Software Design Specification

Z-Wave 700 Lock Bits and User Data Page Contents

Document No.:	SDS14306
Version:	4
Description:	-
Written By:	JFR;JBU;NOBRIOT;AYURTTAS
Date:	2019-03-13
Reviewed By:	OPP;PSH;JSI;COLSEN;JBU;ALAURBERG;SSE;SRO;JROSEVALL;NOBRIOT;LTHOMSEN;JKA;EFH;AES;SCBROWNI
Restrictions:	Public

Approved by:

Date	CET	Initials	Name	Justification
2019-03-13	05:08:28	NTJ	Niels Johansen	

This document is the property of Silicon Labs. The data contained herein, in whole or in part, may not be duplicated, used or disclosed outside the recipient for any purpose. This restriction does not limit the recipient's right to use information contained in the data if it is obtained from another source without restriction.

REVISION RECORD

Doc. Rev	Date	By	Pages affected	Brief description of changes
1	20180207	JFR	ALL	Initial Draft
2	20181004	JFR	ALL	Lock Bits and User Data page defined
3	20181126	JFR	Section 3 and 4	Alignment of manufacturing tokens and changed offset addresses
4	20190116	MLEDESMA	ALL	Grammar and structure (consistent format) modification

Table of Contents

1 ABBREVIATIONS....1

2 INTRODUCTION....1

2.1 Purpose....1

3 LOCK BITS PAGE EXTENSIONS....2

3.1 TOKEN_MFG_ZW_PUK – Public Key for S2 devices (32 Bytes)....2
3.2 TOKEN_MFG_ZW_PRK – Private Key for S2 devices (32 Bytes)....2
3.3 TOKEN_MFG_ZW_QR_CODE – QR code (90 Bytes)....2

4 USER DATA PAGE EXTENSIONS....4

REFERENCES....5

INDEX....6

1 ABBREVIATIONS

Abbreviation	Explanation
EOF	End Of File
MSB	Most Significant Byte

2 INTRODUCTION

2.1 Purpose

This document defines the Z-Wave extensions to the Lock Bits and User Data Page [1] in the Zen Gecko SoCs. Both the Zen Gecko Lock Bits and the User Data Page must be configured before any application-specific code can be executed.

3 LOCK BITS PAGE EXTENSIONS

The Z-Wave additions to Zen Gecko Lock Bits Page [1] are shown in the table below.

Offset from Lock Bits starting address	Size (Bytes)	Name	Description
0x458	4	TOKEN_MFG_ZW_INITIALIZED	0xFFFFFFFF = Following Z-Wave fields are not initialized
0x3AC	32	TOKEN_MFG_ZW_PRK	Private key
0x3CC	32	TOKEN_MFG_ZW_PUK	Public key
0x3EC	90	TOKEN_MFG_ZW_QR_CODE	QR code string using UTF-8 encoding (Fixed length using Acme Light Dimmer example in SDS13937 - Section 3.3.1)

3.1 TOKEN_MFG_ZW_PUK – Public Key for S2 devices (32 Bytes)

The PUK1-32 field contains the public key of the Curve25519 ECDH keypair used during S2 inclusion. The PUK MUST always be stored in the Z-Wave Lock Bits Page of S2 enabled devices. PUK1 is MSB.

The PUK is generated on the chip and written to this field when the chip is first powered up.

3.2 TOKEN_MFG_ZW_PRK – Private Key for S2 devices (32 Bytes)

The PRK1-32 field contains the private key of the Curve25519 ECDH Key pair used for key exchange in S2 inclusion. The PRK MUST always be stored in the Z-Wave Lock Bits Page of S2 enabled devices. PRK1 is MSB.

The PRK is generated as a hardware-backed random number on the chip and written to this field when the chip is first powered up.

3.3 TOKEN_MFG_ZW_QR_CODE – QR code (90 Bytes)

This field contains the QR code string using UTF-8 encoding. Fixed length using Acme Light Dimmer example in SDS13937 - Section 3.3.1. This field contains ASCII charters in the range ‘0’ to ‘9’.

The QR code is generated on the chip and written to this field when the chip is first powered up.

Once a module has been programmed with a PUK, PRK, and QR code, the QR code must be read out from the lock bits page and printed on the packaging or casing of that particular module. Finally, the Read Back protection for the Lock Bits page must be enabled to protect the PRK.

4 USER DATA PAGE EXTENSIONS

The Z-Wave additions to Zen Gecko User Data Page [1] are shown in the table below.

Offset from User Data starting address	Size (Bytes)	Name	Description
0x068	4	TOKEN_MFG_COUNTRY_FREQ	To set the country frequency, add a *"#define APP_FREQ"* to one of the values defined in the ZW_Region_t enum in *<sdk>/Z-Wave/Include/ZW_radio_api. The define must be placed in config_app.h, present in each application. The path is <sdk>/app/TestApplications/<app_name>/ config_app.h*
0x06C	4	TOKEN_MFG_HW_VERSION	Hardware version value is the version of the entire product. It is reported in command class Version Report Command. For details, refer to document SDS13782.
0x080	16	TOKEN_MFG_SERIAL_NUMBER	Serial number value of the entire product in binary representation. It is reported in command class Device Specific Report Command. For details, refer to document SDS13782.
0x070	16	TOKEN_MFG_PSEUDO_ RANDOM_NUMBER	Pseudo Random value in binary representation. It is reported in command class Device Specific Report Command. For details, refer to document SDS13782.

The Z-Wave User Data Page is from 0x0FE00000 through 0x0FE00800.

REFERENCES

[1] Silicon Labs, AN961: Bringing Up Custom Devices for Mighty Gecko and Flex Gecko Families.
[2] Silicon Labs, SDS13782, Software Design Specification, Z-Wave Management Command Class Specification.
[3] Silicon Labs, SDS13937, Software Design Specification, Node Provisioning QR Code Format (S2, SmartStart).

INDEX

The Index list is empty