Dragonchip

Secure Read/Write EEPROM/Data Flash

AppNote071

Document Revision 1.2

January, 2018

Table of Content

1 Introduction

The objective of this document is to highlight the critical steps on how to securely write default settings to EEPROM / Data Flash memory.

For the purpose of enhancing data integrity, Dragonchip recommends users to do following procedures,

- Download the initialized data flash hex file in programming
- Implement secure Read/Write in software

Details of the above procedures are described in this document.

Any product with configurable flash memory includes:

1. DC6688FLT
2. DC6388FD
3. DC6688FLE

Any product with non-configurable flash memory includes:

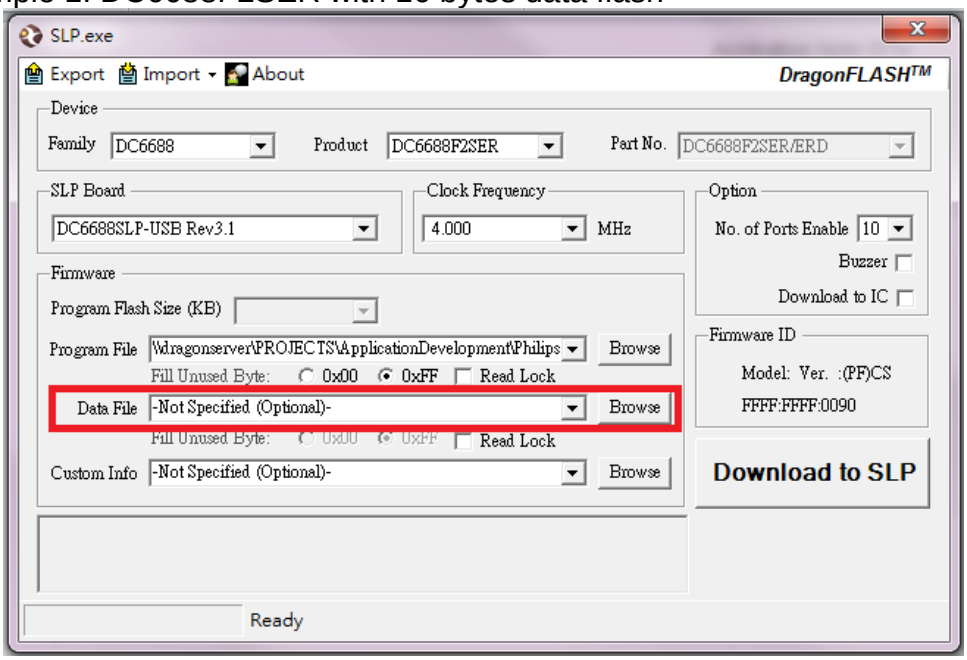
1. DC6688FST
2. DC6688FSE
3. DC6688F2R
4. DC6688F2T

2 Data flash download in programming

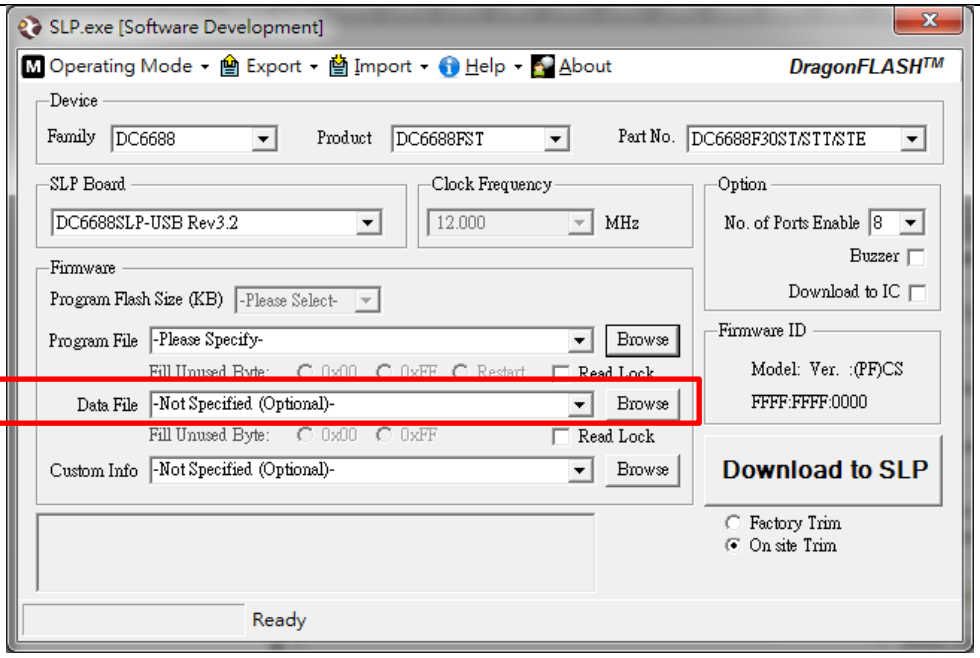
Users are recommended to initialize the data flash by downloading the data file hex code separately in programming. This procedure avoids the data flash from being initialized in power up process, as unstable power in power up process is possible to corrupt the data flash.

The figure below shows the location to download the data flash. While users use the software SLP in programming, data file can also be selected in the user interface, as indicated by the red box.

Example 1: DC6688F2SER with 16 bytes data flash



Example 2: DC6688F30STT

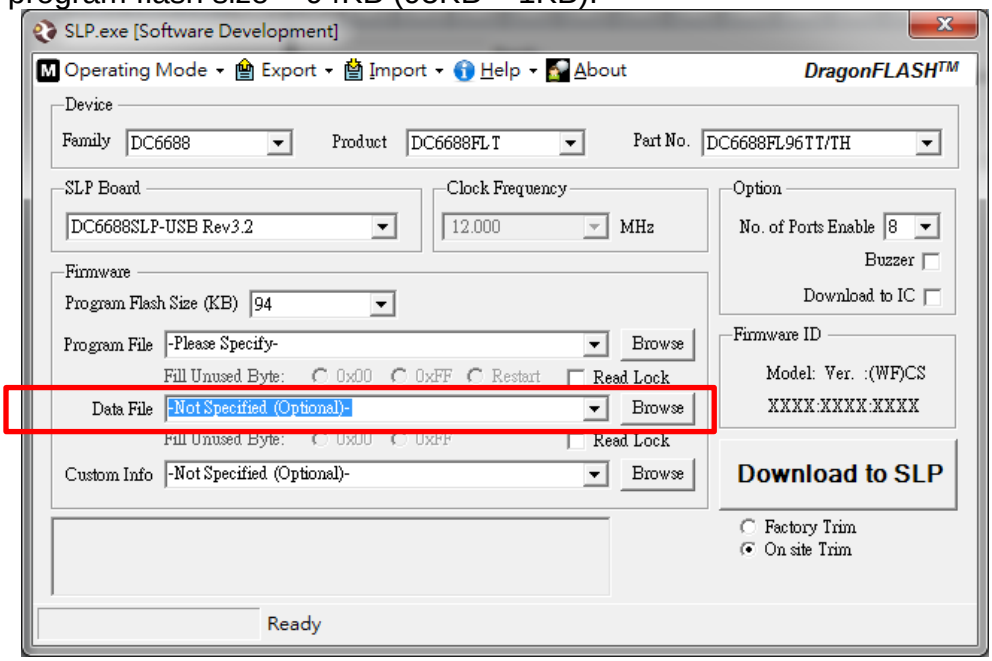


Example 3: DC6688FL96TT

For any product with configurable flash memory, there are two options:

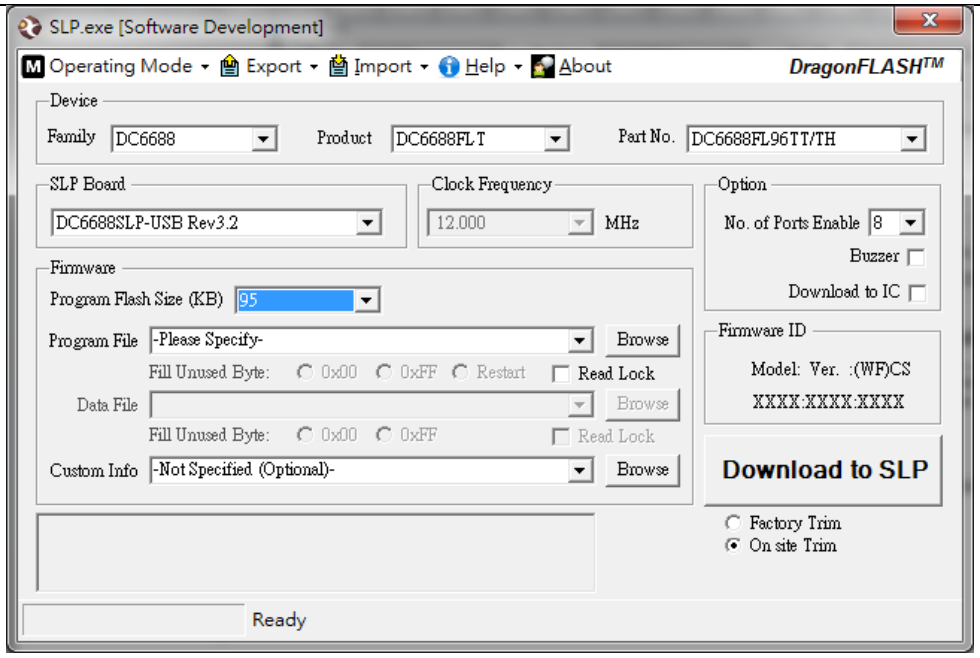
1) Option A

   Use data file. For example, the application needs 1KB data flash. Thus, program flash size = 94KB (95KB – 1KB).



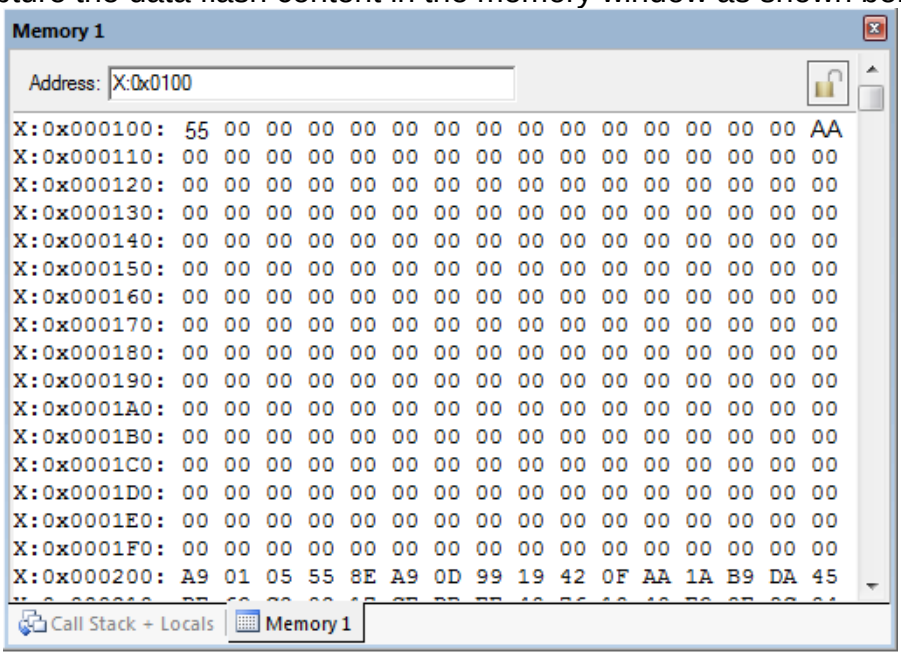
2) Option B

   Include in source code. Detail can refer AppNote008. The setting is shown below.

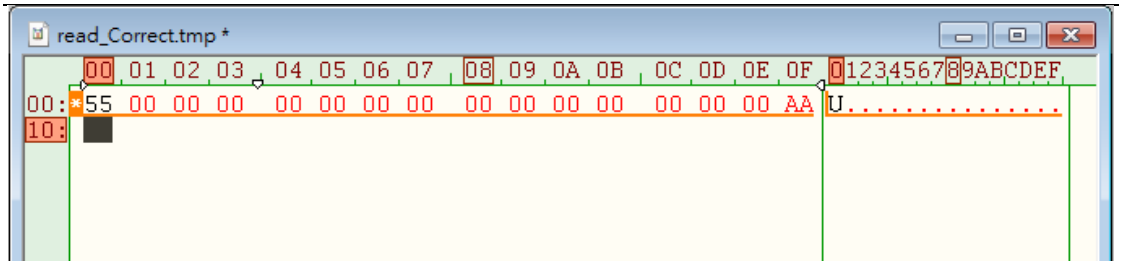


2.1 Create data flash file

To create a data flash file, users can capture the data flash content in emulator.
Users can compile the project source code and enter the emulator mode. A break point should be added right after the data flash is initialized. Then, users can capture the data flash content in the memory window as shown below.



Users can create a bin file in Hex editor according to the data captured.

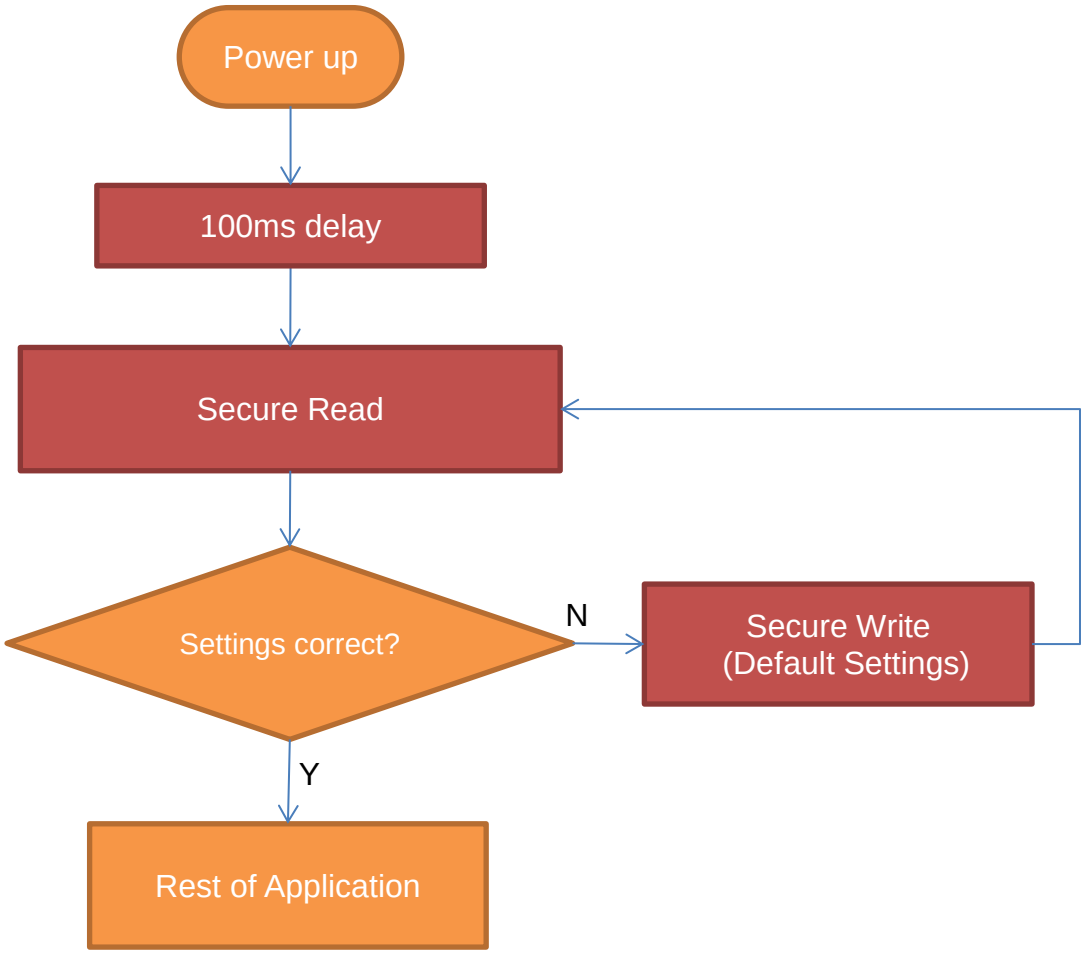


The file can then be loaded to the software SLP for programming.

3 Secure R/W on power up

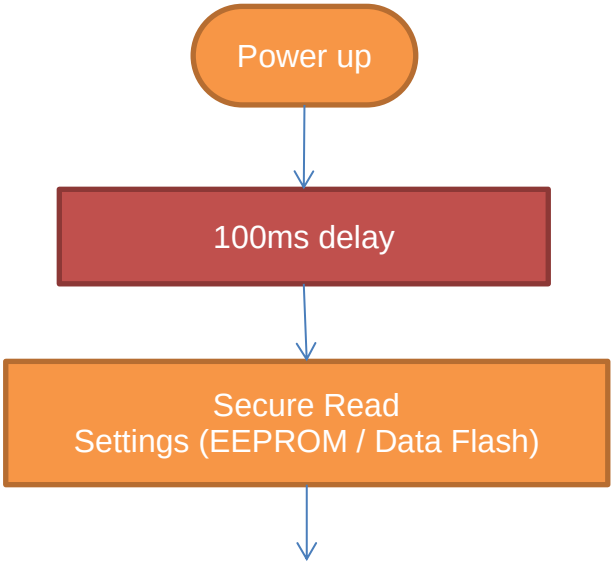
In universal remote control application, it is usually required to store user settings in EEPROM / Data Flash memory.

Below shows a typical software flow chart on power up to check the validation of EEPROM / Data Flash memory content.



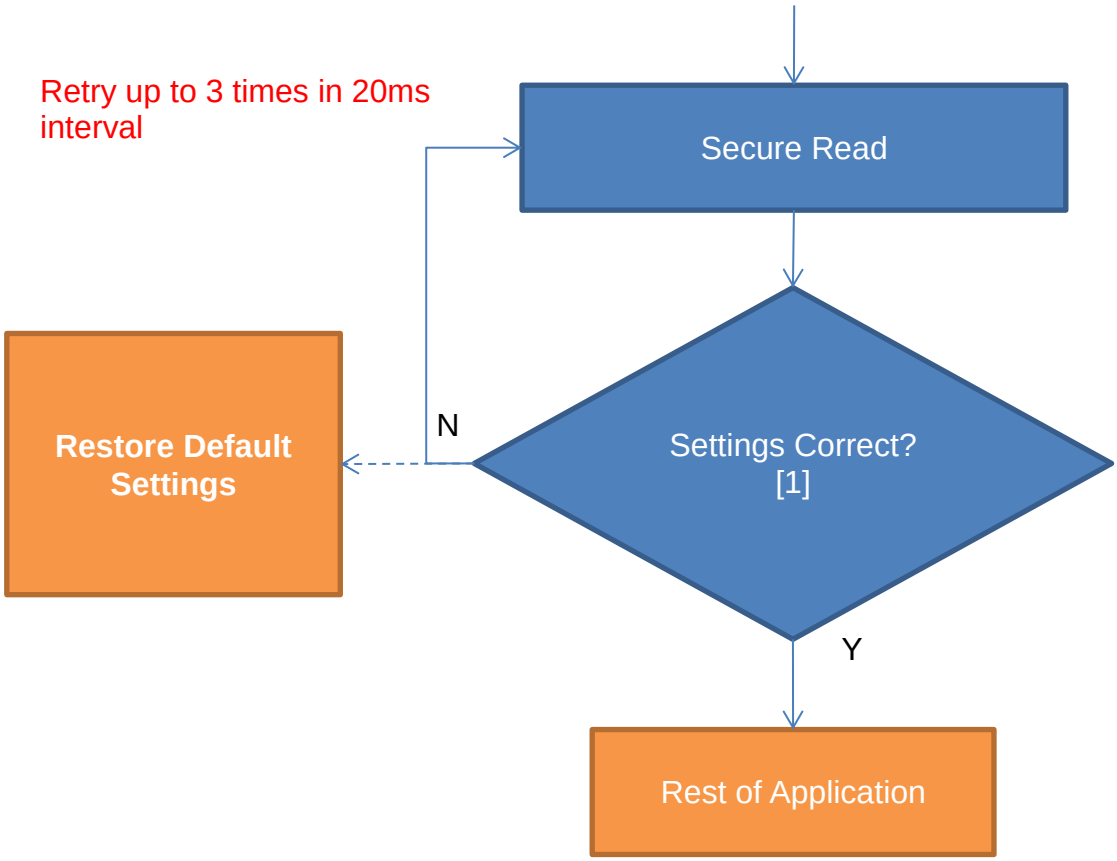
3.1 Add 100ms delay

Add 100ms delay to let power stable before CPU starting any operation. The flow chart is shown below.



3.2 Secure Read

The secure read is illustrated below the chart in blue.



Remarks:
[1] Check Setting
To verify the read back from EEPROM / Data Flash memory, one can check the followings:
1) Verify the checksum
2) Compare the signature

For any product with configurable Flash memory, the expected checksum and signature must be stored together with the settings within the same page (512-byte size) of data flash memory.

For any product with non-configurable Flash memory, the expected checksum and signature must be stored together with the settings in data flash memory.

Suggested checksum formula = + every location's content + constant

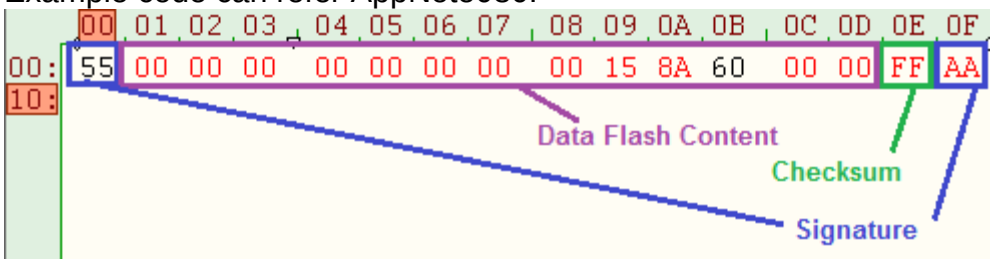
Constant should neither be zero or 0xFF value.

The signature is a pattern. It should avoid using 0xFF.

An example is shown below.

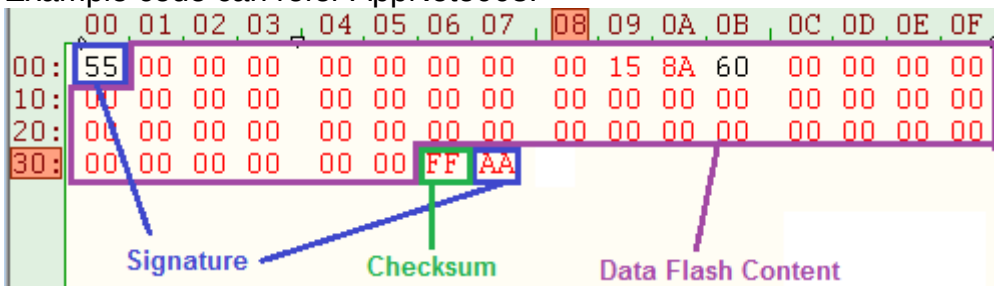
For 16-byte Data Flash

A single byte of beginning and ending signature is recommended to indicate the beginning and ending position of the data flash.
A single byte of checksum is also recommended for checking the content of data flash.
Example code can refer AppNote080.



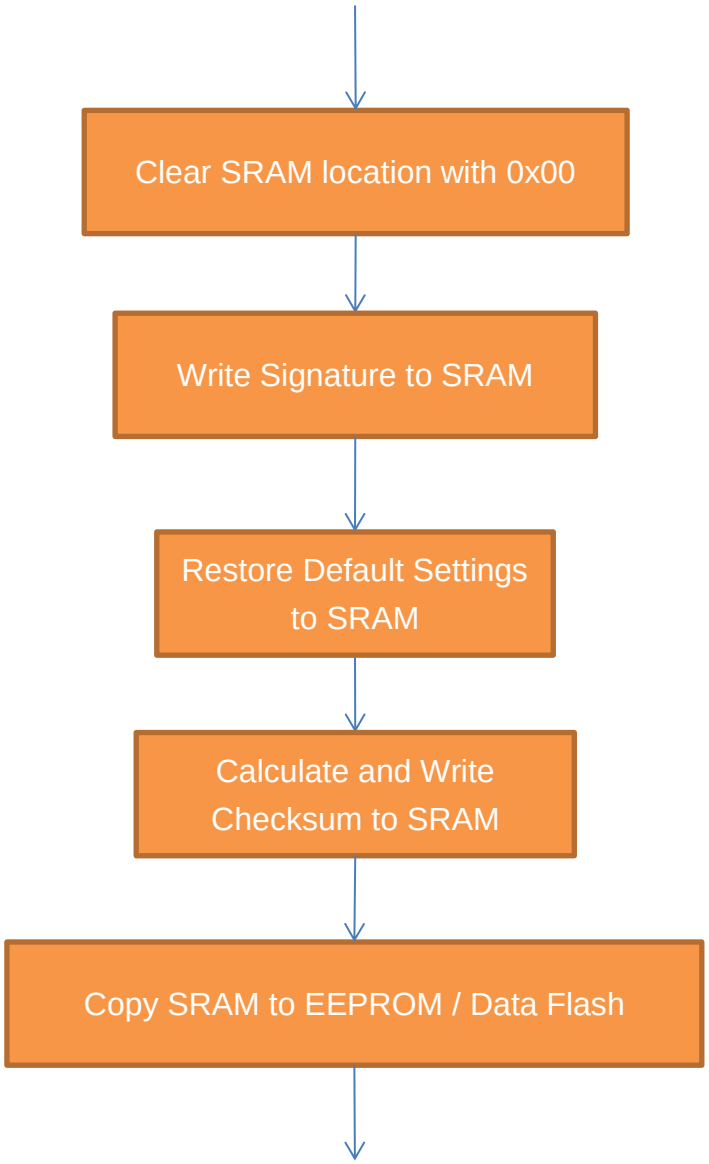
For 64-byte Data Flash

A single byte of beginning and ending signature is recommended to indicate the beginning and ending position of the data flash.
A single byte of checksum is also recommended for checking the content of data flash.
Example code can refer AppNote008.



3.3 Secure Write (Restore Default Settings)

Using the example in last section “secure read”, to prepare the data before writing default settings to Data Flash memory. Below is guideline on how to prepare it.



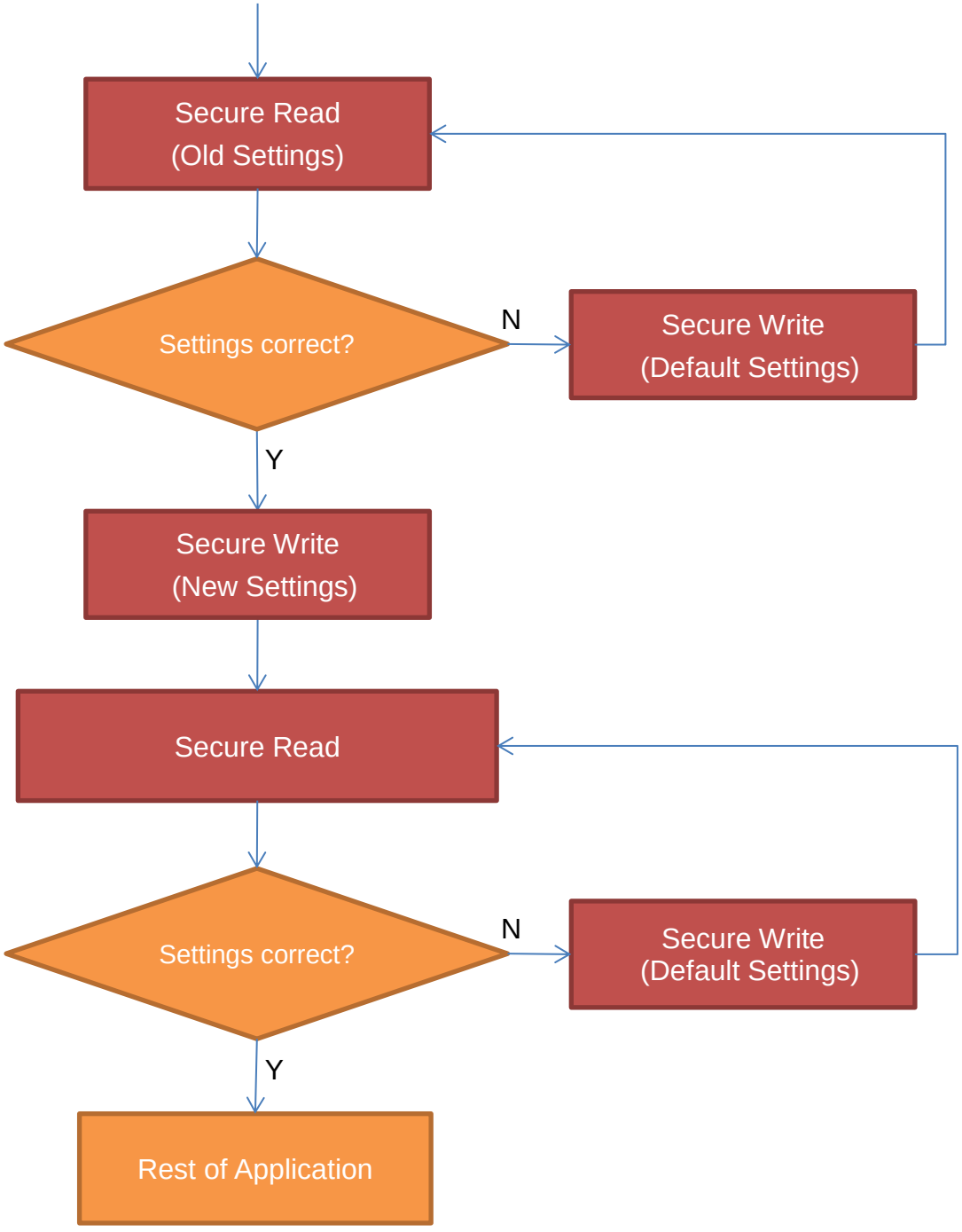
The sequence is important, and must be followed.
The signature must be done before any data preparation.

After prepared the Default settings and written to EEPROM / Data Flash memory, it must be verified.

An example of software implementation is shown in AppNote008 / Appnote080.

4 Secure R/W to update EEPROM / Data flash memory

Below shows a typical software flow chart to update EEPROM / Data Flash memory content.



Prior to writing new settings to EEPROM / Data Flash memory, read the old settings (we say an image) to SRAM. For any product with configurable flash

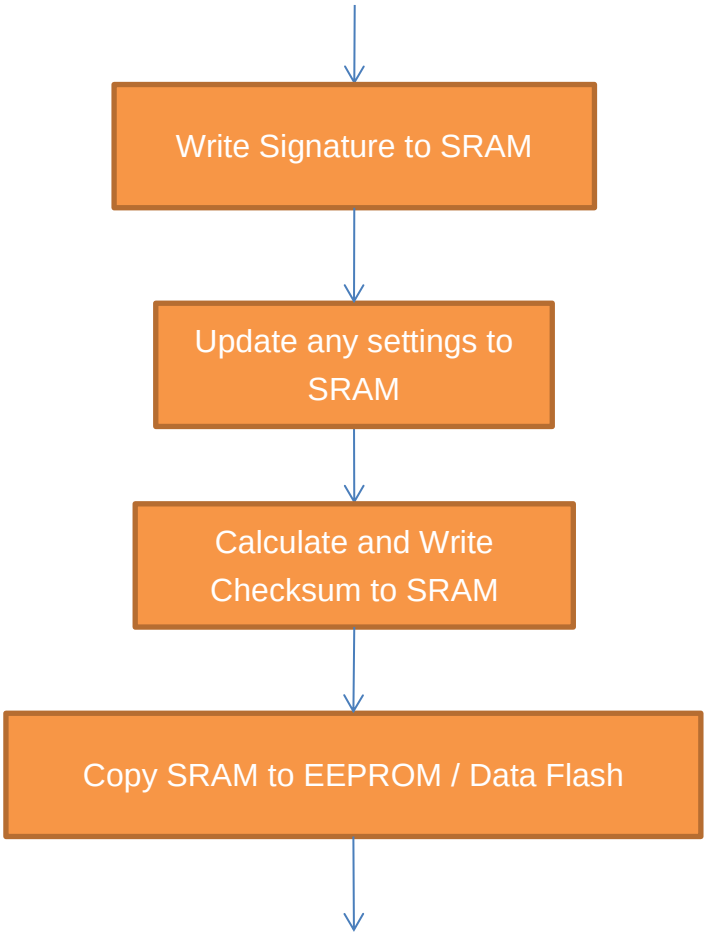
memory, the target SRAM is expanded SRAM. For any product with non-configurable flash memory, the target is 256B SRAM.
Then, modify the image in SRAM. Once finished, the new image is copy to EEPROM / Data Flash memory. At this moment, validation is checked by reading back the image.

4.1 Secure Read

Detail refers section 3.2.

4.2 Secure Write (New Settings)

Below is guideline on how to prepare new settings and write to EEPROM / Data Flash memory



For any product with configurable flash memory, the target SRAM is expanded SRAM. For any product with non-configurable flash memory, the target is 256B SRAM.

4.3 Secure Write (Restore Default Settings)

Detail refers section 3.3.

Revision History

Document Rev. No.	Issued Date	Section	Page	Description	Edited By	Reviewed By
1.0	July, 2012			Preliminary	Danny Ho	Celia Ki
1.1	Sept, 2014	2	4	Added section 2 “Data flash download in programming”	Philip Hung	Danny Ho
		3.2	9, 10	Added guidance in Secure R/W for 16-byte and 64-byte data flash		
1.2	Jan, 2018	2		Added examples for different products	Danny Ho	Patrick Li
		4		Added update in data flash memory		

Copyright Notice

Disclaimer

Dragonchip Ltd. assumes no responsibility for any errors contained herein.

Dragonchip Ltd.
TEL: (852) 2776-0111
FAX: (852) 2776-0996
http://www.dragonchip.com