Payload

Keypad Data
1 Byte

Responder (ACK from PDA)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-12 LED & Buzzer Diagnostic packet format

The following figure shows the Negative Flow of the LED, Keypad & Buzzer Diagnostics

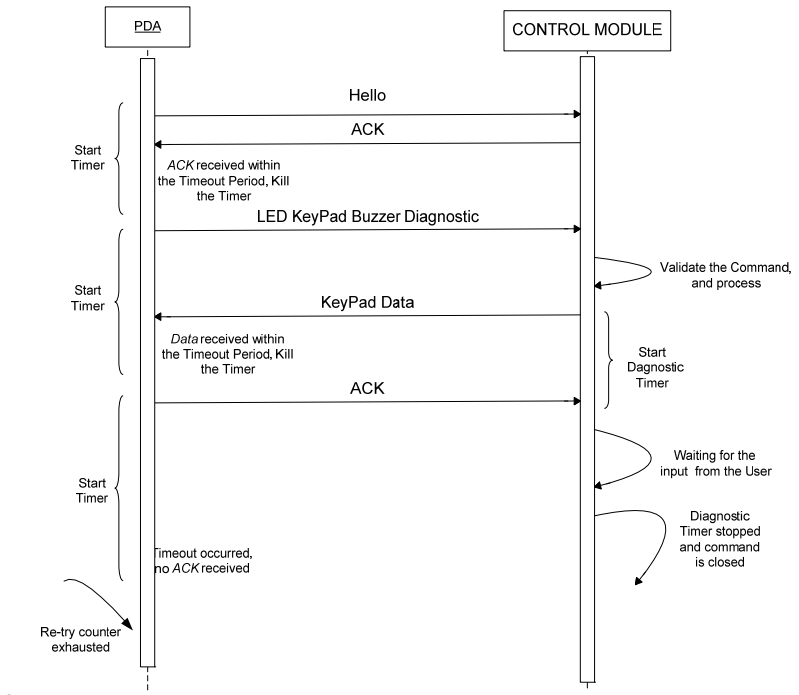

Figure 4-7 LED, Keypad & Buzzer Diagnostics (Negative Flow)

The following diagram shows the successful execution of LED, Keypad & Buzzer Diagnostics with Stop command sent from PDA.

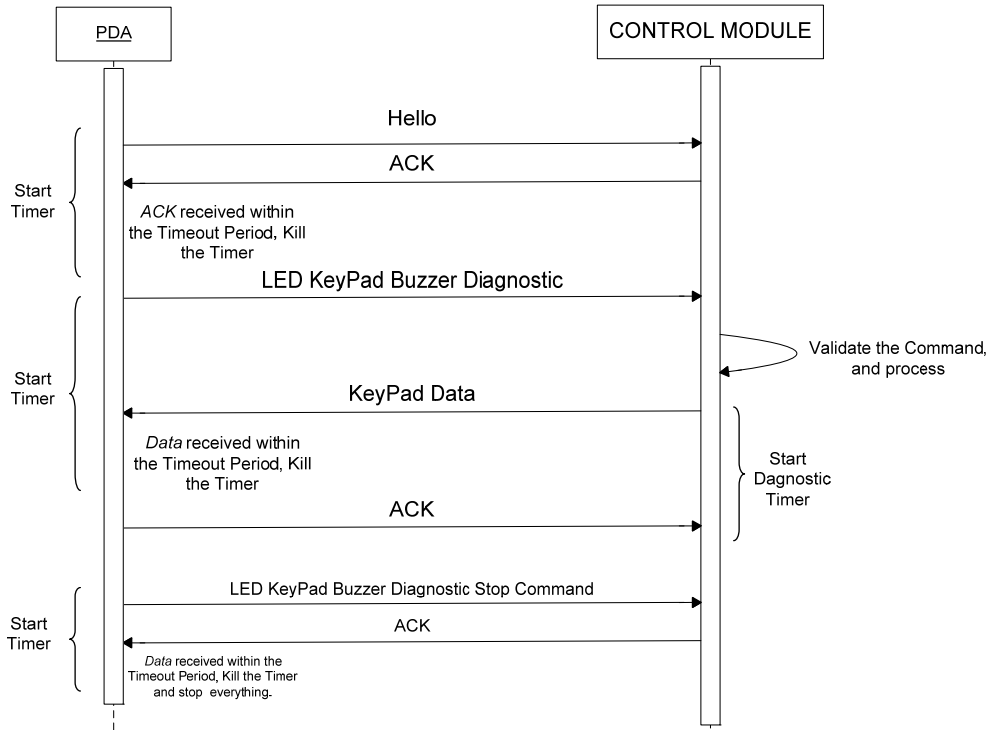

Figure 4-8 LED, Keypad & Buzzer Diagnostics (Successful Execution)

4.14 Get Battery Level

The Battery Level information shall be embedded in the ACK packet as shown in Figure 3.14.2

Initiator (Get Battery level Command Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x10	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed, Battery Level Sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes	2 Bytes
0x0B	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Payload

Battery Level
2 Bytes

Example
Say the Battery Level to be sent is 75%, the Responder packet will be:

Responder (ACK from CM- Command Executed, Battery Level Sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Byte	2 Bytes
0x0B	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	0x004B	Refer ORP Packet Structure

Responder (ACK from LMS for Battery Level)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-13 Get Battery Level packet format

4.15 Read Lock Info

The Lock information shall be embedded in the ACK packet as shown in Fig.3.15.2.

Initiator (Read ACU Lock Command – Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x11	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed ACU Lock Info Packet 1 Sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	138 Bytes	2 Bytes
0x8F	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Payload for Read Lock Info

Manufacturing Time Stamp (ACU)	Lock ID	Firmware Version (ACU)	Hardware Version (ACU)	ACU Circuit Board Serial No.	Lock Name
5 Bytes	4 Bytes	4 Bytes	10 Bytes	16 Bytes	40 Bytes

Manufacturing Time Stamp (Reader)	Firmware Version (Reader)	Hardware Version (Reader)	Serial No. of the Reader Circuit Board
5 Bytes	4 Bytes	10 Bytes	16 Bytes

Firmware Version (WLM)	Serial Number (WLM)
6 Bytes (see below)	10 Bytes

Lock status	Door Status	Deadbolt Status	Battery Voltage Level	Current Lock Mode	Number Of Users
1 Byte	1 Byte	1 Byte	2 Bytes	1 byte	2 bytes
0 = Locked 1 = Unlocked	0 = Close 1 = Open	0 = Disabled 1 = Enabled	0 through 100%	See Table 4-7 Change Mode Packet	

				format	

WLM Firmware Version Format (displayed as Major.Minor.Build)

Major Version	Minor Version	Build Number
1 Byte	2 Bytes	3 Bytes

WLM Serial Number Format

Serial Number	Location Code	Date Code	HW Version	Reserved
3 Bytes	1 Bytes	2 Bytes	1 Byte	3 Bytes

The WLM serial number is displayed as Date Code (converted to decimal integer) followed by Location Code (ASCII digit) followed by Serial Number (converted to decimal integer) without any spaces between each. Currently the HW version and reserved bytes are always set to zero and should not be displayed.

Example:

WLM Serial Number : 80 47 03 4E 65 12 00 00 00 00

Serial Number : 0x034780
Location Code : 0x4E
Date Code : 0x1265

This should be displayed as : 4709N214912

CM and Reader Firmware Version:-
e.g. Firmware Version to be displayed as 1.4.2.0. It is transmitted as 0x01040200, in little endian format.

CM and Reader Hardware Version:- The data for Hardware version is sent in ASCII format with a NULL to indicate the end of data.

Serial No. of Circuit Board: The serial no. is stored in ASCII format without any NULL since the length will always be 16 characters.

Lock Name:- The data for Lock Name is sent in ASCII format with a NULL to indicate the end of data.

Responder (ACK from LMS for ACU Lock Info)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-14 Read ACU Lock Info packet format

4.16 Read from EEPROM (WLM Only)

Initiator (Read From EEPROM) Command Sent from WLM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x1D	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed Read From EEPROM Data Sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	8 Bytes	2 Bytes
0x11	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload

WAP ID	WAP Physical ID
4 Bytes	4 Bytes

Responder (ACK from WLM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-15 Read From EEPROM packet format

4.17 Read RTC Info

Initiator (Read RTC Info) Command Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x1E	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed Read RTC Info Sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	5 Bytes	2 Bytes
0x0E	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload-RTC Info

Year	Month	Day	Hour	Min	Sec	Unused
7 Bits	4 Bits	5 Bits	5 Bits	6 Bits	6 Bits	7 Bits

Responder (ACK from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-16 Read RTC Info packet format

4.18 Read Lock Type

Initiator (Read Lock Type Command Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x2B	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2Byte	2 Bytes
0x0B	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please Refer below	Refer ORP Packet Structure

Payload

Lock Type	Card reader Technology
1 Byte	1 Byte
Refer below	Refer below

Lock Type

Lock Type Bits	Lock Type
0x00	ACU

Card reader Technology

Value	Card Reader Technology
0x00	Magnetic
0x01	iCLASS
0x02	AWID / HID Prox

Responder (ACK from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x00	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-17 Read Lock Type Packet Format

4.19 Get Lock Status

Initiator (Get Lock Status Command Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x4E	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed, Lock Status sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	1 Bytes	2 Bytes
0x0A	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer Below	Refer ORP Packet Structure

Payload

Door Status
1 Bytes 0x01 :Unlocked 0x00:Locked

Example
Say the Lock Status is Unlocked , the Responder packet will be:
Responder (ACK from CM- Command Executed, Lock status Sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	1 Byte	2 Bytes
0x0A	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	0x01	Refer ORP Packet Structure

Responder (ACK from LMS for door status)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-18 Get Lock Status Packet format

4.20 Get Door Status

Initiator (Get Door Status Command Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x44	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed, Door Status sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	1 Bytes	2 Bytes
0x0A	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer Below	Refer ORP Packet Structure

Payload

Door Status
1 Bytes 0x01 :open 0x00:close

Example
Say the Door Status is open , the Responder packet will be:
Responder (ACK from CM- Command Executed Door status: Sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	1 Byte	2 Bytes
0x0A	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	0x01	Refer ORP Packet Structure

Responder (ACK from LMS for door status)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-19 Get Door Status Packet format

4.21 Get Dead Bolt Status

Initiator (Get Dead bolt Status Command Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x45	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed, Dead bolt Status sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	1 Bytes	2 Bytes
0x0A	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Payload

Door Status
1 Bytes 0x01 :enabled 0x00:disabled

Example
Say the *Dead bolt Status* is enabled , the Responder packet will be:
Responder (ACK from CM- Command Executed, Dead bolt Status Sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	1 Byte	2 Bytes
0x0A	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	0x01	Refer ORP Packet Structure

Responder (ACK from LMS for door status)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-20 Get dead bolt status Packet format

4.22 Get number of user, firmware version and RTC

When the LMS sends the command *Get number of user, firmware version and current time and date,* the Control Module shall validate this command. After successfully validating it, it shall then execute the command. An *ACK* shall be sent only after the command is successfully executed. Number of user present in the lock, firmware version and lock current date and time shall be embedded in the ACK packet. If an ACK is not received within the timeout period the command is sent again. The numbers of retries are configurable from 1-10.

Initiator (Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x47	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	11 Bytes	2 Bytes
0x14	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Payload

Number of user	Firmware Version	Lock current date and time
2 Bytes	4 Bytes	5 Bytes

Date and time bit format

Year	Month	Day	Hour	Min	Sec	Unused
7 Bits	4 Bits	5 Bits	5 Bits	6 Bits	6 Bits	7 Bits

Table 4-21 Get number of user, firmware version and current time and date packet format

Firmware Version Example:-
Firmware Version to be displayed as 1.4.2.0. It is transmitted as 0x01, 0x04, 0x02, and 0x00

4.23 Read Audit Trail

The sequence numbers for the packets below (in the packet format) are given based on the assumption that there is only one packet for each of the Audit Trail payload. However there could be more packets and the sequence numbers have to be updated accordingly.

Initiator (Read Audit Trail Command Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x03	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed Audit Trail Data Sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload Audit Trail	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Total audit bytes + 4 Bytes	2 Bytes
Payload length + 9	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Payload for Read Audit Trail response

No. Of Records	Badge ID Length (in bytes)	Issue code length (in bytes)	Audits
2 Bytes	1 Byte	1 Byte	No. of audit records bytes Refer below for one audit record format

One audit record format

Event ID	Year	Month	Day	Hour	Min	Sec	Unused	Audit Source	User Id	Issue Code
1 byte	7 Bits	4 Bits	5 Bits	5 Bits	6 Bits	6 Bits	3 Bits	4 bits	2-8 Bytes (variable)	1-4 Bytes (variable)

Audit Source Format

Audit Source	Description	Details
0x00	Unkown	-
0x01	Event generated due to WLM command	User Id is not valid and will have default value for user ID (0x00000000)

Audit Source	Description	Details
0x02	Event generated due to PDA command	User Id contains the PDA operator Id
0x03	Event generated due to CM Functionality	User Id contains the Badge/User Id of the card. Automatic events (Non card audit in CM) will have default value for user ID (0x00000000)

The event “RTC update” audit has extra 5 bytes for old timestamp.

The firmware upgrade events (ACU firmware upgraded, Reader firmware upgraded, WLM firmware upgraded) has extra 6 bytes for new firmware version. The firmware version format is same as in *Payload for Read Lock Info* command. For the ACU and Reader firmware version, the first 4 bytes will contain the firmware version and the last 2 bytes shall be zero.

Responder (ACK from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (EOT sent from CM in case of Multiple packet)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x0B	0x00	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from LMS for EOT sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-22 Read Audit Trail packet format

4.24 Sleep

This command is used by the WLM to request ACU to enter the low power mode.

Initiator (Sleep Command Sent from WLM)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x33	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	TBD

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-23 Sleep Packet format

4.25 Update Lock

If the Update Lock command packet payload exceeds 128 bytes, it is broken down into multiple packets by the front end and sent via the WLM to the lock .Therefore the next command packet is sent by the WLM after ACK is received for the previous one. The Control Module expects a packet to be sent to it until there is an EOT packet from LMS.

The Lock Data payload consists of

- Lock Configuration and data
- Site Details
- User Details
- DST Details
- Holidays
- Time Zones
- Automatic changes
- ACF information
- SCF information

The Lock Configuration Data and Site Details are sent in first packet
The User Details is sent in multiple packets if its payload (including user count) exceeds 128 bytes.
The DST Details is sent in multiple packets if its payload (including DST count) exceeds 128 bytes.
The Holidays is sent in multiple packets if its payload (including holiday count) exceeds 128 bytes.
The Time Zones is sent in multiple packets if its payload (including timezone count) exceeds 128 bytes.
The Automatic Changes is sent in multiple packets if its payload (including automatic changes count) exceeds 128 bytes.

The ACF details are sent in a single packet with maximum payload of 109 bytes.

The SCF details are sent in a single packet with maximum payload of 45 bytes.

For the User Details, DST, Holidays, Time Zones and Automatic Changes the first 2 bytes of the payload is the total number of records. For ACF and SCF updates, the first one byte is the total number of records. Based on the number of records field in the payload it can be determined if single or multiple packets are expected. In case of multiple packets, the first packet will contain the 2 bytes of number of records information and 126 bytes of payload information and rest of the packets will have only the payload information spilt to fit the maximum size of payload (128).

If ACU/WLM communication parameters or wireless operational parameters get updated as part of Update Lock operation from LMS or PDA, the lock ACU sends the new values to WLM using the Operational Parameters command or the Configure Wireless Operational parameters command respectively. These commands are described in the ACU – WLM Identification [section 4.1.1]. The exception to this are the channel ID, FA mode and output power parameters within the door configuration packet. If these fields are changed from LMS, then the ACU ignores these fields, does not update them and does not propagate them to WLM. These fields can only be modified through PDA.

The sequence numbers for the packets below (in the packet format) are given based on the assumption that there is only one packet for each of the above given Lock Data payload. However there could be multiple data packets and the sequence numbers have to be updated (incremented) accordingly.

Initiator (Update Lock Command Sent from LMS – Packet 1, Door and site configuration)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	60 to 80 Bytes	2 Bytes
Payload length + 9 bytes	0x19	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please read below	Refer ORP Packet Structure

The payload for the door and site configuration is same as the payload for write door config command [section 4.32]. Please refer *Payload- Door Configuration and Site Configuration* for details on payload.

Responder (ACK from CM - Command Executed- Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Update Lock Command Sent from LMS – Packet 2, User details

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	No of Users * (6-25 Bytes) + 2 Bytes	2 Bytes
Payload length + 9	0x19	0x01	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Please read below	Refer ORP Packet Structure

The payload for user details is same as the payload for Add Users command [section 4.28]. Please refer *Payload for Add / Update Users*. The ACU validates the Badge ID length, Issue Code length and Time Format provided in *User Details* packet, such that they are in sync with the same parameters provided in *Door and Site Configuration* packet. If any of these parameters are not identical in both packets, the ACU will respond to *User Details* packet with a "Invalid Payload" NACK.

Responder (ACK from CM - Command Executed- Packet 2)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

(Update Lock Command Sent from LMS – Packet 3, DST)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Number of DST * 5 + 2 Bytes	2 Bytes
Payload length + 9 bytes	0x19	0x02	0x0002	Refer ORP Packet Structure	Refer ORP Packet Structure	Please read below	Refer ORP Packet Structure

The payload for DST update is same as the payload for Update DST command [section 0]. Please refer to *Update DST Payload for details.*

Responder (ACK from CM - Command Executed- Packet 3)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0002	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

(Update Lock Command Sent from LMS – Packet 4, Holidays)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Number of Holidays * 9 + 2 Bytes	2 Bytes
Payload length + 9 bytes	0x19	0x03	0x0003	Refer ORP Packet Structure	Refer ORP Packet Structure	Please read below	Refer ORP Packet Structure

The payload for holidays is the same as the payload for Modify Holiday Table command [section 4.33]. Please refer *Modify Holidays Payload* for details.

Responder (ACK from CM - Command Executed- Packet 4)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0003	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

(Update Lock Command Sent from LMS – Packet 5, Timezones)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Number of Time Zones * 21 + 2 Bytes	2 Bytes
Payload length + 9 bytes	0x19	0x04	0x0004	Refer ORP Packet Structure	Refer ORP Packet Structure	Please read below	Refer ORP Packet Structure

The payload for timezones is the same as the payload for Modify Timezones command [section 4.31]. Please refer *Modify Time Zones Payload* for details.

Please refer Time zones section in the appendix for complete time zone packet parsing example

Responder (ACK from CM - Command Executed- Packet 5)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0004	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

(Update Lock Command Sent from LMS – Packet 6, Automatic Changes)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Number Of Automatic Changes*3 + 2 Bytes	2 Bytes
TBD	0x19	0x05	0x0005	Refer ORP Packet Structure	Refer ORP Packet Structure	Please read below	Refer ORP Packet Structure

The payload for automatic changes is the same as the payload for Change Automatic Changes command [section 4.34]. Please refer *Automatic Changes Payload* for details.

Responder (ACK from CM - Command Executed – Packet 6)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0005	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

(Update Lock Command Sent from LMS – Packet 7, SCF)

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	1/12/23/34/45 Bytes	2 Bytes
	0x19	0x06				Refer Payload	

The payload for SCF is the same as the payload for Update SCF command [section 4.39]. Please refer *Payload for SCF* for details.

Responder (ACK from CM - Command Executed – Packet 7)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0006	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

(Update Lock Command Sent from LMS – Packet 8, ACF)

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	(1/28/55/82/109) Bytes	2 Bytes
	0x19	0x07				Refer Payload	

The payload for ACF is the same as the payload for Update ACF command [section 4.38]. Please refer *Payload for Update ACF* for details.

Responder (ACK from CM - Command Executed – Packet 8)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0007	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

EOT sent from LMS

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x0B	0x00	0x0008	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM for EOT sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0008	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-24 Update Lock Packet format

Note: If any of the above individual packets with different subcommands (Ex: Time Zones, automatic changes… etc) are not applicable for the particular lock, those packets will not be sent with Update/Initialize commands.

4.26 Update ACU Clock (RTC)

This command is sent from PDA to update the clock on the lock. This command may not be used from LMS, since the inherent delays in wireless communication invalidates the current time in the packet.

Initiator (Update ACU Clock Command Sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	5 bytes	2 Bytes
0x0E	0x1A	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload

Year	Month	Day	Hour	Min	Sec	Unused
7 Bits	4 Bits	5 Bits	5 Bits	6 Bits	6 Bits	7 Bits

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-25 Update ACU Clock (RTC) Packet format

4.27 Write NWK Data to EEPROM

Initiator (Write to EEPROM Command Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	8 bytes	2 Bytes
0x11	0x16	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload

WAP Id	WAP Physical ID
4 Bytes	4 Bytes

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-26 Write NWK Data to EEPROM Packet format

4.28 Add / Update Users

This command is used to either add a new user or update an existing user. In the first packet sent to the Control Module, the first 2 bytes contains number of users. This is present in the first packet only.

Note that the user data must be sorted in ascending order by “Badge ID”. The “Badge ID” must be unique across all user records.

The ACU is expected to add as many users as there is space in the database. So, for example, if the command contains 200 new users to be added and 100 existing users to be updated and the lock only has space for 150 new users – lock will add 150 new users, update the 100 existing users and send a NACK response with NACK_SUBCMD_NO_SPACE_IN_MEMORY error code. This ensures that the lock populated the database with maximum number of users possible.

(Add a User Command Sent from LMS – Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Number of Users * 8 + 2 Bytes	2 Bytes
Payload length + 9 bytes	0x1F	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload for Add / Update Users

Number of users	Badge ID Length (in bytes)	Issue code length (in bytes)	Date & Time Format	User records
2 Bytes	1 Byte	1 Byte	1 byte	No of users * (6 to 25) (one user record size) bytes

One User Record

Badge ID	Issue Code	Activation Date and Time	Expiration Date and Time	User Type	Attributes
2-8 Bytes (variable)	1-4 Bytes (variable)	0, 2 or 5 Bytes (variable)	0, 2 or 5 Bytes (variable)	1 Byte	2 Byte

The Date and Time Format values are defined in Table *Date and Time Format Values* in Write Door CFG Payload description in section 4.32.

Activation / Deactivation Date Only Format

Year	Month	Day
7 Bits	4 Bits	5 Bits

Activation / Deactivation Date and Time Format

Year	Month	Day	Hour	Min	Sec	Unused
7 Bits	4 Bits	5 Bits	5 Bits	6 Bits	6 Bits	7 Bits

User Type

User Type	
0x00	Standard
0x01	Blocking
0x02	Network Join
0x03	Test LMS Communication
0x04	Emergency Lock
0x05	Emergency Unlock

Attributes

Lock Owner	Blocking Override	ADA	Time zone	Unused
1 bit	1 bit	1 bit	6 bits	7 bits

Responder (ACK from CM - Command Executed- Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Initiator (EOT sent, if user data spans multiple ORP packets)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x0B	0x00	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM for EOT sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-27 Add a User Packet format

4.29 Delete Users

This command is used to delete users from the lock. Note that the users should be sorted in ascending order by "Badge ID". The badge IDs must be unique.

Initiator (Delete Users Command Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	6 bytes	2 Bytes
0x0D	0x20	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload

Number of users	Badge ID Length (in bytes)	Badge IDs
2 bytes	1 Byte	(Number of Users) * Badge ID length (2 to 8 bytes)

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-28 Delete a User Packet format

4.30 Update DST

This command is used to set the daylight savings time information on the lock. Note that the DST data must be sorted in ascending order by date and time information. Each DST date and time must be unique across all DST records.

(Update DST Sent from LMS – Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Number of DST *5 +2 Bytes	2 Bytes
TBD	0x21	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Update DST Payload

Number of DST	DST Data
2 Bytes	No of DST * 5 (one DST data size) Bytes

One DST Data

Year	Month	Day	Hour	Min	Sec	Forward/Reverse	Unused
7 Bits	4 Bits	5 Bits	5 Bits	6 Bits	6 Bits	1 Bit	6 Bits

Responder (ACK from CM for DST Information sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-29 Update DST Packet format

4.31 Modify Time Zones

In the first packet sent to the Control Module, the first 2 bytes contains number of Time Zones. This is present in the first packet only.

There can be a maximum of 64 time zones with index range from 0x00 through 0x3F. Index 0x00 and Index 0x3F are predefined time zones as NEVER and ALWAYS respectively and 0x01 to 0x3E are user defined time zones. So the valid ranges for the modify time zone are 0x01 to 0x3E.

Note: The Week Day field in modify time zone, represents the days of the week from Sunday to Saturday and the Holiday. The bit representation is as follows.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Holiday	Saturday	Friday	Thursday	Wednesday	Tuesday	Monday	Sunday

With this bit mask we can set the valid days for a time zone and days which needs to be set as holidays(to avoid access to users)

The time zones data must be sorted in ascending order by “Time Zone Index” field. The Time Zone Index must be unique across all timezone records.

Please refer Time zones section in the appendix for complete time zone packet parsing example

The sequence numbers for the packets below (in the packet format) are given based on the assumption that there is only one packet for each of the above given Time Zone data payload. However there could be more packets and the sequence numbers have to be updated accordingly.

(Modify Time Zones Command Sent from LMS – Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Number of Time Zones*21 +2 Bytes	2 Bytes
TBD	0x22	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Modify Time Zones Payload

Number of Time Zones	Timezones Data
2 Bytes	No of timezones * 21 (one timezone data size) Bytes

One Timezone Data

StartTimeMin2	StartTimeHour1	EndTimeMin1	EndTimeHour1	Unused	Weekday
6 Bits	5 Bits	6 Bits	5 Bits	2 Bits	1 Byte

StartTimeMin2	StartTimeHour2	EndTimeMin2	EndTimeHour2	Unused	Weekday
6 Bits	5 Bits	6 Bits	5 Bits	2 Bits	1 Byte

StartTimeMin3	StartTimeHour3	EndTimeMin3	EndTimeHour3	Unused	Weekday
6 Bits	5 Bits	6 Bits	5 Bits	2 Bits	1 Byte

StartTimeMin4	StartTimeHour4	EndTimeMin4	EndTimeHour4	Unused	Weekday
6 Bits	5 Bits	6 Bits	5 Bits	2 Bits	1 Byte

StartTimeMin5	StartTimeHour5	EndTimeMin5	EndTimeHour5	Unused	Weekday	Time Zone Index
6 Bits	5 Bits	6 Bits	5 Bits	2 Bits	1 Byte	1 Byte

Responder (ACK from CM - Command Executed- Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (EOT sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x0B	0x00	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM for EOT sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-30 Modify Time Zones Packet format – Sub Command Id 0x00

ACK for CM_Wakeup

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

(Modify Time Zones Command Sent from LMS – Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Number of Time Zones*21 +2 Bytes	2 Bytes
TBD	0x22	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload

Number of Time Zones	StartTimeMin1	StartTimeHour1	EndTimeMin1	EndTimeHour1	Unused	Weekday
2 Bytes	6 Bits	5 Bits	6 Bits	5 Bits	2Bits	1 Byte

StartTimeMin2	StartTimeHour2	EndTimeMin2	EndTimeHour2	Unused	Weekday
6 Bits	5 Bits	6 Bits	5 Bits	2 Bits	1 Byte

StartTimeMin3	StartTimeHour3	EndTimeMin3	EndTimeHour3	Unused	Weekday
6 Bits	5 Bits	6 Bits	5 Bits	2 Bits	1 Byte

StartTimeMin4	StartTimeHour4	EndTimeMin4	EndTimeHour4	Unused	Weekday
6 Bits	5 Bits	6 Bits	5 Bits	2 Bits	1 Byte

StartTimeMin5	StartTimeHour5	EndTimeMin5	EndTimeHour5	Unused	Weekday	Time Zone Index
6 Bits	5 Bits	6 Bits	5 Bits	2 Bits	1 Byte	1 Byte

Responder (ACK from CM - Command Executed- Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (EOT sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x0B	0x00	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM for EOT sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-31 Modify Time Zones Packet format – Sub Command Id 0x01

4.32 Write Door CFG

If ACU/WLM communication parameters or wireless operational parameters get updated as part of Write Door CFG command from LMS or PDA, the lock ACU sends the new values to WLM using the Operational Parameters command or the Configure Wireless Operational parameters command respectively. These commands are described in the ACU – WLM Identification [section 4.1.1].

Initiator (Write Door CFG Command Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	71 to 91 Bytes	2 Bytes
0x50 to 0x64	0x24	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload- Door Configuration and Site Configuration

Lock Name	Reserved for Common PIN	Authorization	Standard Open time	Extended Open time	Enable Keypad	Enable Locking back	Enable Privacy
40 Bytes	4 Bytes	1 Byte	1 Byte	1 Byte	1 bit	1 bit	1 bit

Enable Office mode with Card	Enable Blocked mode with Card	Enable buzzer	Enable Latch monitoring	Enable Door Sensor Switch	Enable AFC on exit – AFC Mode	Enable AFC on entry – AFC Card	Enable AFC RELOCK Timer
1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

Deadbolt ends AFC mode	Precedence of card or Lock Data	Date & Time Format	Enable Door held open Alarm	Relock timer	Issue Code look ahead	Badge ID Length (in bytes)	Issue Code length (in bytes)
1 bit	1 bit	2 bits	1 bit	1 Byte	1 Byte	1 Byte	1 Byte

Standard Door Held Open Time	Extended Door Held Open Time	Door Held Open Alarm Duration	Host wait time	Enable DST	Reserved - General No of Authorization
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

HB Rate (in sec)	RF O/P Power	Channel ID	FA Mode	ACU/WLM Retry Count	ACU/WLM Timeout Period
4 Bytes Default : 300 Range : 60 – 86400	1 Bytes Default : 3 Range : 1 -4	1 Bytes Default : 1 Range : 1 -26	1 Bytes Default : 1 Range : 0 -1	1 Byte Default : 3 Range : 1 - 10	1 Byte Default : 5 (500 msec) Range : 5 to 50

ACU/LMS Retry Count	ACU/LMS Timeout Period	No Of Events	Priority Events (Max 20)
1 Byte Default : 3 Range : 1 - 10	1 Byte Default : 6 (6 sec) Range : 1 to 10	1 Byte	0 to 20 Bytes

Date and Time Format Values

Value	Description
00	No date or time
01	Date Only
10	Date and Time
11	Reserved

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-32 Write Door CFG Packet format

The ACU/LMS Timeout Period is the time that ACU waits for an ACK from the LMS before retrying the ORP packet. This applies to the events sent from the ACU and Request Data type commands**.** This timeout value is not used by the LMS, since the LMS timeout is governed by the WLM heartbeat period.

The ACU/LMS Retry Count is the number of times the ACU or the LMS retries a packet if it times out waiting for an ACK.

4.33 Modify Holiday Table

This command can be used to update the entire holiday table. Note that in the first packet sent to the Control Module, the first 2 bytes contains number of Holidays. This is present in the first packet only.

The holiday data must be sorted in ascending order by start date and time. Each holiday start date and time must be unique across all holidays.

(Modify Holiday Table Command Sent from LMS – Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Number of Holidays *9 + 2 Bytes	2 Bytes
TBD	0x28	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Modify Holidays Payload

Number of Holidays	Holidays Data
2 Bytes	No of holidays * 9 (1 holiday data size) Bytes

One Holiday Data

Start Year	Start Month	Start Day	Start Hour	Start Min	Start Sec
7 Bits	4 Bits	5 Bits	5 Bits	6 Bits	6 Bits

End Year	End Month	End Day	End Hour	End Min	End Sec	Unused
7 Bits	4 Bits	5 Bits	5 Bits	6 Bits	6 Bits	6 Bits

Responder (ACK from CM - Command Executed- Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (EOT sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x0B	0x00	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM for EOT sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-33 Modify Holiday Table Packet format

4.34 Change Automatic Changes

In the first packet sent to the Control Module, the first 2 bytes contains number of Automatic Changes. This is present in the first packet only.

The sequence numbers for the packets below (in the packet format) are given based on the assumption that there is only one packet for each of the above given Automatic Changes payload. However there could be more packets and the sequence numbers have to be updated accordingly.

Note that the automatic changes must be sorted in ascending order by StartTimeMin and StartTimeHour. The start time (combination of hour and minutes) must be unique across all automatic changes.

(Change Automatic Changes Command Sent from LMS – Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Number Of Automatic Changes*3 + 2 Bytes	2 Bytes
TBD	0x25	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Automatic Changes Payload

Number Of Automatic Changes	Automatic Changes Data
2 Bytes	No. of automatic changes * 3 bytes

One Automatic Change Data

StartTimeMin	StartTimeHour	Mode	Unused	Week Days
6 Bits	5 Bits	3 Bits	2 Bits	1 Byte

Responder (ACK from CM - Command Executed – Packet 1)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (EOT sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x0B	0x00	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM for EOT sent)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0001	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-34 Change Automatic Changes Packet format

4.35 Read Lock Operational Cycles

This command can be used to get the number of lock / unlock cycles that a lock has gone through since it has been in use. The lock / unlock cycles do not get reset in factory mode and also accounts for the lock usage in factory mode.

Initiator (Command Sent from WLM)

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x62	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Response Sent from ACU

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	4 bytes	2 Bytes
	0x08	0x01				No of lock / unlock cycles	

Table 4-35 Read Lock Operational Cycles Packet Format

4.36 Send Events to OGACS:

The lock ACU uses this command to send a priority one event to LMS.

Command Sent from ACU

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	Total bytes for events	2 Bytes
Total payload bytes + 9 bytes	0x64	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Table 4-36 Send Events to OGACS Packet Format

The payload for this command is same as the payload for the response for Read Audit Trail command [section 4.23], except that for this command the payload is no more than 128 bytes. This means that there is a limit on the number of events that can be included in this command depending on the length of each event. Please refer *Payload for Read Audit Trail response* for payload details.

4.37 Request Clock (RTC) Command:

This command is used by the lock to request the current time from LMS. LMS sends the current local time in response to the command.

Initiator (Command Sent from ACU)

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x65	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Response Sent from WLM

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	5 bytes	2 Bytes
	0x08	0x01				Refer below	

Payload

Year	Month	Day	Hour	Min	Sec	Unused
7 Bits	4 Bits	5 Bits	5 Bits	6 Bits	6 Bits	7 Bits

Table 4-37 Request Clock Packet Format

4.38 Update ACF

This command is used to provide the ACF configuration to the control module.

The ACF data must be sorted in ascending order by “Priority Number”. The “Priority Number” must be unique across all the ACFs.

Initiator (Command Sent from WLM)

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	No of ACF (max 4) * 27 + 2 Bytes	2 Bytes
Total payload bytes + 9 bytes	0x60	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Payload for Update ACF

Number of ACFs	ACFs
2 Bytes	Maximum of (27*4 ACFs) = 108 Bytes
	Refer below for one ACF

Payload for One ACF

Priority Number	ACF Type	Total Bit count that is present on the card	Parity Type	Facility Code for ACF	Facility Code Start Bits	No of bits associated with Facility Code	Card Number Start Bits
1 Byte	1 Byte	2 Bytes	1 Byte	4 Bytes	1 Byte	1 Byte	1 Byte
	Refer below		Refer below				

No of bits associated with Card Number	Issue Code Start Bits	No of bits associated with Issue Code	Activation Date and Time Start Bits	No of bits with Activation Date and Time	De-activation Date and Time Start Bits	No of bits with De-activation Date and Time	ADA Start Bits
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

No of bits associated with ADA Attribute	Authorization Start Bits	No of bits associated with Authorization	Even Parity Info	Odd Parity Info
1 Byte	1 Byte	1 Byte	2 Bytes	2 Bytes

ACF type

ACF Type	Description
0x00	Wiegand data format
0x01	Integra data format

Parity type

Parity Type	Description
0x00	None
0x01	Standard
0x02	Non Standard – HID Corp 1000

Table 4-38 Update ACF Packet Format

4.39 Update SCF

This command is used to provide the SCF configuration to the control module and the reader module.

The SCF data must be sorted in ascending order by “Priority Number”. The “Priority Number” must be unique across all the SCFs.

Note: After completion of this command, the ACU sends the new SCF information to the reader and during this time, the ACU will not be able to execute any new commands from LMS. For this reason, if both ACF and SCF are changed at the LMS, it is recommended that LMS send Update ACF before Update SCF command.

Initiator (Command Sent from WLM)

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	(No of SCF (max 4) * 11) + 2 Bytes	2 Bytes
Total payload bytes + 9 bytes	0x61	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Payload for SCF

Number of SCFs	SCFs
2 Bytes	Maximum of (11*4 SCFs) = 44 Bytes
	Refer below for one SCF

Payload for one SCF

Priority Number	Format Type	Application Location	Application Key
1 Byte	1 Byte	1 Byte	8 Bytes (for iCLASS Reader)
	Refer Below	Refer Below	

Format Type

Format Type	Description
0x00	ISO14443A_CSN
0x01	ISO14443B_CSN
0x02	ISO15693_CSN
0x03	ICLASS_HID

Format Type	Description
0x04	ICLASS_LENEL
0x05	MIFARE_LENEL

Table 4-39 Update SCF Packet Format

Note: *the Application Location and Application Key fields are not used for Format Types ISO 14443A_CSN, ISO 14443B_CSN, ISO 15693_CSN and iCLASS_HID.*

Application location for ICLASS_LENEL Format Type

Book	Page	Application ID	Unused
1 Bit	3Bits	1 Bit	3 Bits
		0 – Application 2 1 – Application 1	

Application location for MIFARE_LENEL Format Type

Sector	Unused
5 bits	3 Bits
Sectors 0 - 31	

Application Key for MIFARE_LENEL Format Type

Read Key Type	Unused	Read Key
1 Byte	1 Byte	6 Bytes
0x00 – Key A 0x01 – Key B		

Example MIFARE_LENEL SCF Payload (LSB to MSB):

0105120100123456789ABC

- Priority Number – 1 (0x01)
- Format Type – MIFARE_LENEL (0x05)
- Application Location – Sector 18 (0x12)
- Application Key
    - Read Key – Key B (0x01)

- Unused – 0x00
- Key (LSB-MSB) - 123456789ABC (0xBC9A78563412)

4.40 Range Verification Command

This command is sent by the Control Module in factory configuration to the WLM to start the range verification with a WAP in the vicinity. The WLM attempts to communicate and verify wireless signal strength and range with any WAP in the vicinity, and if it is successful (meaning the signal strength with the WAP is good), it flashes the green LED on the lock using the Flash LED (Green) command. If range verification fails, the WLM sends Flash LED (Red) command to CM.

This command has no payload.

Initiator (Command Sent from CM to WLM)

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
9	0x69	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-40 Range Verification Packet Format

4.41 Enable/Disable Communication of Events Command:

This command can be used to configure up to 20 events as priority one events that get sent to LMS as they happen.

The priority events must be sorted in ascending order by event ID. The Event IDs must be unique.

Initiator (Command Sent from WLM)

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	No of events + 1 Bytes	2 Bytes
Total payload bytes + 9 bytes	0x66	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Payload

No of Events	Event Id 1	Event Id 2	….	….	Event Id 20
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte

Table 4-41 Enable/Disable Communication of Events Packet Format

4.42 Check Lock Mode

This command is sent from the PDA. If PDA wants to send any command to CM it will send *Hello Command* packet first. Then only it will send the respective command packet (in this case *Check Lock Mode)*. Kindly refer Section 3.5 for Hello command.

After CM receives the *Check Lock* command packet it will validate the command packet and after successfully validating the command it will process the command. Otherwise a NACK with the appropriate error code is sent. Kindly refer to Section 7.1 for Error Codes.

An *ACK* shall be sent only after the command is successfully executed. The Lock Mode Information shall be embedded in the ACK packet as shown in Figure 6.2.1. If an ACK is not received within the timeout period the command is sent again. The numbers of retries are configurable from 1-10.

Initiator (Check Lock Mode Command Sent from PDA)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x4A	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed with Lock Mode Information)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Byte	2 Bytes
0x0B	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Payload

Lock Mode
2 Bytes

Responder (ACK from PDA for door status)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-42 Check Mode Packet format

4.43 Switch Test

This command is sent from the PDA. If PDA wants to send any command to CM it will send *Hello Command* packet first. Then only it will send the respective command packet (in this case *Switch Test)*. Kindly refer Section 3.5 for Hello command.

After CM receives the *Switch Test* command packet it will validate the command packet and after successfully validating the command it will process the command. Otherwise a NACK with the appropriate error code is sent. Kindly refer to Section 7.1 for Error Codes.

After successfully validating the command, the CM will check if any key is pressed by the user. If any key is pressed within the Diagnostic timeout, *ACK* shall be sent with key pressed information embedded as shown in Fig 6.3.1 and the Diagnostic timeout timer is restarted. For every ACK (with key-pressed information sent), CM shall expect an ACK from PDA. If an ACK is not received within the timeout period (this timeout is different from the Diagnostic timeout) the key-pressed information packet (ACK) is sent again. The numbers of retries are configurable from 1-10.

CM shall continue to send ACK with the payload each time a key is pressed within the diagnostic timeout period. If timeout happens, CM shall terminate the command. The Diagnostic Timeout is 10 sec.

If PDA sends a Stop Switch Test command in between of switch test, CM will terminate the command and send ACK for command executed.

Initiator (Switch Test Command Sent from PDA)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x4B	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Stop Switch Test Command Sent from PDA in between the command

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x4B	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed with Key pressed information)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	1 Byte	2 Bytes
0x0A	0x08	0x01	TBD	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Payload

Key pressed Byte
1 Byte

Responder (ACK from PDA)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	TBD	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM - Command Executed for Stop Switch Test command)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x0A	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-43 Switch Test packet format

4.44 Send System Code

When PDA supposed to send command to Control Module, it will start with *Hello Command* and then actual will be sent. Please refer Section 3.5 for Hello command.

After successful hello command identification, PDA sends the “Send System Code” command to Control Module. On receiving the command, Control Module shall validate the command and after successful validation, ACK command shall be sent to PDA. Otherwise Control Module shall send NACK with the appropriate error code. Please refer to Section 8.1 for Error Codes.

Send System Code Command Sent from PDA

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	4 Byte	2 Bytes
0x0D	0x4C	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload

System Code
4 Bytes

ACK from CM - Command Executed

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-44 Send System Code Packet format

4.45 Send Lock ID

When PDA supposed to send command to Control Module, it will start with *Hello Command* and then actual will be sent. Please refer Section 3.5 for Hello command.

After successful hello command identification, PDA sends the “Send Lock ID” command to Control Module. On receiving the command, Control Module shall validate the command and after successful validation, ACK command shall be sent to PDA. Otherwise Control Module shall send NACK with the appropriate error code. Please refer to Section 8.1 for Error Codes.

Initiator (Send Lock ID Command Sent from PDA)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	4 Byte	2 Bytes
0x0D	0x4D	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload

Lock ID
4 Bytes

Responder (ACK from CM - Command Executed with Lock ID Information)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-45 Send Lock ID Packet format

4.46 Network Join

When PDA supposed to send command to Control Module, it will start with *Hello Command* and then the actual command will be sent. Please refer Section 4.5 for Hello command.

PDA sends *Network Join* command to Control Module. Control Module shall validate the command, after successful validation, sends ACK to PDA and then sends the *Reset* command to WLM.

WLM shall validate the command and after successful validation, WLM shall execute the command to reset itself. After reset, normal identification sequence will take place (refer section 4.1.1). As part successful identification, network join process will start in WLM. The network join process duration shall be 2 seconds.

On completion of the network join process WLM shall send ACK/NACK to Control Module depending on network join status.

WLM shall then send *Write NWK Data to EEPROM*) and *Flash Red/Green LED* command to ACU.

After successful execution of Flash *Red/Green LED* command, Control Module shall send ACK to PDA if Green LED is flashed; otherwise it will send NACK to PDA.

If control module is unable to start the network join process with WLM, or if the WLM join fails, then control module will send a NACK to the PDA.

The PDA will timeout after 2 minutes if it does not receive an ACK / NACK to indicate WLM join success or failure.

Note that the ACU follows similar procedure when the network join card is presented. The ACU initiates the join procedure by sending the Reset command to WLM. The WLM upon reboot, initiates the identification with the ACU and attempts to join a WAP. After a successful join, the WLM flashes the green LED on lock. If join fails WLM flashes the red LED on the lock. In this case, there is nothing else for ACU to do besides sending a Reset command to WLM.

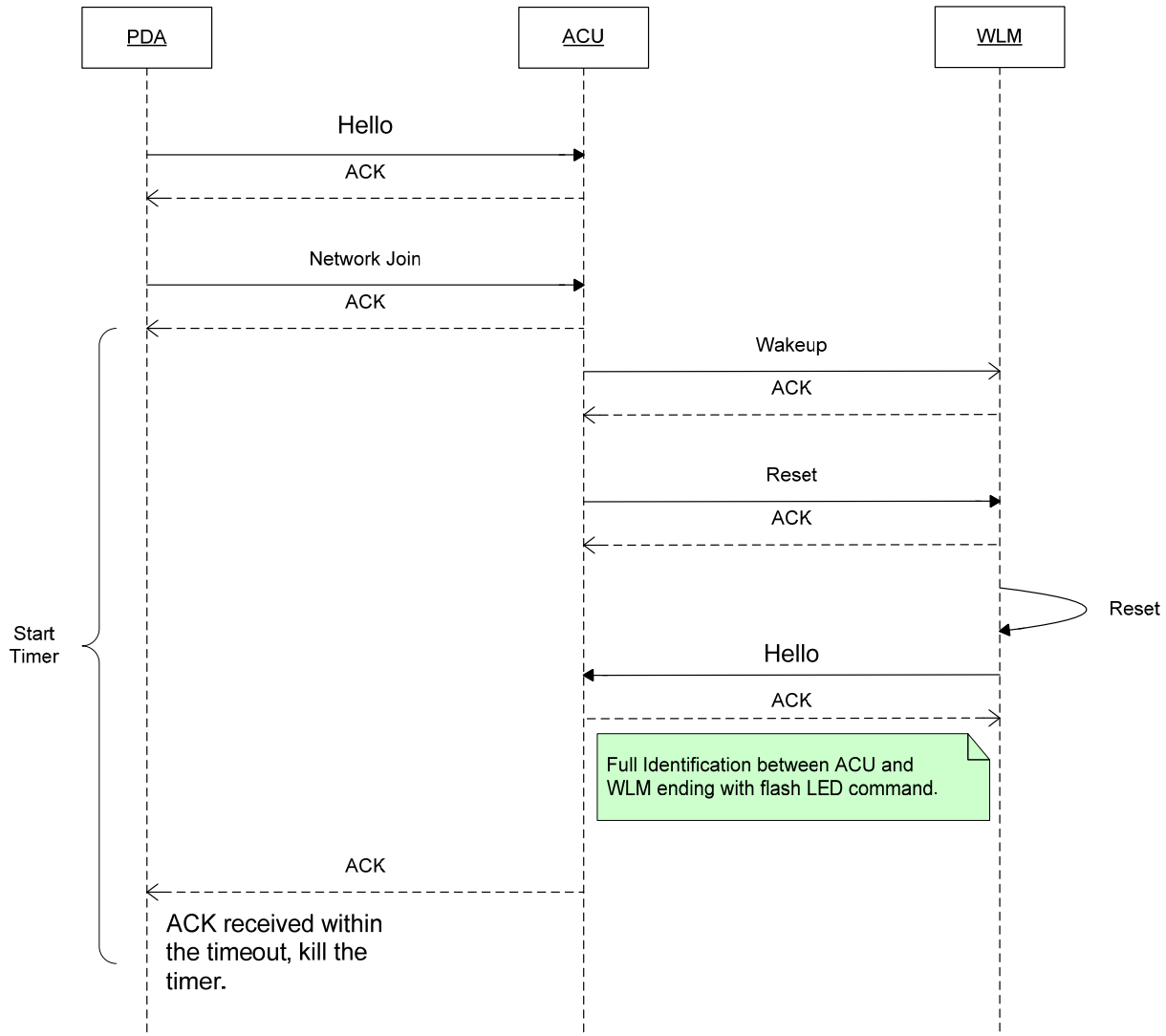

Figure 4-9 Network Join Command

Packet Sequence from PDA to ACU

Initiator (Network Join Command Sent from PDA)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x38	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM – Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Packet Sequence from ACU to WLM

Initiator (Reset Command Sent from ACU)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x4F	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from WLM – Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM – to PDA Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-46 Network Join Packet format

4.47 Test LMS Communication

When PDA supposed to send command to Control Module, it will start with *Hello Command* and then actual will be sent. Please refer Section 3.5 for Hello command.

PDA sends *Test LMS Communication* command to Control Module. This command is used to test the communication between the lock and LMS. Control Module shall validate the command, after successful validation, sends ACK to PDA and then sends the command to LMS and waits for a ACK in response. If the connection between LMS and lock is active, LMS will receive the command and will send an ACK.

The ACU flashes the green LED on receiving the ACK and sends an ACK to PDA to indicate successful communication with LMS.

If the ACU times out waiting for an ACK, it will retry the command to LMS as per the retry count. If all the retries are exhausted, the ACU flashes the red LED and sends a NACK to PDA to indicate communication failure.

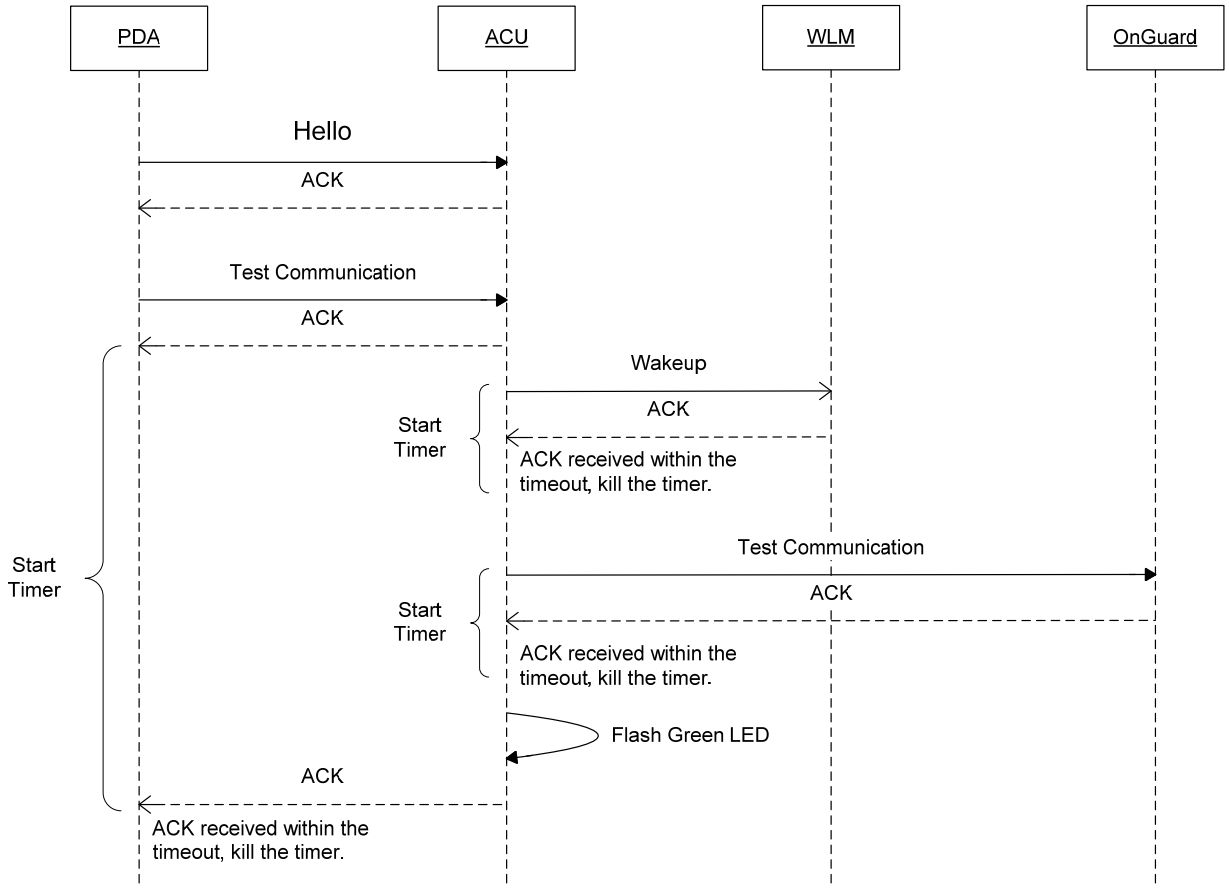

Figure 4-10 Test LMS Communication Command – Successful Execution

Packet Sequence from PDA to ACU

Initiator (Test LMS Communication Command Sent from PDA)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x39	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM – Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x02	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Packet Sequence from ACU to WLM

Initiator (Test LMS Communication Command Sent from ACU)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x39	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from LMS – Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Responder (ACK from CM – to PDA Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-47 Test LMS Communication packet Format

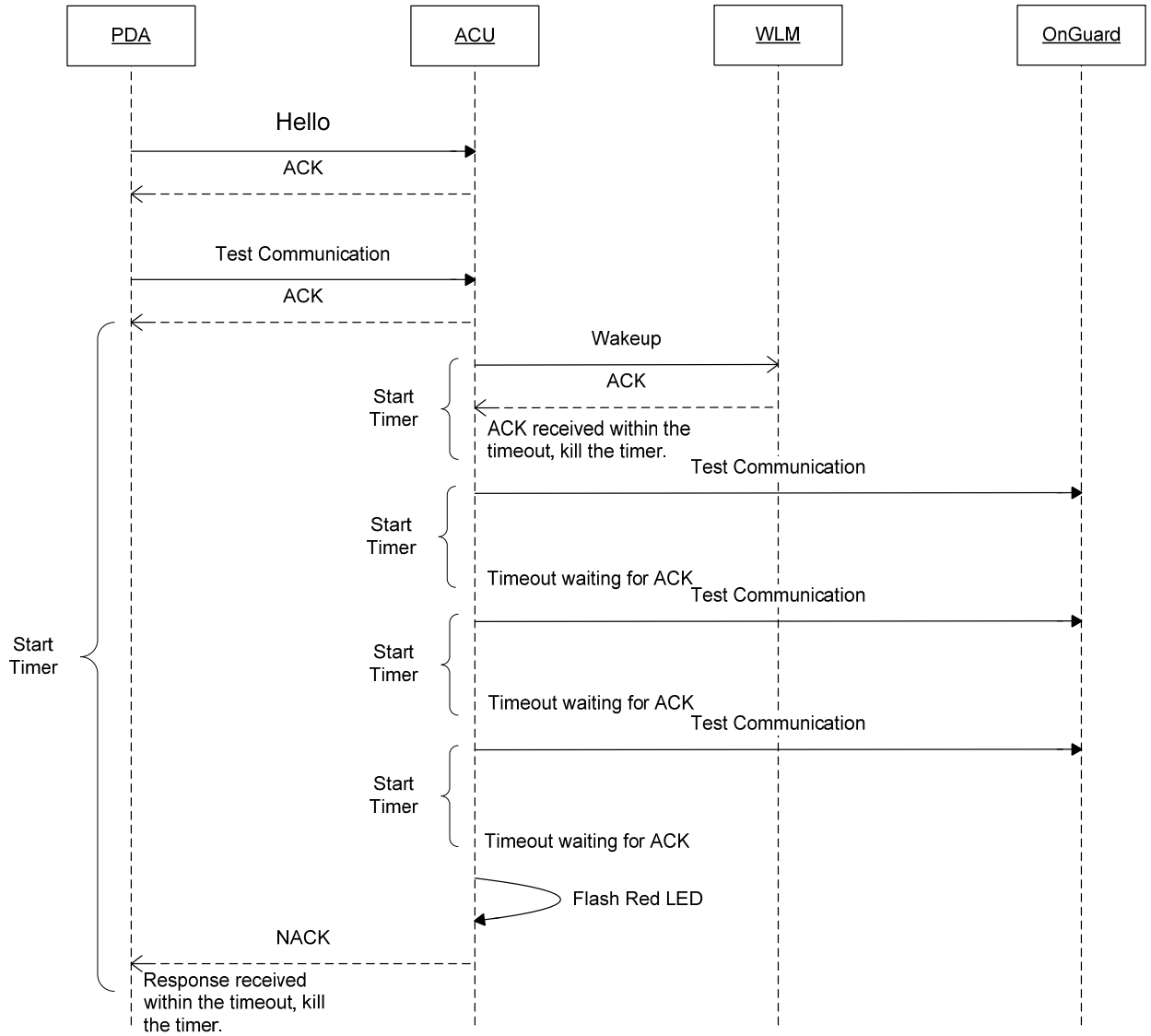

Figure 4-11 Test LMS Communication Command (Missing ACK from LMS)

4.48 ACU Firmware Upgrade

The ACU firmware can be upgraded either through the PDA or through LMS (via WLM). The ACU firmware is segmented into multiple ORP packets and sent to the ACU. The ACU waits to receive the entire firmware, assembles it and then initiates writing to program flash. On completion of flash update, ACU resets itself. Upon reboot, the ACU sends “Firmware Upgrade Success” command to PDA or LMS (whoever initiated the firmware upgrade). ACU logs the firmware upgrade success into the audit trail and sends a ACU_FW_UPGRADED event to LMS.

Figure 4-12 shows the flow of messages when the ACU firmware is upgrade through LMS via the PDA.

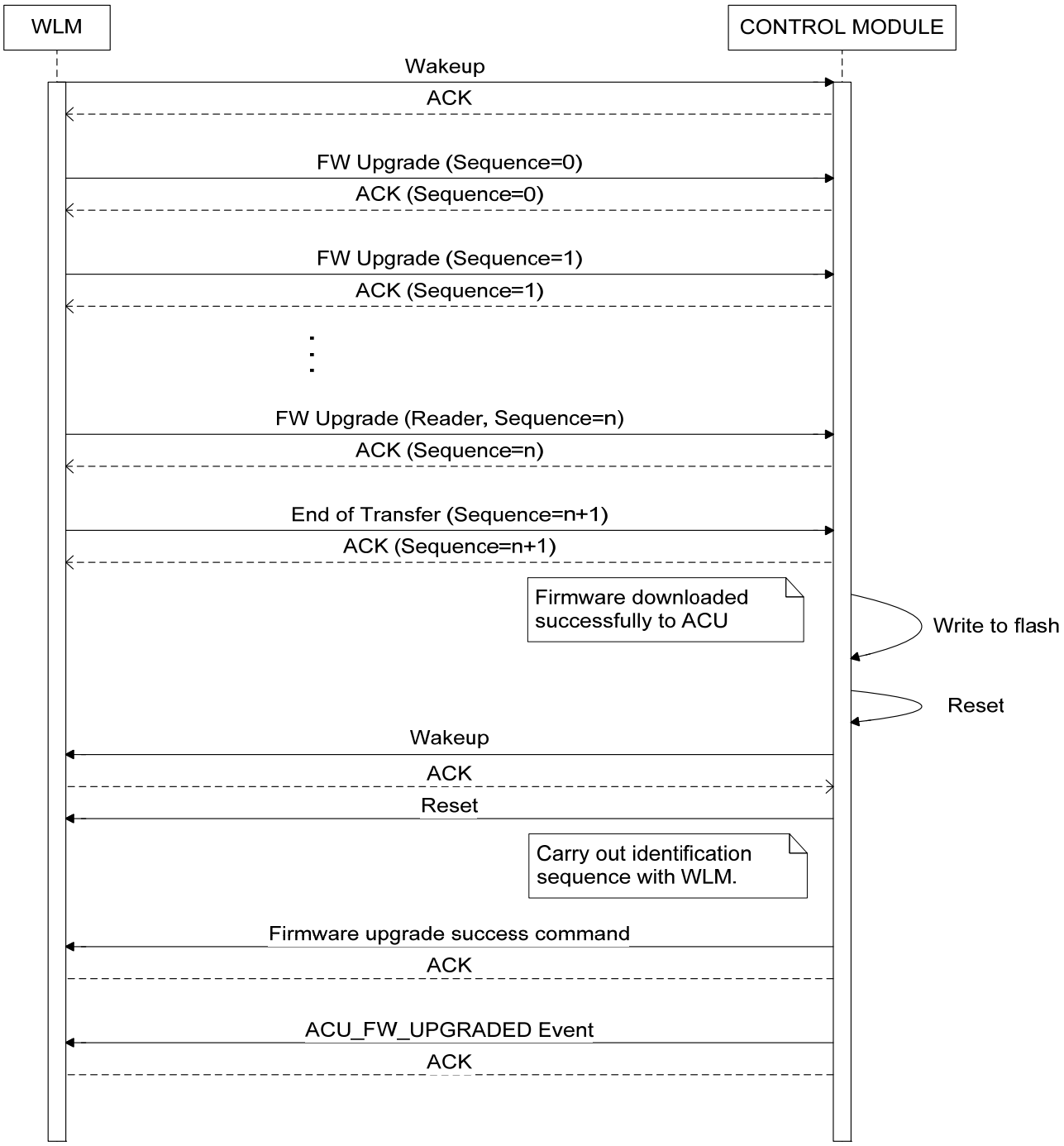

Figure 4-12 ACU Firmware Upgrade - Successful Execution

The ACU shall not execute the firmware upgrade if the battery level is not sufficient. The ACU checks the battery level when it receives the first firmware upgrade packet and also when it receives the last EOT packet. If the battery is too low, it NACKs the firmware upgrade or EOT packet with the error code NACK_SUBCMD_LOW_BATTERY. In both cases, the ACU terminates the ACU firmware upgrade command.

Note that this is different from “Low Battery Event” condition – in this condition, the battery is not sufficient for firmware upgrade, but may not be below the low battery threshold and hence no event is logged into the audit trail. OnGuard is expected to appropriately inform the user about the firmware upgrade failure due to insufficient battery.

Note that the ACU firmware upgrade from PDA is similar to that from LMS except that there is identification between ACU and PDA priori to the firmware upgrade. Also, once the firmware upgrade is complete, the “firmware upgrade success” command is sent to the PDA, but the ACU_FW_UPGRADED event is sent to LMS.

After the last End of Transfer packet, it can take up to 15 seconds for the ACU to send the Firmware upgrade success command. This includes the time it takes to write the firmware to flash and reboot.

After successful firmware upgrade, the lock configuration must be updated using the Update Lock command (either through PDA or LMS).

Initiator (Flash (Reprogram) the ACU Command Sent from LMS)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	128 Bytes	2 Bytes
0x89	0x0C	0x00	X	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload

Offset	Data
2 Bytes	126 Bytes

Responder (ACK from CM for Packet x- Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	X	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-48 Flash (Reprogram) the ACU Packet format

The packet format for the Firmware Upgrade Success command is described in section 4.51.

4.49 Reader Firmware Upgrade

The reader firmware can be upgraded either through the PDA or through LMS (via WLM). The reader firmware is sent to the lock ACU segmented into multiple ORP packets. The ACU waits to receive the entire firmware, assembles it and then initiates communication with the reader to upgrade the firmware on the reader. Once the reader finishes writing the new firmware to the flash, it resets itself and upon reboot initiates identification with the ACU. After successful identification, the ACU sends Firmware Upgrade Success command to PDA or LMS (the initiator of the fw upgrade). ACU logs the reader firmware upgrade success into the audit trail and sends a reader firmware upgrade event to LMS.

Figure 4-13**Error! Reference source not found.** shows the sequence of packets when the reader firmware is upgraded from LMS via WLM.

After the last End of Transfer packet, It can take up to 15 seconds for the ACU to send the Firmware upgrade success event. This includes the time it takes to transfer the firmware to reader and carry out identification upon reboot.

The ACU shall not execute the reader firmware upgrade if the battery level is not sufficient. The ACU checks the battery level when it receives the first reader firmware upgrade packet and also when it receives the last EOT packet. If the battery is too low, it NACKs the reader firmware upgrade or EOT packet with the error code NACK_SUBCMD_LOW_BATTERY. In both cases, the ACU terminates the reader firmware upgrade command.

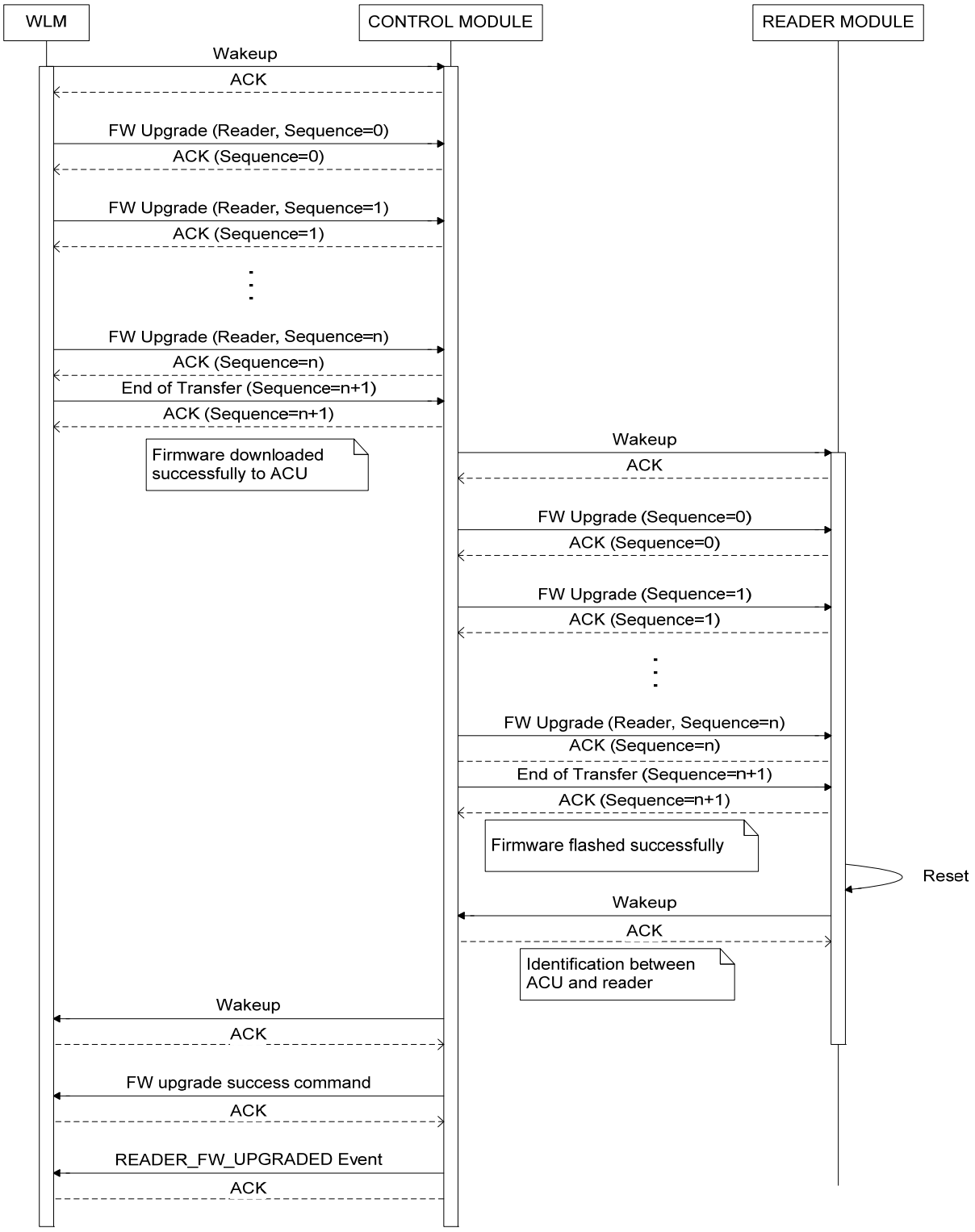

Figure 4-13 Flash (Reprogram) reader in Lock (Successful Execution)

Note that when the reader firmware is upgraded from PDA, the ACU follows similar sequence as described above, except that there is no wakeup between PDA and ACU. Instead there is identification between PDA and ACU following by the firmware upgrade messages. After firmware upgrade is complete, the firmware upgrade success command is sent to PDA and the READER_FW_UPGRADED event is sent to LMS.

The sub command IDs for upgrading firmware on different readers are detailed below:

Sub command ID	Description
0x02	iClass Reader
0x03	AWID Reader

Initiator (Flash(Reprogram) Reader in Lock Command Sent from WLM – Packet x)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	128 Bytes	2 Bytes
0x51	0x0C	0x02 / 0x03	X	Refer ORP Packet Structure	Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

Payload

Offset	Data
2 Bytes	126 Bytes

Table 4-49 Flash (Reprogram) reader in Lock Packet format

Note: The 'Offset' in the payload refers to the offset within the firmware file from which the firmware data is read and provided in the packet. This offset is specified for each packet of firmware upgrade and must be zero for the first packet, 126 for the second packet and so on.

The packet format for the Firmware Upgrade Success command is described in section 4.51.

4.50 WLM Firmware Upgrade

This command is used to upgrade the WLM firmware from the PDA. Note that this command cannot be used for WLM firmware upgrade from LMS and this is not covered by ORP. Figure 4-14 depicts the flow of packets when WLM firmware upgrade from PDA is successful.

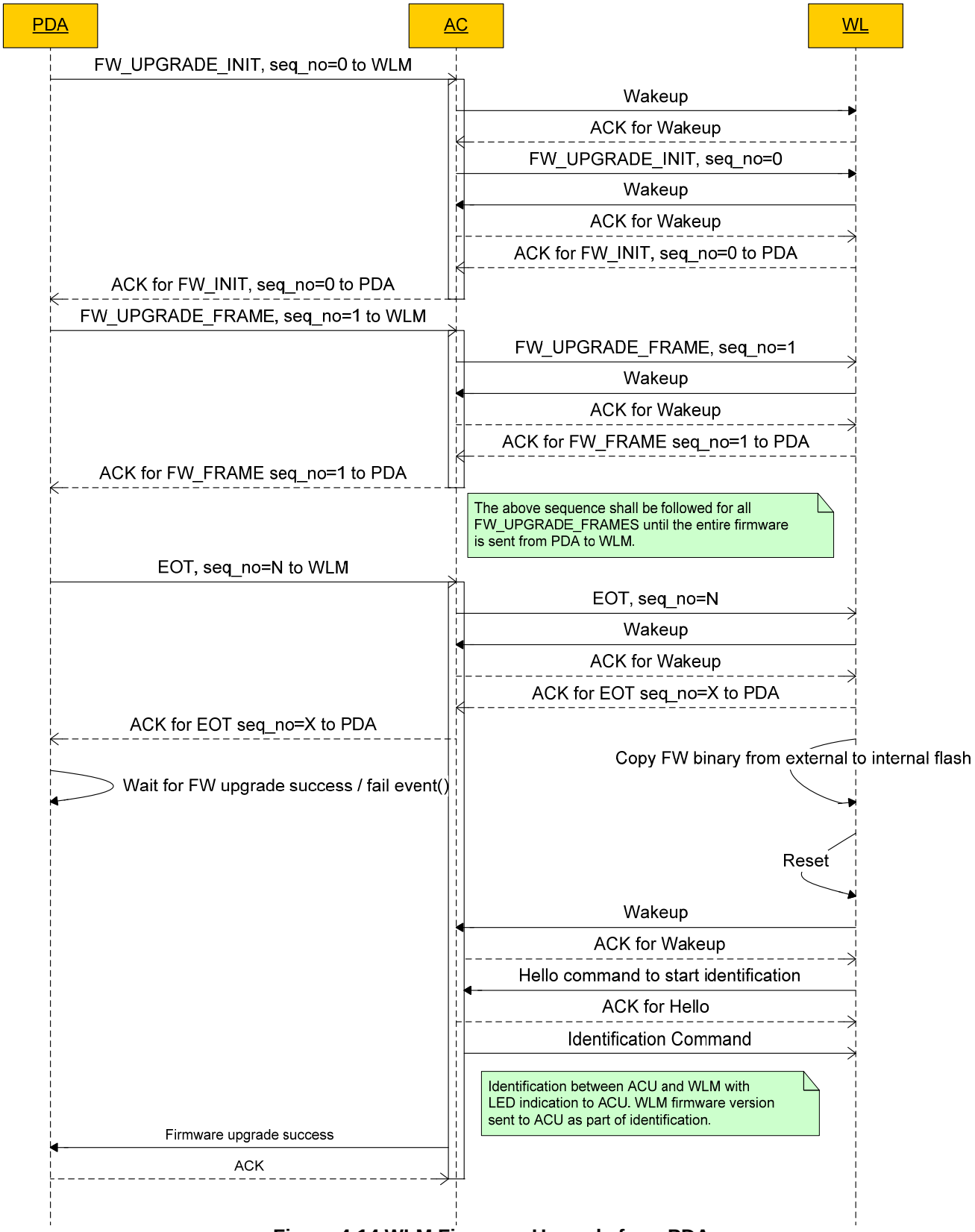

Figure 4-14 WLM Firmware Upgrade from PDA

FW_UPGRADE_INIT packet format:

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	7 Bytes	2 Bytes
0x10	0x67	0x02	0x0000	PDA - Refer ORP Packet Structure	WLM - Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

FW_UPGRADE_INIT Payload:

Firmware Size (in bytes)	Number of Frames	Maximum frame size
4 Bytes	2 Bytes	1 Byte
1 to 122880	Depends on size of each frame	Default = 125

Note that the “Number Of Frames” field does not include the FW_INIT packet itself and the EOT packet.

FW_UPGRADE_FRAME packet format:

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	7 Bytes	2 Bytes
0x10	0x67	0x03	0x0000	PDA - Refer ORP Packet Structure	WLM - Refer ORP Packet Structure	Please refer below	Refer ORP Packet Structure

FW_UPGRADE_FRAME Payload:

Frame Number	Frame Length	Firmware Binary
2 Bytes	1 Byte	Frame Length

If firmware upgrade is interrupted or is unsuccessful, then WLM may send a NACK to PDA. The NACK codes are described below.

NACK Sub-command ID	Description	WLM Action after NACK
0x16	Check sum for the received frame is invalid	WLM waits for next frame. If it does not receive the next frame within the timeout period (5 seconds), it terminates Firmware upgrade
0x20	There was a mismatch between the received frame number and the expected frame number.	WLM waits for next frame. If it does not receive the next frame within the timeout period (5 seconds), it terminates Firmware upgrade

NACK Sub-command ID	Description	WLM Action after NACK
0x21	The received frame length was either 0 or more than the max frame size specified by FW_INIT	WLM waits for next frame, with the correct size. If it does not receive the next frame within the timeout period (5 seconds), it terminates Firmware upgrade
0x22	After receiving the last frame, if the size of the complete image turns out to be different from that sent by FW_Init packet	WLM terminates Firmware upgrade
0x23	If flash write operation fails	WLM terminates Firmware upgrade
0x24	After receiving the last frame, if the CRC for the complete image does not match CRC received with the image	WLM terminates Firmware upgrade
0x25	If a firmware frame is received without receiving the firmware Init frame	WLM is ready to receive any packet

Please note the following regarding WLM firmware upgrade from PDA.

Sending of ACK to FW_UPGRADE_FRAME time would vary from frame to frame as WLM writes firmware bytes to flash after accumulating 256 bytes. The ACK for FW_UPGRADE_FRAME would take significantly longer (~3 seconds) for the last frame, as WLM performs CRC validation on the complete firmware image before sending the ACK.

After sending the ACK for the last frame, WLM issues a software reset and handsover the control to bootloader, which copies the firmware from external flash to internal program memory. After upgrading the firmware, WLM first sends out firmware upgrade successful event with new firmware version number to the PDA and then proceeds with the identification sequence with the lock ACU. WLM proceeds with the identification even if the fw upgrade event fails.

After receiving the ACK for EOT packet, ACU waits for 20 seconds for firmware upgrade successful event.

For firmware ACK packet sent by WLM to PDA, if all WLM-to-ACU wake-up retries get exhausted (without receiving wk-up ACK from ACU) or if a NACK is received in response, WLM will start inactivity timer for terminating FW upgrade.

On receiving a packet with invalid checksum, WLM will send a NACK without sending any wakeup signal.

If EOT packet fails (i.e. either it is not received by WLM or PDA doesn't get an ACK for it), WLM still continues with the firmware upgrade as it has already received all the firmware bytes.

If WLM receives FW_INIT packet in the middle of an ongoing firmware transfer (e.g. after receiving 10 FW frames), WLM clears the ongoing transfer and re-initiates the firmware transfer from beginning.

While the WLM firmware upgrade is ongoing from PDA, the reader activity may be ignored by the ACU. This implies that a card swipe or presentation of a card may not result in access decision (grant or deny). This is not considered a significant constraint, since no such use case is being foreseen that a user credential will be presented at the same time as the PDA operator is upgrading WLM firmware. Figure 4-15 depicts the scenario in which the reader activity is ignored by the ACU.

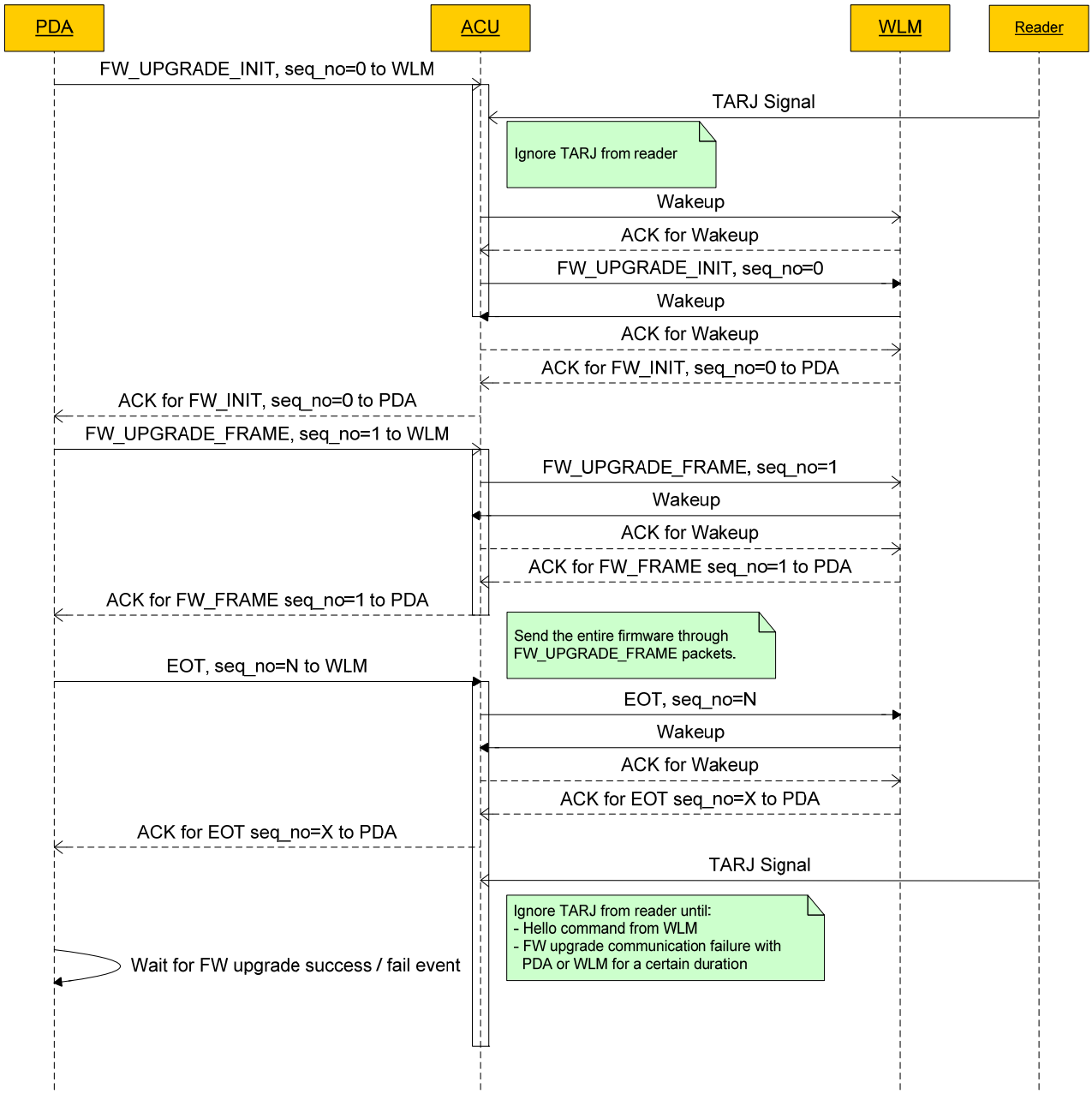

Figure 4-15 Reader Activity during WLM Firmware Upgrade

4.51 Firmware Upgrade Success

This command is sent by ACU to either PDA or LMS after a successful firmware upgrade of ACU, reader or WLM as described in sections 4.48, 4.49 and 4.50.

Command Sent from ACU

Packet Length	Command Id	Sub Command Id	Packet Seq No.	Source ID	Destination ID	Payload	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	6 Bytes	2 Bytes
0x0F	0x68	Refer below	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer below	Refer ORP Packet Structure

Sub Command IDs

Sub command id	Description
0x00	WLM Firmware Upgrade success
0x01	ACU Firmware Upgrade Success
0x02	Reader Firmware Upgrade Success

Payload

6 Bytes
Firmware Version

Note: In case of ACU and Reader firmware upgrade, only 4 bytes are used to specify firmware version and last two byte (MSB) shall be ignored. But in case of WLM firmware upgrade 6 bytes are used.

Responder (ACK from CM - Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer ORP Packet Structure

Table 4-50 Firmware Upgrade Success Packet Format

4.52 Activate All

When it is desired to send command to the Control Module, the PTE shall pull CM Wakeup signal high. The Control Module acknowledges the signal. After the ACK is received within the timeout period the PTE shall pull the CM Wakeup signal low.

PTE sends Activate All command to Control Module. Control Module shall validate the command, after successful validation and execution, Control Module sends ACK to PTE.

If an ACK is not received within the specified timeout period, the command shall be sent again by PTE. The number of retries are configurable from 1-10.

ACK for CM_Wakeup

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer Packet Structure

Initiator (Activate All Command Sent from PTE)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x50	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer Packet Structure

Responder (ACK from CM – Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer Packet Structure

Table 4-51 Activate All Command format

If no ACK is received for CM_Wakeup signal, then the CM_Wakeup signal is retried until the retry count is exhausted.

If the command is invalid, then the control module responds with a NACK packet.

If no response (ACK or NACK) is received for the Activate all command, the command is retried until the retry count is exhausted.

4.53 VANA

When it is desired to send command to the Control Module, the PTE shall pull CM Wakeup signal high. The Control Module acknowledges the signal. After the ACK is received within the timeout period the PTE shall pull the CM Wakeup signal low. If no ACK is received for CM_Wakeup signal, then the CM_Wakeup signal is retried until the retry count is exhausted.

PTE sends VANA command to Control Module. Control Module shall validate the command, after successful validation and execution, Control Module sends ACK to PTE.

If an ACK or NACK is not received within the specified timeout period, the command shall be sent again by PTE. The number of retries are configurable from 1-10.

ACK for CM_Wakeup

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer Packet Structure

Initiator (VANA Command Sent from PTE)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x51	0x00	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer Packet Structure

Responder (ACK from CM – Command Executed)

Packet Length	Command Id	Sub Command Id	Packet Sequence No.	Source ID	Destination ID	Checksum
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	1 Byte	2 Bytes
0x09	0x08	0x01	0x0000	Refer ORP Packet Structure	Refer ORP Packet Structure	Refer Packet Structure

Table 4-52 VANA Command format

5 Error and Event Codes

5.1 Error Codes

This section lists the various error codes (sub-commands) for the NACK command.

Sub Command Name	Sub-Command Id	Description
NACK_SUBCMD_RESERVED	0x00	Reserved
NACK_SUBCMD_INVALID_COMMAND	0x01	Received command ID is not valid ORP command
NACK_SUBCMD_INVALID_SUBCOMMAND	0x02	Received sub command ID for the command is not valid
NACK_SUBCMD_INVALID_SEQNUM	0x03	Received sequence number is greater than expected sequence number
NACK_SUBCMD_INVALID_PKT_SOURCE	0x04	Source of the packet is not from valid defined source
NACK_SUBCMD_INVALID_PKT_DESTINATION	0x05	Destination of the packet is not to valid defined destination
NACK_SUBCMD_INVALID_PAYLOAD_LENGTH	0x06	Invalid payload length of the fixed payload length command
NACK_SUBCMD_INVALID_CHECKSUM	0x07	Checksum error
NACK_SUBCMD_LOCK_NOT_INITIALIZED	0x08	Lock is in factory mode
NACK_SUBCMD_LOCK_BUSY	0x09	Lock is busy
NACK_SUBCMD_NO_SPACE_IN_MEMORY	0x0A	EEPROM memory is full
NACK_SUBCMD_IDENTIFICATION_NEEDED	0x0B	Need identification to proceed with further commands
NACK_SUBCMD_INVALID_PAYLOAD	0x0C	The payload is not what is expected for the particular command
NACK_SUBCMD_LOW_BATTERY	0x0D	Operation failed due to low battery
NACK_SUBCMD_NETWORK_JOIN_FAILED	0x0E	The network join operation failed
NACK_SUBCMD_TEST_KEY_FAILED	0x0F	The OnGuard connection test operation failed
NACK_SUBCMD_REINITIALIZATION_NEEDED	0x10	Configuration parameter is not matching with the initial initialization
NACK_SUBCMD_INVALID_FIRMWARE_FILE	0x11	Invalid ACU or reader firmware file
NACK_SUBCMD_INVALID_TIMEZONE_INDEX	0x12	Timezone index specified to modify does not exist in the lcok
NACK_SUBCMD_INVALID_FW_FRAME_NUM	0x20	Invalid firmware frame number during firmware upgrade
NACK_SUBCMD_INVALID_FW_FRAME_SIZE	0x21	Invalid firmware frame size during firmware upgrade
NACK_SUBCMD_INVALID_FW_SIZE	0x22	Invalid firmware size
NACK_SUBCMD_FW_FLASH_WRITE_FAILED	0x23	Writing to FLASH failed
NACK_SUBCMD_INVALID _FW_CRC	0x24	Invalid firmware checksum during firmware upgrade
NACK_SUBCMD_FW_UPGRADE_NOT_STARTED	0x25	Firmware upgrade is not started before sending firmware packet

Table 5-1 Error Codes

5.2 Event Codes

This section lists the various event codes for the NACK command.

Event ID	Event Name
1	GRANTED_ACCESS
2	GRANTED_ACCESS_DOOR_OPENED
3	GRANTED_ACCESS_DOOR_NOT_OPENED
10	EMERGENCY_OPENING
11	DOOR_OPENED_INTERIOR
12	MECHANICAL_KEY_OVERRIDE
13	DEADBOLT_PROJECTED_FROM_INSIDE
14	DEADBOLT_WITHDRAWN_FROM_INTERIOR
15	DOOR_HELD_OPEN
16	DOOR_FORCED_OPEN
17	DOOR_HELD_OPEN_RESTORED
18	DOOR_FORCED_OPEN_RESTORED
19	MECHANICAL_KEY_OVERRIDE_REVERTED
20	CARD_NOT_ACTIVE
21	CARD_EXPIRED
22	INVALID_BADGE
23	INVALID_AUTHORIZATION
24	INVALID_ISSUE_CODE
25	ACCESS_DENIED_INVALID_TIMEZONE
26	ACCESS_DENIED_PRIVACY
27	ACCESS_DENIED_EMERGENCY_LOCK
28	ACCESS_DENIED_BLOCKED
29	ACCESS_DENIED_LOW_BATTERY
40	LOCK_UNLOCKED_UNDER_OFFICE_FIRST
41	LOCK_LOCKED_UNDER_OFFICE_FIRST
42	LOCK_UNLOCKED_UNDER_AFC
43	LOCK_LOCKED_UNDER_AFC
50	ENTERED_STANDARD_MODE
51	ENTERED_OFFICE_FIRST_MODE
52	ENTERED_OFFICE_MODE
53	ENTERED_BLOCKED_MODE
54	ENTERED_EMERGENCY_LOCK
55	ENTERED_EMERGENCY_UNLOCK
56	ENTERED_FOYER_MODE

Event ID	Event Name
60	AUTOMATIC_STANDARD_DENIED_BLOCKED_MODE
61	AUTOMATIC_OFFICE_DENIED_BLOCKED_MODE
62	AUTOMATIC_OFFICEFIRST_DENIED_BLOCKED_MODE
63	AUTOMATIC_FOYER_DENIED_BLOCKED_MODE
64	AUTOMATIC_STANDARD_DENIED_EMERGENCY_MODE
65	AUTOMATIC_OFFICEFIRST_DENIED_EMERGENCY_MODE
66	AUTOMATIC_OFFICE_DENIED_EMERGENCY_MODE
67	AUTOMATIC_FOYER_DENIED_EMERGENCY_MODE
68	OFFICE_DENIED_LOW_BATTERY
80	UPDATE_OF_LOCK
81	UPDATE_FIRMWARE_READER
82	UPDATE_FIRMWARE_ACU
83	UPDATE_FIRMWARE_WLM
84	UPDATE_RTC
85	DAYLIGHT_SAVINGS_EVENT
86	LOW_BATTERY_EVENT
88	AUDIT_TRIAL_LIMIT
89	LOCK_POWER_UP_PP
90	INITIALIZATION_OF_LOCK_BY_PP
91	LOW_BATTERY_EVENT_RESTORED
100	ACF_INVALID_DATA
101	ACF_INVALID_FACILITY_CODE
102	ACF_INVALID_PARITY
103	ACF_INVALID_DATA_LENGTH
104	ACF_INVALID_TYPE
105	ACF_NOT_FOUND
110	SCF_INVALID_DATA
111	SCF_INVALID_AUTHENTICATION
112	SCF_INVALID_LOCATION
113	SCF_INVALID_CARD
114	SCF_NOT_FOUND

Table 5-2 Event Codes

6 Appendix

6.1 Time Zone record packet formation

The following example details the time zone bit pattern.

Consider the following time zone data with,

1. Start time – 01:02
   End time – 03:04
   Week day = 0x82

2. Start time – 05:06
   End time – 07:08
   Week day = 0x2B

3. Start time – 09:10
   End time – 11:12
   Week day = 0xD4

4. Start time – 13:14
   End time – 15:16
   Week day = 0x1E

5. Start time – 17:18
   End time – 19:20
   Week day = 0xE1

Index = 0x01

Week day bit pattern

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Holiday	Saturday	Friday	Thursday	Wednesday	Tuesday	Monday	Sunday

One Time zone record Bit pattern

Note: Bits in gray are unused bits. Red and Green are used to group the bits to make a byte. Digit in () represents number of bits.

Index
0x01

TimeZone 5				
Week Day	End Time		Start Time	
	Hour(5)	Min(6)	Hour(5)	Min(6)
0xE1	19	20	17	18
1110 0001	00010011	010100	10001	010010
0xE1	0x26	0xA4	0x52	

TimeZone 4				
Week Day	End Time		Start Time	
	Hour(5)	Min(6)	Hour(5)	Min(6)
0x1E	15	16	13	14
0001 1110	00001111	010000	01101	001110
0x1E	0x1E	0x83	0x4E	

TimeZone 3				
Week Day	End Time		Start Time	
	Hour(5)	Min(6)	Hour(5)	Min(6)
0xD4	11	12	9	10
1101 0100	00001011	001100	01001	001010
0xD4	0x16	0x62	0x4A	

TimeZone 2				
Week Day	End Time		Start Time	
	Hour(5)	Min(6)	Hour(5)	Min(6)
0x2B	7	8	5	6
0010 1011	00000111	001000	00101	000110
0x2B	0x0E	0x41	0x46	

TimeZone 1				
Week Day	End Time		Start Time	
	Hour(5)	Min(6)	Hour(5)	Min(6)
0x82	3	4	1	2
1000 0010	00000011	000100	00001	000010
0x82	0x06	0x20	0x42	

The final byte array for one time zone record is shown below:

0x42	0x20	0x06	0x82	0x46	0x41	0x0E	0x2B	0x4A	0x62

0x16	0xD4	0x4E	0x83	0x1E	0x1E	0x52	0xA4	0x26	0xE1	0x01

6.2 Date and Time Example

Below is an example of how date and time is encoded.

The date and time to encode is August 17, 2010 1:42:39 PM

The date and time format is 5 bytes long as shown below:

Year	Month	Day	Hour	Min	Sec	Unused
7 Bits	4 Bits	5 Bits	5 Bits	6 Bits	6 Bits	7 Bits

Table 6-1: Date and time format

The Year starts at the lowest significant byte and the unused bits are part of the highest significant byte. Note that year value is based off of year 2000, i.e. to represent year 2010, the year value should be 10.

Unused	Sec	Min	Hour	Day	Month	Year
7 Bits	6 Bits	6 Bits	5 Bits	5 Bits	4 Bits	7 Bits
0x0	39 = 0x27	42 = 0x2A	13 = 0x0D	17 = 0x11	8 = 0x8	10 = 0xA
00000000	10 0111	10 1010	0 1101	1 0001	1000	000 1010
00000000	100111	101010	01101	10001	1000	0001010
0x01	0x3D	0x4D		0x8C	0x0A	

Table 6-2: Date and time encoding example

The 5 bytes representing the date and time August 17, 2010 1:42:39 PM is

0x0A 0x8C 0x4D 0x3D 0x01