AN1164
APPLICATION NOTE

Using the Security Block in M29 Series Flash Memories

Some STMicroelectronics Flash memories have an extra memory area set aside for Security Data. The Security Memory Block is usually 256 bytes of Read-Only Memory that can be read from the Flash by issuing the Security Data command. The data in the Security Block can be used in a variety of different ways to protect or encrypt data or as a method of identifying products and authenticating them. Parts that currently include a Security Memory Block include the M29W800A, M29W008A, M29W116B and M29W160B. Future Flash memories are expected to include Security Memory Blocks.

The Security Memory Block is programmed with a unique code by STMicroelectronics during the test phase of the Flash memory. Each part can contain a serial number that is unique to that part. In addition to the serial number, volume customers are able to request that specific data is programmed into each part. Because the Security Memory Block is large (256 bytes, compared to 128-bit security codes often offered), complex encryption keys can be specified. Note that normal parts will have undefined data in the Security Block; it is necessary to ask for a serial number or a unique code.

Applications can use the Security Memory Block in a variety of different ways. Products that communicate over a network (network cards, mobile phones, etc.) can use the data in the Security Memory Block to check authentication codes against entries in a database and set access and privilege levels. Furthermore, because the Security Memory Block cannot be modified, network identifiers cannot be changed and the chances of fraud are significantly reduced. It will not be possible to clone a product because, even though the Flash memory can be copied, it will not be possible to copy the Security Memory Block.

The 8M parts and the 16M parts are slightly different. The design of the 16M memory devices allows the Security Area to be used for the CFI (Common Flash Interface) instead of the Security Data. Volume customers can request that the CFI Data Structure is programmed into the Read-Only Memory and the Security Data Command changed to the CFI Query Command.

Because of the way the CFI works there are some restrictions on the way the Security Block works in the x8/x16 parts that support a Security Memory Block or the CFI (currently this only applies to the M29W160B, the M29W800A cannot support CFI). In the x8/x16 parts the Security code should only be considered to be 8-bits wide. Even when accessing the part in x16 mode, only the lower 8-bits will contain valid data. When specifying the data to be programmed into these parts ensure that only 256 *bytes* of data are specified. The 256 bytes will be read in the lower 8-bits of the word in x16 mode; in x8 mode the 256 bytes will be spread across 512 bytes of memory space, DQ15A–1 = 0 or DQ15A–1 = 1 will read the same value. Table 1 shows an example of how the data specified will be read.

Table 1. Example of Data Read from Security Memory Block in M29W160B and other CFI compatible memories

Data Specified		Read in x8 mode		Read in x16 mode	
Offset	Value	Address (A6-DQ15A–1)	Data	Address (A7-A0)	Data
00h	AAh	00h	AAh	00h	00AAh
01h	BBh	01h	AAh	01h	00BBh
02h	CCh	02h	BBh	02h	00CCh
03h	DDh	03h	BBh	03h	00DDh
04h	EEh	04h	CCh	04h	00EEh
05h	FFh	05h	CCh	05h	00FFh

In conclusion the Security Memory Block in Flash memories from STMicroelectronics provides customers with a greater opportunity to protect their products from fraud. The large memory space provided for security allows long authentication codes to be stored. CFI compatible devices store and access the Security Memory area using a technique that is compatible with the CFI.

If security is a concern to you, make sure you choose an STMicroelectronics Flash memory with a Security Memory Block in your next design.

If you have any questions or suggestion concerning the matters raised in this document please send them to the following electronic mail address:

ask.memory@st.com (for general enquiries)

Please remember to include your name, company, location, telephone number and fax number.