User Guide

BOOT Interface Instruction User Guide

Introduction

User guide mainly describes the BOOT interface instructions of N32G45x series, N32G4FR series and N32WB452 series MCU, which is easy to download and develop by using the National technology BOOT Loader.

This document is only applicable to Nsing MCU products. Currently, the supported product series include N32G45x series, N32G4FR series, N32WB452 series.

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

Contents

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

1 BOOT Brief Introductions

The user guide applicable to N32G45x, N32G4FR, N32WB452 series chips, provids user download function instructions, as follows:

- Interface support:
  - Supports USART1 interface. Refer Section 2.2.1 for details about the baud rate
  - Supports USB interface, download using DFU protocol

    The physical interface list is as follows:

Series/Model	USART1-TX	USART1-RX	USB-DP	USB-DM
N32G452/5/7 series	PA9	PA10	PA12	PA11
N32WB452REQ6 N32WB452LEQ6	PA9	PA10	PA12	PA11
N32WB452CEQ6	PB6	PB7	PA12	PA11

  - Difference between USART automatic baud rate detection and USART baud rate negotiation:

    1. USART baud rate automatic detection:

       After power-on, 0x7F is transmitted through the USART of the upper computer, and MCU detects the data transmitted by the upper computer and identifies the baud rate of USART communication. This method is only applicable to BOOT V2.1.

    2. USART baud rate negotiation:

       After power-on, when the upper computer communicates with the universal MCU through the USART, the baud rate of 9600bps is used for communication. Run the CMD_SET_BR command to reset the baud rate, and the response will take effect after a successful response is returned. If the specified baud rate is not supported, the state will return to failure.

- Supports Flash erasure (make sure the page has been erased before downloading);
- Supports data or program download function;
- Supports download data CRC32 verification;
- Supports power-on BOOT self-verification.
- Supports jump to the user area for execution.
- Supports software reset chip operation;
- Supports Flash partition and key authentication during partition erase or programming
- Supports partition key update;

- Support encrypted download (AES-128 ECB)

This document describes in detail the functions, implementation and usage of the universal MCU chip BOOT.

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

2 BOOT Process and Command Processing

The BOOT program supports downloading user programs and data through USART/USB interfaces.During power-on, the interface is automatically identified.The following describes the command processing process.

2.1 Commands and Data Structures

2.1.1 Commands List

Table 2-1 Command Definition

Name of the Command	Key Value	Brief Description
CMD_SET_BR	0x01	Set the baud rate of the USART (Valid only when USART are used)
CMD_GET_INF	0x10	Read chip model index, BOOT version number, chip ID
CMD_GET_RNG	0x20	Get random number
CMD_KEY_UPDATE	0x21	Update the encryption download key or partition authentication key
CMD_FLASH_ERASE	0x30	Erase FLASH
CMD_FLASH_DWNLD	0x31	Download user programs to FLASH
CMD_DATA_CRC_CHECK	0x32	CRC verification download user program
CMD_OPT_RW	0x40	Read/configure option bytes (including read protection level, FLASH page write protection, Data0/1 configuration, USER configuration)
CMD_USERX_OP	0x41	Get the partition USERX size and configure the partition USERX size
CMD_SYS_RESET	0x50	The system reset
CMD_APP_GO	0x51	Jump to user area to execute the program

2.1.2 Data Structure

This section describes some conventions in the following sections. "<>" represents fields that must be included, and "()"

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road, Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

represents fields that must be included according to parameters.

- **Logical layer instruction data structure**
  - Upper instruction structure:

    <CMD_H + CMD_L + LEN + Par> + (DAT).

    CMD_H indicates the level-1 command field, and CMD_L indicates the level-2 command field.LEN indicates the length of data to be transmitted. Par represents a four-byte command parameter; DAT represents the specific data transmitted from the upper level instruction to the lower level;

  - Lower response structure:

    < CMD_H + CMD_L + LEN > + (DAT) + <CR1+CR2>.

    CMD_H indicates the level-1 command field, and CMD_L indicates the level-2 command field. The command fields at the lower level are the same as those at the upper level.LEN indicates the length of data to be transmitted. DAT indicates the specific data that the lower layer replies to the upper layer.CR1+CR2 indicates the command execution result returned to the upper layer. If the level-1 and level-2 command fields do not belong to any command, BOOT replies CR1=0xBB and CR2 = 0xCC.

- **Physical layer instruction data structure**
  - USB interface instruction data structure

    USB interface adopts DFU protocol, refer to 'DFU_1.1' for details:

    1. The upper computer transmitted the upper instruction:

       Use the DFU_DNLOAD request to transmitted the upper-layer instruction data.

    2. The upper computer receive the lower-layer response command:

       Use the DFU_GETSTATUS request to receive the lower-layer reply instruction data.

  - USART command data structure:

    1. The upper computer issues the upper instruction:

       STA1 + STA2 + {superstructure} + XOR.

    STA1 and STA2 are the start bytes of commands transmitted through the USART. STA1=0xAA and STA2=0x55.The chip can use it to identify the serial port data stream transmitted by the upper computer.

    XOR represents the XOR operation value of the previous command byte (STA1 + STA2 + {superstructure}).

    2. The upper computer receives the lower-layer response:

       STA1 + STA2 + {lower response structure} + XOR.

    STA1 and STA2 are the start bytes of commands transmitted through the serial port. STA1=0xAA and STA2=0x55.It is used for the host computer to identify the chip and transmitted serial port data stream

    XOR represents the XOR operation value of the previous command byte (STA1 + STA2 + {underlying reply structure}).

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road, Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

2.2 Command Description

2.2.1 CMD_SET_BR

This command is used to modify the USART baud rate, only applicable to BOOT versions that support baud rate negotiation, and effective only during serial port downloads.

Upper-level instructions:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x01 Level-1 command field							
1(CMD_L)	0x00 Level-2 command field							
2~3(LEN)	Length of transmitting data: 0x00, 0x00							
4~7(Par)	Par[0~3] : set baud rate parameters							
(DAT)	None							

- Par[0~3], the USART baud rate negotiation value can be set to the maximum, the setting range is 2.4Kbps ~ 4.5Mbps
- Reserved value: 0x00

Underlying response:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x01 Level-1 command field							
1(CMD_L)	0x00 Level-2 command field							
2~3(LEN)	Length of transmitting data: 0x00, 0x00							
(DAT)	There is no							
4(CR1)	Status byte 1							
5(CR2)	Status byte 2							

- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  - Return success: status flag bit (0xA0, 0x00).
  - Return failure: status flag bits (0xB0, 0x00).

The following are the baud rate values supported by baud rate negotiation (√ : supported; / : not supported) :

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road, Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

- The baud rates supported by the BOOT V2.1 version of N32G45x, N32G4FR, and N32WB452 series MCUs.

Clock Parameters (MHz)		Baud Rate								
		2400	4800	9600	14400	19200	38400	57600	115200	128000
External Clock	4	√	√	√	√	√	√	√	√	√
	6	√	√	√	√	√	√	√	√	√
	8	√	√	√	√	√	√	√	√	√
	12	√	√	√	√	√	√	√	√	√
	16	√	√	√	√	√	√	√	√	√
	24	√	√	√	√	√	√	√	√	√
	32	√	√	√	√	√	√	√	√	√
Internal Clock	8	√	√	√	√	√	√	√	√	√

- The baud rates supported by the BOOT V2.2 version of N32G45x, N32G4FR, and N32WB452 series MCUs.

	Baud Rate

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

Clock Parameters (MHz)		2400	4800	9600	14400	19200	38400	57600	115200	128000	256000	576000	923076	1M	2M	2.25 M
External Clock	4	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	6	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	8	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	12	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	16	√	√	√	√	√	√	√	√	√	√	√	√	√	/	/
	24	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	32	√	√	√	√	√	√	√	√	√	√	√	√	√	/	/
Internal Clock	8	√	√	√	√	√	√	√	√	√	√	√	√	√	/	/

- The baud rates supported by the BOOT V2.3 and V2.4 version of N32G45x, N32G4FR, and N32WB452 series MCUs.

Clock Parameters (MHz)	Baud Rate																	
	2400	4800	9600	14400	19200	38400	57600	115200	128000	256000	576000	923076	1M	2M	2.25 M	3M	4M	4.5 M

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

External Clock	4	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	6	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	8	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	12	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	16	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	24	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	32	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
Internal Clock	8	√	√	√	√	√	√	√	√	√	√	√	√	√	/	/	/	/	/

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

2.2.2 CMD_GET_INF

The command reads the BOOT version number, chip model index, chip ID, and chip serialization information.

Upper-level instructions:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x10 Level-1 command field							
1(CMD_L)	0x00 Level 2 command field							
2~3 (LEN)	Length of transmitting data							
4~7(Par)	reserved							
(DAT)	None							

- Reserved value: 0x00.
- LEN is the length of transmitting data: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] +(LEN[1]<<8).

Underlying response:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x10 Level-1 command field							
1(CMD_L)	0x00 Level 2 command field							
2~3 (LEN)	The length of the data							
4~54(DAT)	BOOT version number, chip model index, chip ID, and chip serialization							
55(CR1)	Status byte 1							
56(CR2)	Status byte 2							

- The procedure byte (CMD_H) corresponds to the upper instruction (CMD_H).
- LEN is the length of transmitting data: 0x33(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- DAT[0]: Chip model index

  Product number: 0x01
- DAT[1]: 0xXY, BOOT command set version number (BCD code)

  0x10: indicates the command set version used by BOOT, indicating that V1.0 command set version is used
- DAT[2] : BOOT code version
- DAT[3~50] 48Byte
  - DAT[3~18] : 16Byte UCID (for example, 36 01 01 A0 15 50 36 33 50 30 35 30 30 30 09 7D 22)
  - DAT[19~30] : 12Byte Chip ID(UID) (example: 36 01 01 50 36 33 50 30 35 09 7D 22)
  - DAT[31~34] : 4Byte DBGMCU_IDCODE (example: 01 54 87 F8)

    UCID, UID, and DBGMCU_IDCODE are defined in the UM_N32G45x Series User Manual, UM_N32G4FR Series User Manual, and UM_N32WB452 Series User Manual.
  - DAT[35~50] : 16 bytes (reserved);
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  - Return success: status flag bit (0xA0, 0x00).

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road, Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

- Return failure: status flag bits (0xB0, 0x00).

2.2.3 CMD_KEY_RNG

Gets the random number of the key that the user needs to verify.

Upper-level instructions:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x20 Level-1 command field							
1(CMD_L)	0x00 Level 2 command field							
2~3(LEN)	Length of transmitting data							
4~7(Par)	reserved							
(DAT)	None							

- Reserved value: 0x00;
- LEN is the length of transmitting data: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).

Underlying response:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x20 Level-1 command field							
1(CMD_L)	0x00 Level 2 command field							
2~3(LEN)	Length of transmitting data							
4~19(DAT)	A truly random number of 16Bytes							
20(CR1)	Status byte 1							
21(CR2)	Status byte 2							

- LEN is the length of transmitting data: 0x10(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- The true random number of 16 bytes is generated by the chip.
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  - Return success: status flag bit (0xA0, 0x00).
  - Return failure: status flag bits (0xB0, 0x00).

2.2.4 CMD_KEY_UPDATE

The user can update the encryption download key and partition authentication key. Before updating, the user needs to use CMD_KEY_RNG to obtain a random number. The random number is used by the upper computer to produce a 16Bytes old key authentication value, which is then transmitted to the BOOT by using the CMD_KEY_UPDATE command. This verifies whether to update the key.The new key needs to be decrypted with the old key.

Upper-level instructions:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x21 Level-1 Command field							
1(CMD_L)	Secondary command field: KEY index ID							

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

2~3(LEN)	Length of transmitting data
4~7(Par)	Reserved value: 0x00
8~55(DAT)	DAT[0~15] : 16Bytes old key authentication value
	DAT[16-31] : indicates the new encryption value of 16 bytes
	DAT[32 to 47] : indicates the CRC32 encryption value 4Bytes CRC32 check value (old key + new key) + 12Bytes fill the value 0x00 The 16Bytes of data are then encrypted with the old key

- CMD_L: indicates the ID of the key index to be updated
  - ID(0x00-0x1f) : indicates the ID of the key index.
- LEN is the length of transmitting data: 0x30(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Reserved value: 0x00.
- DAT[32 to 47] : indicates the CRC32 verification value.
- DAT[0~15] : a 16-bit random number obtained by CMD_KEY_RNG and an authentication value generated by the old key.
- DAT[16-31] : indicates a new key encrypted with the old key. BOOT decrypts the new key with the old key and then stores it.

Underlying response:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x21 Level-1 Command field							
1(CMD_L)	Secondary command field: key ID							
2~3(LEN)	Length of transmitting data							
(DAT)	There is no							
4(CR1)	Status byte 1							
5(CR2)	Status byte 2							

- LEN is the length of transmitting data: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  - Return success: status flag bit (0xA0, 0x00).
  - Return failure: status flag bits (CR1, CR2)
    1. (0xB0, 0x00) : return failed.
    2. (0xB0, 0x10) : the key index ID range is incorrect.
    3. (0xB0, 0x11) : the CRC check of the new key is incorrect.
    4. (0xB0, 0x20) : authentication of the old key fails.
    5. (0xB0, 0x21) : the number of old key authentication failures exceeds the limit.
    6. (0xB0, 0x3F) : failed to update the management information.

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

2.2.5 CMD_FLASH_ERASE

BOOT erases the FLASH by page. The page address number and page number can be specified by the user. The erasure space cannot exceed the entire Flash space and at least one page must be erased.

If the authentication function is enabled, the CMD_KEY_RNG command is used to obtain a random number and perform authentication before erasing the function.

Upper-level instructions:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x30 Level-1 command field							
1(CMD_L)	Level 2 command field: Erase partition number							
2~3(LEN)	Length of transmitting data							
4~7(Par)	Page address number 2 bytes: 0 to 255 Page Number 2 bytes :1 to 256							
8~23(DAT)	DAT[0:15] : 16 bytes User1/2/3 partition authentication key authentication value, used only when authentication is enabled							

- CMD_L: erases the partition number
  - 0 x00 = USER1;
  - 0 x01 = USER2;
  - 0 x02 = USER3;
- LEN is the length of transmitting data: 0x10(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- The erase address and range consist of four bytes in the Par field

  Par[0~1] : page address number 2 bytes (0~255)

  Page address = Par [0] + (Par [1]<<8);

  Par[2~3] : Page number 2 bytes (1~256)

  Page count = Par [2] + (Par [3]<<8);

  The beginning address of page 0 is 0x0800_0000. The number of subsequent pages is incremented by 1, and the first address is incremented by 0x800.

  For example :The beginning address of page 1 is 0x0800_0000 + 1*0x800 = 0x0800_0800

  The beginning address of page 2 is 0x0800_0000 + 2*0x800 = 0x0800_1000

  The entire address range erased

  For example, the page address is 0x01 and the number of pages is 0x02

  Erasing address range:

  (0x0800_0000 + 1*0x800) ~ (0x0800_0000 + 1*0x800 + 2*0x800)

  That is, (first address of the page number) to (First address of the page number + number of pages x page size)

Underlying response:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road, Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

0(CMD_H)	0x30 Level-1 command field
1(CMD_L)	Secondary command field: Erase area
2~3(LEN)	Length of transmitting data
(DAT)	None
4(CR1)	Status byte 1
5(CR2)	Status byte 2

- LEN is the length of transmitting data: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  - Return success: status flag bit (0xA0, 0x00).
  - Return failure: status flag bits (CR1, CR2).
    1. (0xB0, 0x00) : return failed.
    2. (0xB0, 0x20) : key authentication fails.
    3. (0xB0, 0x21) : the number of key authentication failures exceeds the limit.
    4. (0xB0, 0x30) : the erased Flash page is protected by RDP.
    5. (0xB0, 0x31) : the erased Flash page is protected by WRP.
    6. (0xB0, 0x32) : deletes the Flash page to be partitioned.
    7. (0xB0, 0x34) : erasing the Flash address range exceeds the threshold (indicates that the Flash size exceeds the threshold).
    8. (0xB0, 0x37) : failed to erase the Flash.
    9. (0xB0, 0x3F) : failed to update the management information.
    10. (0xB0, 0x3F) : Failed to update the management information.

2.2.6 CMD_FLASH_DWNLD

This command provides the user to download the code into the specified FLASH, and the data length must be 16 bytes aligned (if less than 16 byte, 0x00 will be automatically added by the upper computer), which is provided by the upper-layer command.

When authentication or encryption is enabled, the CMD_KEY_RNG command is used to obtain a random number before authentication or encryption is enabled. For partition authentication and encryption download, you need to provide the partition number. The data downloaded with encryption is first decrypted into plaintext using the encryption download key (the key corresponding to the partition authentication), and then written to FLASH.

Upper-level instructions:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
1(CMD_H)	0x31 Level-1 command field							
2(CMD_L)	Secondary command field: Download partition number							
3~4(LEN)	Length of transmitting data							
5~8(Par)	Start address for downloading the FLASH							
8~23+N(DAT)	DAT[0:15] : 16 bytes Key authentication value for user1/2/3 partition authentication DAT[16~16+N] : Specific data downloaded (encrypted or unencrypted)							

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

	DAT[N+1 to N+4] : indicates the 4 byte CRC32 check value of unencrypted data

- CMD_L: indicates the number of the download partition
  - 0 x00 = USER1;
  - 0 x01 = USER2;
  - 0 x02 = USER3;
- LEN is the length of transmitting data: 0xXX(LEN[0]), 0xXX(LEN[1]), LEN = LEN[0] + (LEN[1]<<8)
- Par [0 ~ 3] : download the starting address of the Flash, synthetic rules to address = Par [0] 8 | | Par [1] < < Par [2] | Par [3] < < < < 16 to 24.
- DAT [0:15], Reserved.
- DAT[16~16+N] : Specific data to be downloaded
  - USB: a maximum of 128 bytes, 15<=N<=143, N+1 must be a multiple of 16.
  - USART: contains a maximum of 128 bytes. 15<=N<=143. N+1 must be a multiple of 16.

DAT[N+1 to N+4] : indicates the 4 byte CRC32 check value of unencrypted data.

Underlying response:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x31 Level-1 command field							
1(CMD_L)	Secondary command field: Download partition number							
2(LEN)	Length of transmitting data							
(DAT)	There is no							
3(CR1)	Status byte 1							
4(CR2)	Status byte 2							
5(XOR)	Xor result							

- LEN is the length of transmitting data: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  - Download success: status flag bit (0xA0, 0x00).
  - Download failed: status flag bit (CR1, CR2).
    1. (0xB0, 0x00) : return failed.
    2. (0xB0, 0x20) : key authentication fails.
    3. (0xB0, 0x21) : the number of key authentication failures exceeds the limit.
    4. (0xB0, 0x30) : the downloaded Flash address is protected by RDP.
    5. (0xB0, 0x31) : the downloaded Flash address is protected by WRP.
    6. (0xB0, 0x32) : the downloaded Flash address is protected by a partition.
    7. (0xB0, 0x33) : download Flash address range across partitions;
    8. (0xB0, 0x34) : the address range of the downloaded Flash exceeds the threshold.
    9. (0xB0, 0x35) : download Flash start address is not 16-byte alignment;
    10. (0xB0, 0x36) : the downloaded Flash data length is not a multiple of 16.

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

11. (0xB0, 0x37) : programming the Flash fails.
12. (0xB0, 0x3F) : the management information fails to be updated.

2.2.7 CMD_DATA_CRC_CHECK

This command is used to check whether the downloaded data is correct. Considering the download speed and low probability of download failure, the CRC check is performed after the downloaded data is complete. The upper-layer command must provide the CRC value, start address, and check length of the downloaded data.

When authentication is enabled, the CMD_KEY_RNG command is used to obtain a random number and perform authentication before CRC verification.

Upper-level instructions:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x32 Level-1 command field							
1(CMD_L)	Level 2 command field: Parity partition number							
2~3(LEN)	Length of transmitting data							
4~7(Par)	32-bit CRC check value							
8~31(DAT)	DAT[0:15] : 16 bytes Key authentication value for user1/2/3 partition authentication DAT[16:19] : indicates the start IP address of the verification DAT[20:23] : parity length (in bytes, minimum length 2KB)							

- CMD_L: indicates the verification partition number
  - 0 x00 = USER1;
  - 0 x01 = USER2;
  - 0 x02 = USER3;
- LEN is the length of transmitting data: 0x18(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Par[0~3] : 32 bit CRC checksum value, the synthetic rules for CRC32 = Par[0] | Par[1]<<8 | Par[2]<<16 | Par[3]<<24.
- DAT[0:15] : authentication key authentication value
- DAT[16~19]: check the starting address, the synthesis rules to address = DAT [16] | DAT [17] < < 8 | DAT [18] < < 16 | DAT [19] < < 24, the Address can only be in the range of the FLASH.
- DAT[20~23] : check length, its synthesis rules for CRC_LEN = DAT [20] | DAT [21] < < 8 | DAT [22] < < 16 | DAT [23] < < 24, CRC_LEN is only within the effective range, length is larger than 2 KB, and is a multiple of 16.

Underlying response:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x32 Level-1 command field							
1(CMD_L)	Level 2 command field: Parity partition number							
2~3(LEN)	Length of transmitting data							
(DAT)	None							
4(CR1)	Status byte 1							
5(CR2)	Status byte 2							

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

- LEN is the length of transmitting data: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  - Verification succeeded: status flag bit (0xA0, 0x00).
  - Verification failure: status flag bits (CR1, CR2)
    1. (0xB0, 0x00) : return failed.
    2. (0xB0, 0x20) : CRC verification key authentication fails.
    3. (0xB0, 0x21) : the number of CRC key authentication failures exceeds the limit.
    4. (0xB0, 0x32) : indicates that CRC check addresses are protected by partitions.
    5. (0xB0, 0x33) : indicates that the address range of CRC check is across partitions.
    6. (0xB0, 0x34) : indicates that the address range of CRC check exceeds the threshold.
    7. (0xB0, 0x35) : indicates that CRC addresses are not aligned with 16 bytes.
    8. (0xB0 or 0x36) : indicates that the CRC check length is not a multiple of 16 or less than 2KB.
    9. (0xB0, 0x38) : CRC verification fails.
    10. (0xB0, 0x3F) : the management information fails to be updated.

2.2.8 CMD_OPT_RW

This command is used for option byte read and write (including read protection level, FLASH page write protection, datA0/1 configuration, and USER configuration).

Upper-level instructions:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x40 Level-1 command field							
1(CMD_L)	Secondary command field							
2~3(LEN)	Length of transmitting data							
4~7(Par)								
8~27(DAT)	Option byte configures 20 bytes							

- CMD_L Secondary command field:
  - 0x00: Gets option bytes.
  - 0x01: Configuration option byte.
  - 0x02: Configuration option byte, reset again.
- LEN is the length of transmitting data: 0x14(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- DAT[0 to 19] : Option byte 20 bytes

  RDP, nRDP, USER, nUSER, Data0, nData0, Data1, nData1, WRP0, nWRP0, WRP1, nWRP1, WRP2, nWRP2, WRP3, nWRP3, RDP2, nRDP2, Reserved, nReserved;
  - CMD_L = 0x00: all values are 0x00.
  - CMD_L = 0x01/0x02: Configuration option bytes are the values to be written.

Underlying response:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road, Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

0(CMD_H)	0x40 Level-1 command field
1(CMD_L)	Secondary command field
2~3(LEN)	Length of transmitting data
4~23(DAT)	Option byte configures 20 bytes
24(CR1)	Status byte 1
25(CR2)	Status byte 2

- LEN is the length of transmitting data: 0x14(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- DAT[0 to 19] : The current option contains 20 bytes

  RDP, nRDP, USER, nUSER, Data0, nData0, Data1, nData1, WRP0, nWRP0, WRP1, nWRP1, WRP2, nWRP2, WRP3, nWRP3, RDP2, nRDP2, Reserved, nReserved;
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  - Return success: status flag bit (0xA0, 0x00).
  - Check failure: status flag bits (CR1, CR2)
    1. (0xB0, 0x00) : return failed.

2.2.9 CMD_USERX_OP

This command is used to read or configure the size of the user1/2/3 partition. After the partition is configured, the partition is automatically sealed.The user1/2/3 partition can be configured only once. The software determines whether the NVR MMU partition has been configured (process variables or random delay are added to determine the NVR value).

The recommended configuration process is as follows:

- If you need to divide two areas, configure USER3 (automatic sealing after configuration completion).If you want to also seal USER1, configure USER1 again.The size of USER1 + USER3 must be the size of the entire FLASH;
- If you nee to divide three areas, configure USER3 (automatic sealing after configuration completion) and then USER2 (automatic sealing after configuration completion). If you want to also seal USER1, configure USER1 again.The size of USER1 + USER2 + USER3 must be the size of the entire FLASH.

Upper-level instructions:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x41 Level-1 command field							
1(CMD_L)	Secondary command field							
2~3(LEN)	Length of transmitting data							
4~7(Par)	Par[0] : Partition User1/2/3							
	Par [1] : Partition user1/2/3 size							
	Par [2] : Partition authentication key index ID							
	Par [3] : Partition authentication and encryption download enable configuration							
DAT	None							

- CMD_L Secondary command field:

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road, Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

- 0x00: Read partition user1/2/3 size configuration.
- 0x01: Partition user1/2/3 size, key ID, and partition authentication/encryption download are enabled.

- LEN is the length of transmitting data: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Par[0] : Partition number
  - 0x00: partition USER1.
  - 0x01: partition USER2.
  - 0x02: partition USER3.
- Par [1] :
  - CMD_L = 0x00:0x00.
  - CMD_L = 0x01: partition user1/2/3 size configuration

  Input range for partition size: 0x1(16KB)... 0x1F(496KB), 0x20(512KB), USER1 + USER2 + USER3 = 512KB;The user area user1/2/3 is automatically sealed after size configuration.

  Partition size and address determined

  The start address of the partition is 0x0800_0000, and the end address of the partition is the start address plus the total FLASH capacity (for example, if the FLASH capacity is 512 KB, the end address is 0x0800_0000 + 512*0x800 = 0x0808_0000).

  If USER1 is partitioned, the partition address of USER1 ranges from 0x0800_0000 to (0x0800_0000 + USER1_Size*0x4000).

  If USER3 is partitioned, the partition address of USER3 ranges from (0x0808_0000 - USER3_Size*0x4000) to 0x0800_8000 (for example, the last FLASH address is 0x0808_0000).

  The initial address of the partition of USER2 is the last address of USER1 and the first address of USER3.If USER1 has no partition, the first address of USER2 needs to be determined by USER2_Size.
- Par [2] :
  - CMD_L = 0x00:0xFF.
  - CMD_L = 0x01:0x00~0x1F Encrypted Download/Partition authentication key index ID,

  0xFF indicates that the index ID is not configured. If the corresponding USERX is not configured with an ID, the value of Par[3] is not judged.
- Par [3] :

  Enable configuration of partition authentication and encrypted download, 0xXY

  X = 0 - If zone authentication is not enabled, set this parameter to 1.

  X = 1 - If zone authentication is enabled, the value cannot be 0.

  Y = 0 - If encrypted download is not enabled, set this parameter to 1.

  Y = 1 - Encrypted download is enabled and cannot be set to 0.
  - CMD_L = 0x00: read status, retain value 0x00;
  - CMD_L = 0x01: configuration status, configuration value 0xXY;

Underlying response:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x41 Level-1 command field							
1(CMD_L)	Secondary command field							
2~3(LEN)	Length of transmitting data							

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road, Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

4~7(DAT)	DAT[0] : partition user1/2/3
	DAT[1] : partition user1/2/3 size
	DAT [2] : Indicates the configuration status of the partition authentication key index ID
	DAT [3] : Read partition authentication and encryption download enable configuration
8(CR1)	Status byte 1
9(CR2)	Status byte 2

- LEN is the length of transmitting data: 0x02(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- DAT[0] : indicates the partition number
  - 0x00: partition USER1.
  - 0x01: partition USER2.
  - 0x02: partition USER3.
- DAT[1] : Read the current partition user1/2/3 size

  Partition size output range: 0x0(0KB), 0x1(16KB)... 0x1F (496 KB), 0x20 (512 KB).

  0x0 indicates that the partition size is not configured. USER1 + USER2 + USER3 = 512KB.
- DAT [2].
  - 0x00, the ID has been configured.
  - 0xFF, ID is not configured
- DAT [3] :

  Read partition authentication and encryption download enable configuration, 0xXY

  X = 0 - If zone authentication is not enabled, set this parameter to 1.

  X = 1 - If zone authentication is enabled, the value cannot be 0.

  Y = 0 - If encrypted download is not enabled, set this parameter to 1.

  Y = 1 - Encrypted download is enabled and cannot be set to 0.
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  - Return success: status flag bit (0xA0, 0x00).
  - Return failure: status flag bit (0x70, 0x00)
    1. (0xB0, 0x00) : return failed.
    2. (0xB0, 0x10) : The key index ID range is incorrect.
    3. (0xB0, 0x3A) : The partition size has been configured and cannot be configured again.
    4. (0xB0, 0x3B) : the partition size is incorrectly configured. USER1 + USER2 + USER3 = FLASH capacity. The minimum value for user1/2 /2/3 is 0x01(16KB).
    5. (0xB0, 0x3C) : The partition configuration sequence is incorrect and USER1 or USER3 must be configured first.
    6. (0xB0, 0x3D) : The partition key index ID fails to be configured or has been configured.
    7. (0xB0, 0x3E) : The configuration of zone authentication and encryption download fails or has been configured.
    8. (0xB0, 0x3F) : Failed to update the management information.

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

2.2.10 CMD_SYS_RESET

This command is used to reset the BOOT program.

Upper-level instructions:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x50 Level-1 command field							
1(CMD_L)	0x00 Level 2 command field							
2~3(LEN)	Length of transmitting data							
4~7(Par)	reserved							
(DAT)	None							

- Reserved value: 0x00;

Underlying response:

Byte \ Bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x50 Level-1 command field							
1(CMD_L)	0x00 Level 2 command field							
2~3(LEN)	Length of transmitting data							
(DAT)	None							
4(CR1)	Status byte 1							
5(CR2)	Status byte 2							

- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  - Return success: status flag bit (0xA0, 0x00).
  - Return failure: status flag bits (0xB0, 0x00).

2.3 Returns the Status Word Description

2.3.1 Returns the Success Status Word

Return success: status flag bit (0xA0, 0x00). It indicates that the command delivered by the upper layer is successfully executed. The returned success status word contains the returned value of the read, update, and configuration commands.

2.3.2 Returns the Failure Status Word

Return failure: status flag bits (0xB0, 0x00).It indicates that the command delivered by the upper layer fails to be executed due to other reasons (such as incorrect command acceptance format or timeout). Failure status word is returned.

2.3.3 Return Other Status Words

The following return status words also indicate return failure. The second byte status word indicates a different error type.

- (0xB0, 0x10) : The key index ID range is incorrect.
- (0xB0, 0x11) : The CRC check of the new key is incorrect.
- (0xB0, 0x20) : Key authentication fails.

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road, Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

- (0xB0, 0x21) : The number of key authentication failures exceeds the limit.
- (0xB0, 0x30) : Eraser/download FLASH page protected by RDP;
- (0xB0, 0x31) : Erasing/downloading FLASH pages are protected by WRP.
- (0xB0, 0x32) : Erase/download /CRC addresses are protected by partitions.
- (0xB0, 0x33) : erase/download /CRC check address range across partitions;
- (0xB0, 0x34) : The address range of erase/download /CRC is out of bounds (indicating that the size of the FLASH exceeds the limit).
- (0xB0, 0x35) : The start address of erase/download /CRC is not 16-byte alignment;
- (0xB0, 0x36) : Indicates that the length of the downloaded /CRC data is not a multiple of 16.Data length indicates the length of erasing FLASH, or the length of downloading code to FLASH, or the length of FLASH CRC values;
- (0xB0, 0x37) : Erasing or downloading the FLASH program fails.
- (0xB0, 0x38) : CRC verification fails.
- (0xB0, 0x39) : A partition has been configured and the read protection level cannot be changed from L1 to L0.
- (0xB0, 0x3A) : The partition has been configured and cannot be configured again.
- (0xB0, 0x3B) : The partition size is incorrect. USER1 + USER2 + USER3 = FLASH capacity.
- (0xB0, 0x3C) : The partition configuration sequence is incorrect and USER1 or USER3 must be configured first.
- (0xB0, 0x3D) : The partition key index ID fails to be configured or has been configured.
- (0xB0, 0x3E) : The configuration of zone authentication and encryption download fails or has been configured.
- (0xB0, 0x3F) : Failed to update the management information.
- (0xBB, 0xCC) : The level 1 and level 2 command fields do not belong to any command.

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

3 BOOT Usage Instructions

3.1 Upper Computer Control Process

Upper computer support user erasing FLASH area, user code download, download code integrity check.By reading partition information, the upper computer automatically identifies the address range of erasing, downloading and checking entered by the user and requires authentication.

The upper computer supports users to choose whether to enable encryption download to protect user code.

The upper computer supports the user to read and configure the partition user1/2/3 size.The partition size cannot be changed after being configured.

The upper computer supports users to update the security key (used for partition authentication and encryption download).

The upper computer supports user update option byte reading and modification.

The upper computer supports software reset command and jump USER1 reset program entry address execution command.

BOOT: after you enter to the BOOT, The chip can interact with the PC TOOL through the USART1 interface or USB interface.

Chip firmware integrity check: Select BOOT from the system storage area, and BOOT automatically verifies the integrity. If the verification fails, an infinite loop will be entered, and subsequent functions cannot be used.

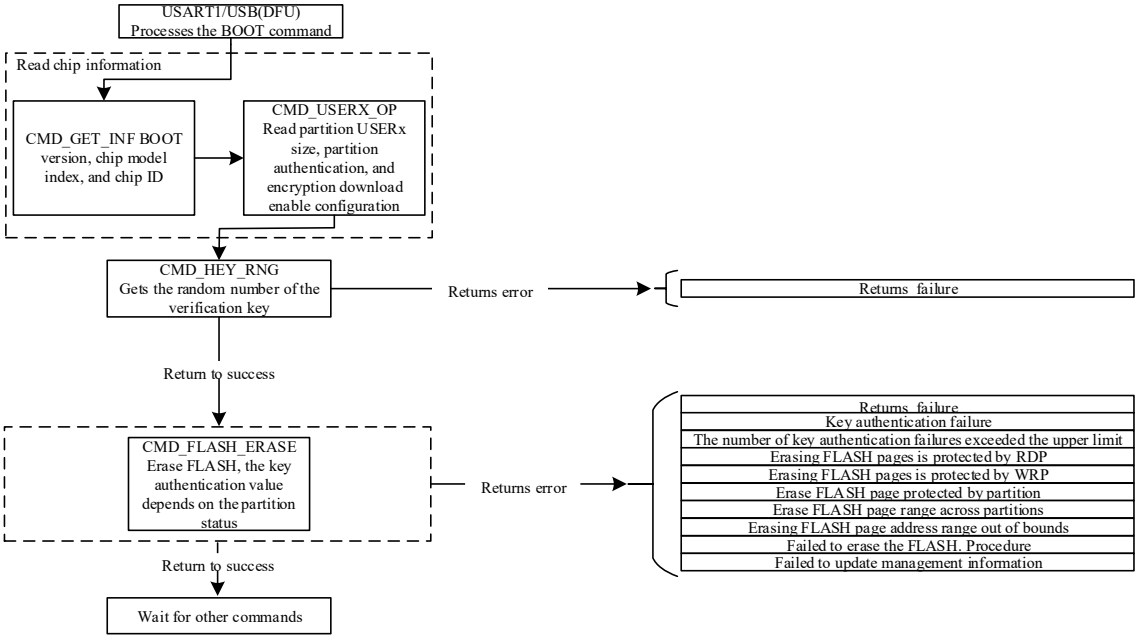
Command set interaction: The PC TOOL transmits different commands based on the command set supported by the BOOT to use corresponding functions.

- Read BOOT version number, chip model index, chip ID;
- Get 16byte true random number;
- Update the security key (for partition authentication and encrypted download);
- Erase FLASH;
- Download user programs to FLASH;
- CRC verification of downloaded user programs;
- Read/configure option bytes (including read protection level, FLASH page write protection, datA0/1 configuration, USER configuration);
- Get partition USERX size, configure partition USERX size;
- System reset, you can reset the BOOT program to run again;
- Jump to USER1 reset program entry address, jump to the reset program entry address of code which is downloaded to USER1 partition

3.1.1 Erase Command Control Flowchart

Figure 3-1 Flowchart of Erasing Command Control

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

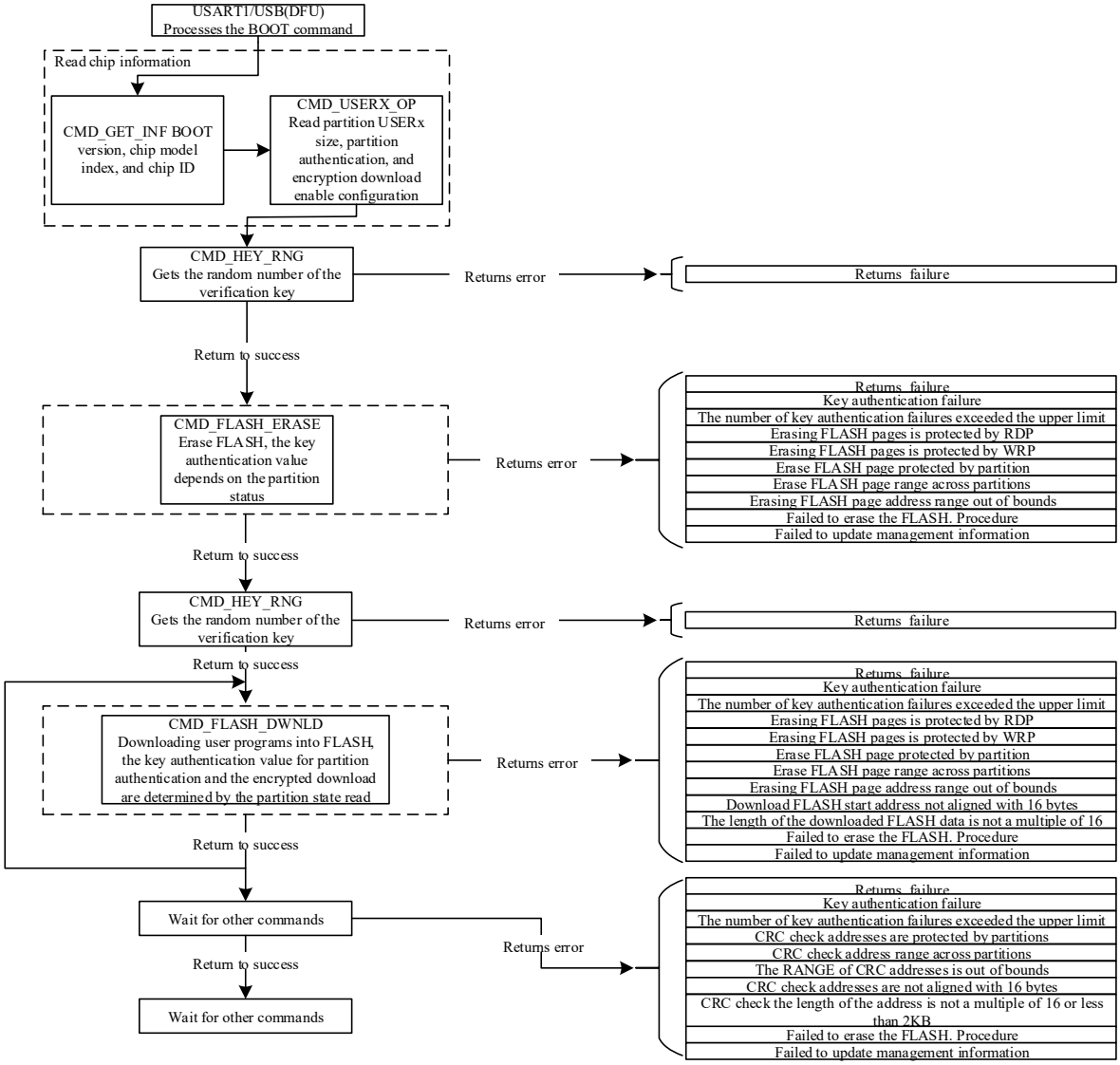


3.1.2 Download Command Control Flowchart

Upper computer obtains a random number before downloading partition authentication encryption, and the host computer uses this random number to generate the key authentication value of 16-byte USER1/2/3 partition authentication.In the case of continuous download, the random number used in the subsequent download command is generated by the random number deriving algorithm of the first time instead of obtaining a new random number.

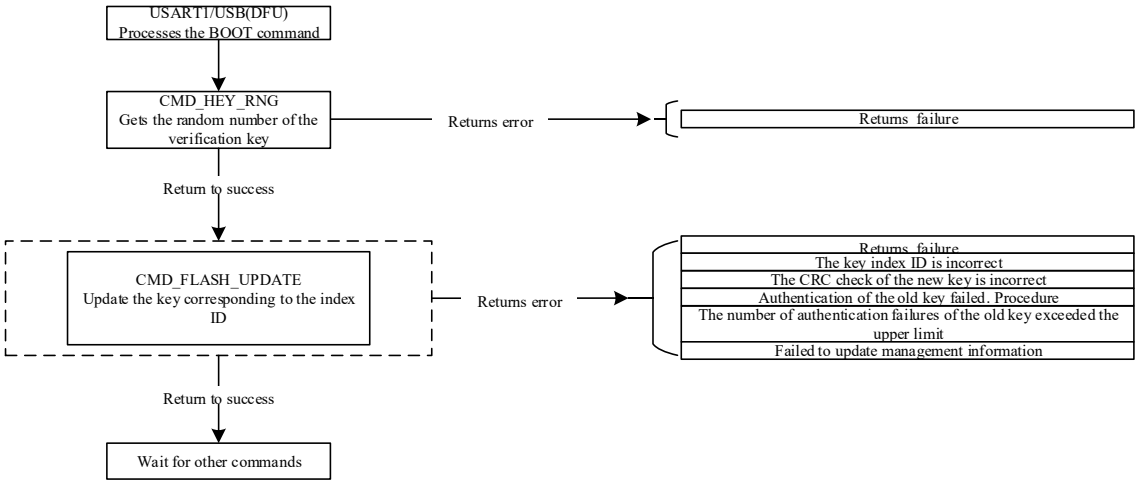
Figure 3-2 Flowchart for Downloading Command Control

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg



3.1.3 Update Key Command Control Flowchart

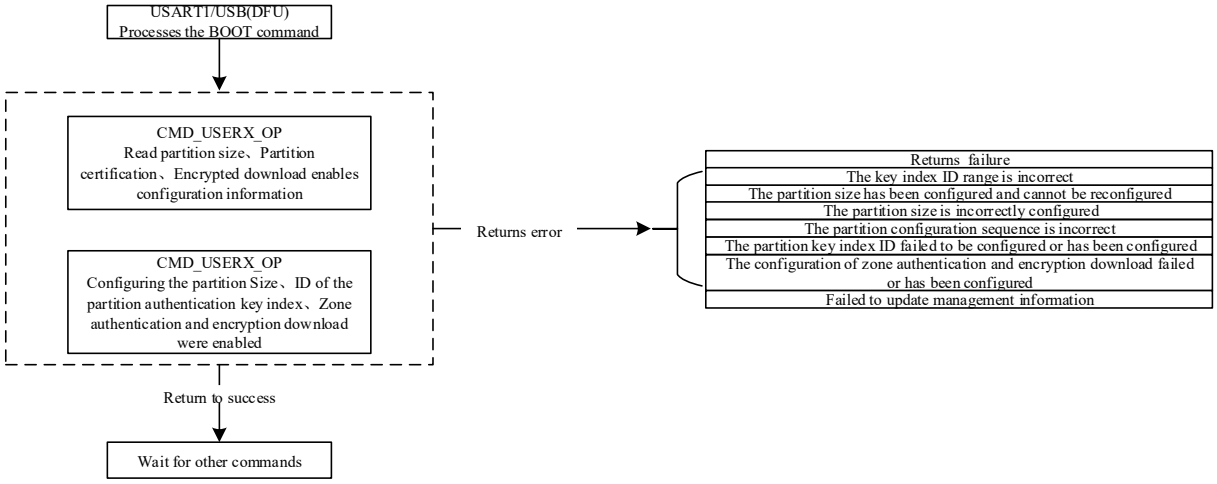
Figure 3-3 Command Control Flowchart for Updating a Key



NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road, Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

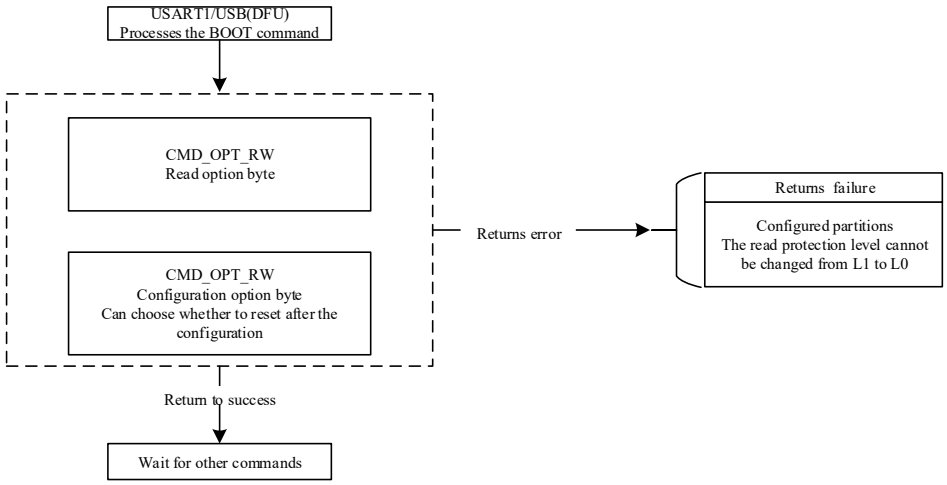
3.1.4 Partition Operation Command Flowchart

Figure 3-4 Flow Chart of Commands for Partition Operations



3.1.5 Option Byte Read/Write Command Control Flowchart

Figure 3-5 Flowchart of Option Byte Read/Write Command Control



NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

4 BOOT Version Description

Version	Changes
V2.1	1. Initial version (Automatic Baud rate detection)
V2.2	1. To optimize the download speed when using UART, automatic baud rate detection is changed to Baud rate negotiation to support higher communication rates. When the clock source is HSI, the maximum baud rate can support 1Mbps, and when the clock source is HSE, the maximum baud rate can support 2.25Mbps. 2. The UART-RX pin is configured by Floating as internal pull-up to optimize the connection stability.
V2.3	1. Add N32WB452CEQ6 UART download function, UART download interface PB6(TX), PB7(RX) 2. When the clock source is HSE, the maximum baud rate can be 4.5Mbps when the crystal frequency is 16MHz and 32MHz.
V2.4	1. Fix the abnormal MCU startup problem when BOOT is started and VBAT is powered on, VDD is powered off and then powered on;

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

5 Version History

Version	Date	Changes
V0.95	2020.09.12	Initial version
V1.0	2020.12.23	1. Update 1.BOOT brief, interface support; 2. Update 2.2.1.CMD_SET_BR, update UART baud rate support list; 3. Update 2.2.4.cmd_key_update; 4. Update 2.2.5.CMD_FLASH_ERASE; 5. Update 2.2.6.CMD_FLASH_DWNLD; 6. Update 2.2.7.CMD_DATA_CRC_CHECK; 7. Updated 2.3.3. Return other status words;
V1.1	2021.09.18	1. Added the BOOT version description section; 2. Added descriptions about BOOT V2.4.

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg

6 Disclaimer

This document is the exclusive property of NSING TECHNOLOGIES PTE. LTD.(Hereinafter referred to as NSING). This document, and the product of NSING described herein (Hereinafter referred to as the Product) are owned by NSING under the laws and treaties of Republic of Singapore and other applicable jurisdictions worldwide. The intellectual properties of the product belong to Nations Technologies Inc. and Nations Technologies Inc. does not grant any third party any license under its patents, copyrights, trademarks, or other intellectual property rights. Names and brands of third party may be mentioned or referred thereto (if any) for identification purposes only. NSING reserves the right to make changes, corrections. enhancements, modifications, and improvements to this document at any time without notice. Please contact NSING and obtain the latest version of this document before placing orders. Although NATIONS has attempted to provide accurate and reliable information, NATIONS assumes no responsibility for the accuracy and reliability of this document. It is the responsibility of the user of this document to properly design, program, and test the functionality and safety of any application made of this information and any resulting product. In no event shall NATIONS be liable for any direct, indirect, incidental, special, exemplary, or consequential damages arising in any way out of the use of this document or the Product.

NATIONS Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, Insecure Usage'. Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, all types of safety devices, and other applications intended to supporter sustain life. All Insecure Usage shall be made at user's risk. User shall indemnify NATIONS and hold NATIONS harmless from and against all claims, costs, damages, and other liabilities, arising from or related to any customer's Insecure Usage Any express or implied warranty with regard to this document or the Product, including, but not limited to. The warranties of merchantability, fitness for a particular purpose and non-infringement are disclaimed to the fullest extent permitted by law. Unless otherwise explicitly permitted by NATIONS, anyone may not use, duplicate, modify, transcribe or otherwise distribute this document for any purposes, in whole or in part.

NSING Technologies Pte. Ltd.
Add: NSING, Teletech Park #02-28, 20 Science Park Road,
Singapore 117674
Tel: +65 69268090
Email: sales@nsing.com.sg