



Power Quotient International Co., Ltd.

IC STORAGE SPECIALIST

Secured DiskOnModule™ Series

Installation Manual

Ver. 1.0

-Index-

1.) Description.....	2
1.1) Features.....	2
1.2) Specifications.....	3
1.3) Block Diagram.....	3
2.) Installation.....	4
2.1) Normal Mode Setup-No Secured Function Installation.....	5
2.2) Secured Mode Setup-Secured Function Installation.....	7
2.2.1) Basic Concept.....	7
2.2.2) Basic Zone Application.....	7
2.2.3) Password.....	9
3.) Design Kit.....	10
3.1) Simply Design.....	10
3.2) Enable Secured Function Step Processes.....	11
3.3) The Secured DiskOnModule Utility.....	11
3.3.1) Support OS with Utility.....	11
3.3.2) Setup Vendor Key – SDOM_VKY.EXE.....	11
3.3.3) Create Partition – SDOM_PWD.EXE	12
3.3.4) Setup Password and Password Key – SDOM_PWD.EXE.....	12
3.3.5) Open/Close ROM Zone, Open/Close Protect Zone	13
3.4) The Secured DiskOnModule Driver.....	13
3.4.1) Function of Driver.....	13
3.4.2) Support OS with Driver.....	14
3.4.3) Built Driver Into the Program	14
3.5) Example to Call Secured DiskOnModule Driver.....	14
3.5.1) Call ROM Zone Function.....	14
3.5.2) Call Protect Zone Function.....	16
4.) The Secured DiskOnModule Mass Production.....	17



Power Quotient International Co., Ltd.

IC STORAGE SPECIALIST

Secured DiskOnModule™ Series

User's Manual

FDxxx-xxxPS.xQx

4MB/8MB/16MB/32MB/64MB/128MB/256MB/384MB

1. Description

PQI **Secured DiskOnModule** is the advanced storage device with unique security algorithm. Our **Secured DiskOnModule** can be worked in most computer operation systems such as Windows, DOS, Linux.etc., and we have developed the multi-layers password system to prohibit any illegal access for your treasured data. You can easily define and partition your **Secured DiskOnModule** to User Zone, Read-Only Zone, and Protected Zone. We will also offers you our library to setup the unique password system, even PQI cannot know the password of the **Secured DiskOnModule**. You will be the only one who can hold all password of the **Secured DiskOnModule**. For your special design, we will provide the whole design kits to help the customer to input the data into the **Secured DiskOnModule**, and they can control the whole production process to prevent the data leak.

FDxxx-xxxPS.xQx series is our **Secured DiskOnModule** based on Hyperstone NAND Type flash memory controller technology. This product complies with 40/44 PIN IDE (ATA) standard interface and is suitable for data storage memory medium for portable system. By using **Secured DiskOnModule**, you can protect your valuable data or program by yourself.

1.1 Features

- Best Secure Function
- High Performance
- Non-volatile Flash Memory (NAND type)
Retention of stored data is guaranteed for at least 10 years, with no battery or other power source required.
- 100% True Mode IDE HDD Compatible
- Broad Operating System and Processors Supports
- Capacities 4~384Mbytes
- Low Power Consumption
- Robust Error Correction
- High Reliability

*Design with Hyperstone series product to access NAND type flash memory.

1.2 Specifications

Environment Specifications

Temperature	Operating	0 to +70
	Non-Operating	-20 to +85
Relative Humidity		8% to 95% (with no condensation)
Vibration	Operating	15G
	Non-operating	15G
Shock	Operating	1000G
	Non-operating	1000G

Configuration

Capacity	4Mbytes to 384Mbytes
Sector size	512Bytes

System Performance

Media transfer rate	write	1. 2MB/sec (typ.)
	read	2. 5MB/sec (typ.)
Interface burst transfer rate		
PIO mode 2		8.3 MB/sec (max)

Reliability

MTBF(@25)	300,000 hours
ECC	22bit per 256bytes

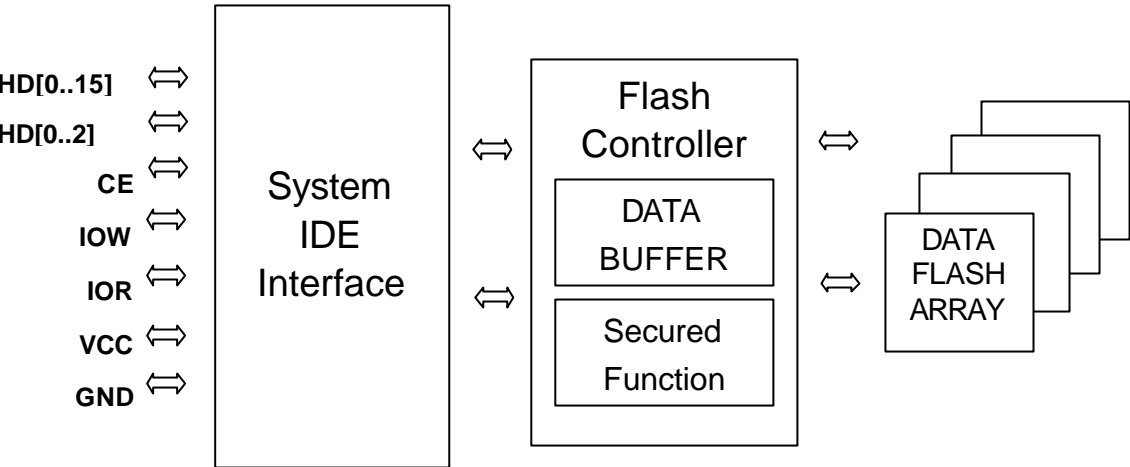
Power Requirement

Voltage	DC+3.3V±5%(Optional)
	DC +5.0V±10%

Power Consumption

Read	21mA (typ.)
Write	28mA (typ.)
Sleep	0.3mA (typ.)

1.3 Block Diagram



2. INSTALLATION GUIDE

BEFORE YOU BEGIN

To protect your DOM from static discharge by making sure you are well grounded before touching the DOM. We recommend wearing a grounded wrist strap throughout the installation process.

There are two kind of mode to setup Secured *DiskOnModule*, please read carefully and follow the steps.

2.1) Normal Mode Setup---- No Secured Function Installation

STEP 1

1. Make sure your computer is turned off before you open the case.
2. Plug the DOM carefully into the IDE slot on your computer or host adapter.
Caution: Make sure to align pin 1 on the computer or host adapter interface connector with pin 1 on your DOM. Pin 1 is indicated by a triangle on the DOM connector.
3. Connect the power cable of the DOM to an unused power connector of the computer.
Caution: If you need to remove your DOM, use BOTH HANDS to carefully pull out it.
4. Check all cable connectors are connected correctly and then replace your computer cover.

STEP 2

Before you format or partition your new drive, you must configure your computer's BIOS so that the computer can recognize your new drive.

1. Turn your computer on. As your computer starts up, watch the screen for a message describing how to run the system setup program (sometimes called BIOS or CMOS setup). This is usually done by pressing a special key, such as DELETE,ESC, or F1, during startup. See your computer manual for more details. Press the appropriate key to access the system setup program.
2. Find the option of Hard Disk setting, which is usually named "Standard BIOS setup or Standard CMOS Setup". If your BIOS provide automatic drive detection (an "AUTO" drive type), select it. This allows your computer to configure itself automatically for your new drive. (Besides, we recommend you to use Normal/CHS mode to partition your DOM to get the maximum formatted capacity.)

Caution!!

If your BIOS does not provide automatic drive detection, select "User-defined" drive setting, enter the CHS values, and please refer to the following table to find your module. Please kindly find the exact one or your Secured *DiskOnModule* may not work correctly.

CHS Table

Capacity	No. of Cylinders	No. of Sectors/Track	No. of Heads	Unformatted Capacity (Bytes)
FD008-xxxxx.xQx (8MB)	495	16	2	8110080
FD016-xxxxx.xQx (16MB)	995	16	2	16384000
FD032-xxxxx.xQx (32MB)	500	16	8	32768000
FD064-xxxxx.xQx (64MB)	500	32	8	65536000
FD128-xxxxx.xQx (128MB)	500	32	16	131072000
FD256-xxxxx.xQx (256MB)	507	63	16	261660672

3. Save the settings and exit the System Setup program.
(Your computer will automatically reboot)
After you configure your computer, you can use the standard DOS commands to partition and format your DOM, as described below.

STEP 3

To partition your new DOM with Microsoft® DOS program:

1. Insert a bootable DOS diskette into your diskette drive and restart your computer.
2. Insert a DOS program diskette that contains the FDISK.EXE and FORMAT.COM programs into your diskette drive. Use the same DOS version that is on your bootable diskette. At the A: prompt, type FDISK and press ENTER.
3. If you have two IDE devices installed, the FDISK menu displays five options. Option five allows you to select the drive you want to partition. Make sure that your new drive is selected.
4. Select "Create DOS partition or logical DOS drive" by pressing 1. Then press ENTER.
5. Select "Create primary DOS partition" by pressing 1 again. Then press ENTER. Create your first drive partition. If you are creating a partition that will be used to boot your computer (drive C), make sure that the partition is marked active.
6. Create an extended partition and additional logical drives as necessary, until all the space on your new hard drive has been partitioned.
7. When the partitioning is complete, FDISK will reboot your computer.

Caution!!

Make sure you use the correct drive letters so that you do not format a drive that already contains data.

8. At the A: prompt, type “format c:/s”, (Suppose c: is the letter of your first new partition your). Repeat the format process for all the new partitions (such as D:, E:, F:,.etc.) you have created.
9. After you format your drive, it is ready to use.

2.2) Secure Mode Setup-----Secured Function Installation

Secured DiskOnModule Structure

Chapter 2.2.1--Description of Secured DiskOnModule Basic Concept

Chapter 2.2.2--Description of Secured DiskOnModule Basic Zone Application

Chapter 2.2.3--Description of Secured DiskOnModule Password

2.2.1) Basic Concept

Secured DiskOnModule could have variously types of utilizing combination through three different zones. (Refer to Figure 1)

)User Zone

The most command area, able to both read and write, and without any password protection.

)ROM Zone

This area is for read only, write function is only able to utilize when “ROM Zone Password” has been entered by user.

)Protect Zone

The most characteristically area which is being protected by the “Protect Zone Password”, is an area that not able to write or read if the user d provide the proper passwords.

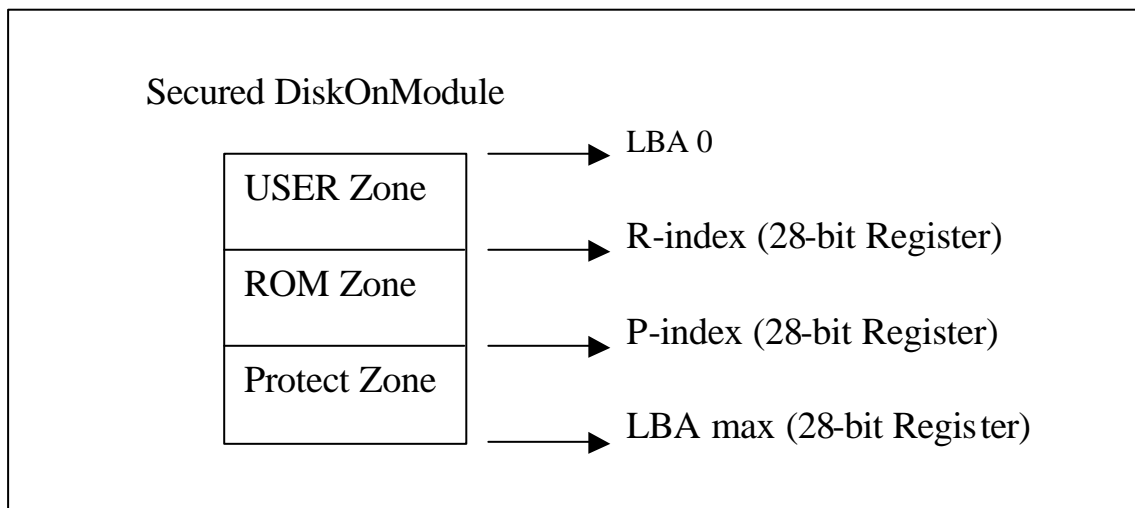


Figure 1 – Secured DiskOnModule Block

2.2.2) Basic Zone Application

The customs could extend the operation functions through three different partition combinations, and that will help us to meet the needs from all types of buyer’s requirements.

Following description is to present you the further description of the operation concept.

Only User Zone

Secured DOM does not need any password if there is only one partition need to be create, the way of operation just same as we operate it on the Hard Disk, just like the Normal Use Setup on p4.

User Zone and ROM Zone

When second partition need to be create in the Secured DOM:
The first Partition will be User Zone (LBA 0 → R-index)
And the second Partition should use Utility “SDOM_PWD.EXE” to set as ROM Zone (R-index → LBA max) (Refer to 3.3.3)

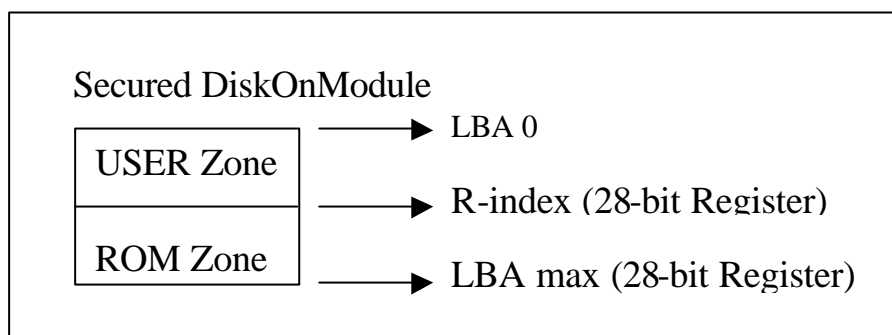


Figure 2 – User Zone and ROM Zone Block

User Zone and Protect Zone

When second partition need to be create in the Secured DOM:
The first Partition will be User Zone (LBA 0 → P-index)
And the second Partition should use Utility “SDOM_PWD.EXE” to set as Protect Zone (P-index → LBA max) (Refer to 3.3.3)

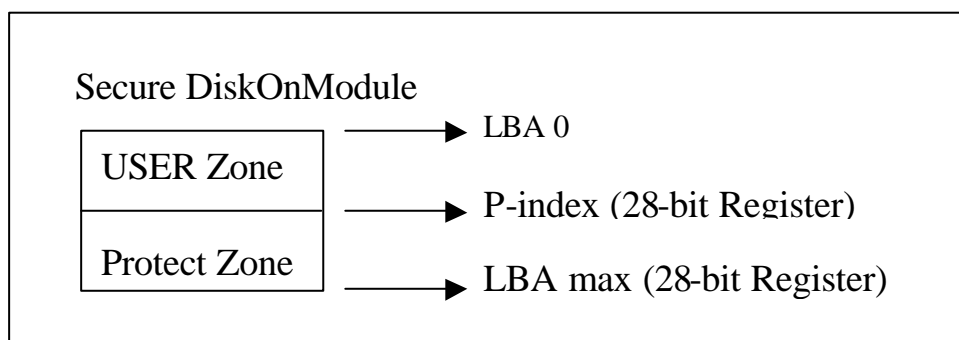


Figure 3 – User Zone and Protect Zone Block

User Zone and ROM Zone and Protect Zone

When Secured DOM need to create three partitions:
The first Partition will be User Zone (LBA 0 → R-index)
Tthe second Partition should use Utility “SDOM_PWD.EXE” to set as ROM Zone (R-index → P-index)
For third partition should also use Utility “SDOM_PWD.EXE” to set as Protect Zone (P-index → LBA max) (Refer to 3.3.3)

2.2.3) Password

Two sets of Secured DOM Password are able to set up through user' s own option.

)ROM Zone Password

ROM Zone Password is assembled by many different parameters, the main propose of this password is to control the access gate to ROM Zone. (Refer to 2.3.1)

)Protect Zone Password

Protect Zone Password is assembled by many different parameters, the main propose of this password is to control the access gate to Protect Zone. (Refer to 2.3.2)

ROM Zone Password

The are four major parameters of ROM Zone Password which as following:

)Vendor Key

Customer could set up this parameter by itself, The Range of Vendor Key is from 0 to 0xFFFF.

(Set Up Indication please refer to 3.3.2)

)ROM Password

Customer could set up this parameter by itself, The Range of ROM Password is from 0 to 0xFFFFFFFFE.

(0xFFFFFFFFF is Initial, Set Up Indication please refer to 3.3.4)

)ROM Password Key1

Customer could set up this parameter by itself, The Range of ROM Password Key 1 is from 0 to 255.

(Set Up Indication please refer to 3.3.4)

)ROM Password Key2

Customer could set up this parameter by itself, The Range of ROM Password Key 2 is from 0 to 255.

(Set Up Indication please refer to 3.3.4)

Protect Zone Password

There are four major parameters of ROM Zone Password which as following:

)Vendor Key

Customer could set up this parameter by itself, The Range of Vendor Key is from 0 to 0xFFFF.

(Set Up Indication please refer to 3.3.2)

)Protect Password

Customer could set up this parameter by itself, The Range of Protect Password is from 0 to 0xFFFFFFFFE.

(0xFFFFFFFFF is Initial, Set Up Indication please refer to 3.3.4)

)Protect Password Key1

Customer could set up this parameter by itself, The Range of Protect Password Key 1 is from 0 to 255.

(Set Up Indication please refer to 3.3.4)

) Protect Password Key2

Customer could set up this parameter by itself, The Range of Protect Password Key 2 is from 0 to 255.

(Set Up Indication please refer to 3.3.4)

3.) Design Kit with Secured DiskOnModule

Five Chapters are included in this section

Chapter	3.1	Description of Secured DOM Simply Design
Chapter	3.2	Description of Secured DOM Setup Processes
Chapter	3.3	Description of Secured DOM Utility
Chapter	3.4	Description of Secured DOM Driver
Chapter	3.5	An Operation Example – How to Call Secured DOM Driver?

3.1) Simply Design

PQI Secured DOM just like your Hard Disk, but with simply design and remarkable Secure Function, it provides your customer a complete Hard Ware Protection.

During the progress of program developing, we divide zones according to the what users need (using the same way that we divide Hard Disk), then place the program which is need to be protected into ROM Zone or Protect Zone, finally we enable the secure system when program development is completed.

Furthermore, PQI also provides DOM Utility which could makes you easily to Debug it and set up parameters, the transparently driver function is perfectly for join any remain drivers.

3.2) Enable Secure Function Setup Processes

There will be four steps of secure function Setup

Step 1: Setup Vendor Key (Refer to 3.3.2)

Step 2: Create Partition (Refer to 3.3.3)

Customer could have three options to completed this process

)Under DOS Environment

If your operation system is DOS or DOS Compatible, then you may use the Utility that provided by the PQI to create partition

) Non-DOS Environment

If your operation system is NON-DOS, you may use PQI s Utility to Create Partition, then use other tools to update the ID CODE of partition, such as DISKEDIT, PFDISK

)Create Partitions by your self

Depending on your own needs, Secured DOM s partition is able to create through properly arrangement -User/ROM/Protect Zone, User/ROM Zone, User/Protect Zone, User Zone Only. (Refer to Chapter 2 – Secured DiskOnModule Basic Concept)

Step 3: Setup ROM Zone Password and Protect Zone Password (Refer to 3.3.4)

ROM Zone Password: Set ROM Password, ROM Password Key1, and ROM Password Key2

Protect Zone Password: Set Protect Password, Protect Password Key1, and Protect Password Key2

ROM/Protect Password Key1 SHOULD ALWAYS BEING DIFFERENT THEN ROM/Protect Password Key2

Step 4: Enable Secure Function

When the system is being “REBOOT” or power shutdown, the secure function will be enable

Always provide ROM/Protect Zone password before you take format action to ROM/Protect Zone. (Refer to 3.3.5)

3.3) The Secured DiskOnModule Utility

PQI provides four utilities for Secured DOM' s operation

)SDOM_VKY.EXE: Set Vendor Key

)SDOM_PWD.EXE, Main functions are as following:

1. Create Partition for DOS
2. Set ROM Password, ROM Password Key1, ROM Password Key2
3. Set Protect Password, Protect Password Key1, Protect Password Key2

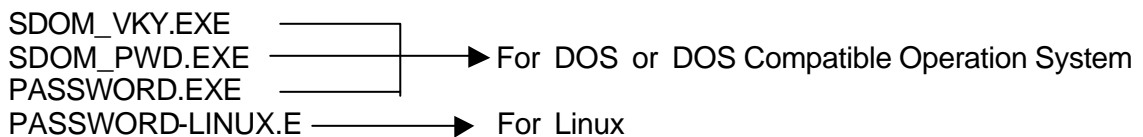
) PASSWORD.EXE:

Open/Close ROM Zone, Open/Close Protect Zone

) PASSWORD-LINUX.E:

Open/Close ROM Zone, Open/Close Protect Zone

3.3.1) Support OS with Utility



3.3.2) Setup Vendor Key – SDOM_VKY.EXE

)Set Vendor Key

Use Utility “SDOM_VKY.EXE” ,

Command: SDOM_VKY -P=0x1f0 (Primary Master)

SDOM_VKY -P=0x170 (Secondary Master)

User should always take this step as the first step when he running Secured DOM Setup process.

Once the user have been completed the set up of Vendor Key , ROM/Protect Zone Password, Password Key1 and Password Key2; should be remember at all time, to initialize the ROM/Protect Password when he would like to make any amendment on the previously setup.

II)Change Vendor Key

Step 1: Check the original ROM/Protect Zone Password,
Yes ---- Go to Step 2
No ----- G0 to Step 3

Step 2: Initial ROM/Protect Password
Use Utility “SDOM_PWD.EXE” Initial ROM Password and Protect Password
(Set Password to 0xFFFFFFFF,see 3.3.4)

Step 3: Set Vendor Key
If the user takes wrong steps to progress the change vendor key set up process, it may cause original ROM/Protect Zone Password being unable to use.

In case if above mentioned phenomenon occurred, user just need to use SDOM_VKY.EXE to make Vendor Key back to the original status, then re-progress it according to proper step.

3.3.3) Create Partition – SDOM_PWD.EXE

Command: SDOM_PWD –P=0x1f0 (IDE Primary Master)
SDOM_PWD –P=0x170 (IDE Secondary Master)

In SDOM_PWD.EXE program, contents the function of Partition Create (for DOS or DOS Compatible), ROM/Protect Zone Set Up and Password create for ROM/Protect Zone.

SDOM_PWD.EXE will support the user if they are intend to Set ROM/Protect Zone Password only.(with no partition)

If the user would like to Create Partitions by themselves, the number of partitions should not over three and also have to follow Secured DiskOnModule Basic Concept.

3.3.4) Setup Password & Password Key –SDOM_PWD.EXE

Command: SDOM_PWD –P=0x1f0 (IDE Primary Master)
SDOM_PWD –P=0x170 (IDE Secondary Master)

The main propose of this program is to set:

ROM Zone Password: Password, Password Key1, and Password Key2
Protect Zone Password: Password, Password Key1, and Password Key2

Remark: Number' s range of Password is from 0 to 0xFFFFFFFF (0xFFFFFFFF is

Initial)

Number' s range of Password Key1 and Password Key2 is from 0 to 255.

3.3.5) Open/Close ROM Zone, Open/Close Protect Zone

PQI provides two types of OS Utilities (DOS & Linux), these both could Open or Close ROM Zone / Protect Zone.

)PASSWORD.EXE (For DOS or DOS Compatible)

Command: PASSWORD 1F0M (IDE Primary Master)

PASSWORD 1F0S (IDE Primary Slave)

PASSWORD 170M (IDE Secondary Master)

PASSWORD 170S (IDE Secondary Slave)

)PASSWORD_LINUX.E (For Linux)

Command: PASSWORD_LINUX 1F0M (IDE Primary Master)

PASSWORD_LINUX 1F0S (IDE Primary Slave)

PASSWORD_LINUX 170M (IDE Secondary Master)

PASSWORD_LINUX 170S (IDE Secondary Slave)

3.4) The Secured DiskOnModule Driver

PQI provides:

A head file " PQI.H"

A DOS Driver "SDOM_LIB.LIB"

A Linux Driver "SDOM_LIB_LINUX.O"

3.4.1) Function of Driver

) SDOM_LIB.LIB : contents three Subroutine

SDOM_R_PASSWORD (ATA-PORT, Vendor Key, ROM Password, ROM Password Key1,

ROM Password Key2) {.....}

SDOM_P_PASSWORD (ATA-PORT, Vendor Key, Protect Password, Protect Password Key1,

Protect Password Key2) {.....}

Keyboard (KBstatus) {.....}

)SDOM_LIB.LINUX.O : It contents two Subroutine

SDOM_R_PASSWORD (ATA-PORT, Vendor Key, ROM Password, ROM Password Key1,

ROM Password Key2) {.....}

SDOM_P_PASSWORD (ATA-PORT, Vendor Key, Protect Password, Protect Password Key1,

Protect Password Key2) {.....}

Keyboard (KBstatus) {.....}

Note:.

When Function Keyboard's Parameter KBstatus shows "0", Keyboard

is "Disable"

When Function Keyboard's Parameter KBstatus shows "1", Keyboard is "Enable"

3.4.2) Support OS with Driver

)SDOM_LIB.LIB → DOS or DOS Compatible system

)SDOM_LIB_LINUX → Linux

3.4.3) Built Driver Into the Program

How user add Secured DOM's driver into the program?

And enable/disable ROM/PROTECT Zone Protect smoothly.

Take three steps as following:

Step1: add Head file "PQI.H" into main program.

Step2: Call out the function which refers to Chapter3.4.2 from main program.

How to Disable the protection of ROM/Protect Zone?:

Type-in the correctly information of ATA-PORT, PASSWORD, Vendor Key, PASSWORD KEY1, PASSWORD KEY2, then the area will be able to open.

How to Enable the protection of ROM/Protect Zone?:

Type-in any incorrectly information of PASSWORD, Vendor Key, PASSWORD KEY1, PASSWORD KEY2, then the area will closed automatically.

Remark: The ATA-PORT address has to be correct at all time.

Step3: Linking Main Program with Driver.

3.5) Example to Call Secured DiskOnModule Driver

3.5.1) and 3.5.2) shows user two operation example.

"Call ROM Zone Function" shows user how to execute read function in ROM Zone area under DOS operation system.

"Call Protect Zone Function" shows user how to execute read function in Protect Zone area under Linux operation system.

3.5.1) Call ROM Zone Function

Following Examples will present you the steps for several SDOM's call ROM Zone user operation

- 1.List ROM Zone files
- 2.Disable Keyboard

3. Disable ROM Zone protect
4. Copy files to ROM Zone
5. Enable ROM Zone protect
6. Enable Keyboard

Put Secured DiskOnModule into Secondary Master IDE socket
Copy Utility & Driver to floppy, then use floppy to boot computer

Step1: Use Utility SDOM_VKY.EXE to set up Vendor Key as 0xABCD

Step2: Use Utility SDOM_PWD.EXE to divide Partition into three parts, C:/ is User Zone, D:/ is ROM Zone, E:/ is Protect Zone,

Step3: Reboot Computer.

Step4: Use Utility SDOM_PWD.EXE to set ROM Password as 0x1234, ROM Password Key1 as 10 and ROM Password Key2 as 20.

Step5:

)Format C:/

)Use Utility PASSWORD.EXE to Open ROM Zone(D:/), then Format D:/, after that use Utility PASSWORD.EXE to disable ROM Zone protect

)Use Utility PASSWORD.EXE to Open Protect Zone(E:/), then Format E:/, after that use Utility PASSWORD.EXE to disable Protect Zone protect

Step6: Use Borland C or Turbo C to open a Project, then add it into main program "PQI.C" and PQI's Driver "SDOM_LIB.LIB"

Step7: Linking PQI.C and SDOM_LIB.LIB, then will be able to access ROM Zone

```

/*Program Name: PQI.C*/
#include<PQI.H>      // Attach this head file is essential
#include<stdlib.h>

Void main ( )
{
System ("DIR *.* D:");    //List ROM Zone files
Keyboard ( 0);          //Disable the Keyboard
SDOM_R_PASSWORD (0x170, 0xABCD, 0x1234, 10, 11);    //Disable ROM Zone
Protect
System ("COPY *.* D:");  //Copy files to ROM Zone
SDOM_R_PASSWORD (0x170, 0, 0, 0, 0);    //Enable ROM Zone Protect
Keyboard ( 1);          //Enable the Keyboard
}

```

3.5.2) Call Protect Zone Function

Following Examples will present you the steps for several SDOM' s call Protect Zone user operation

- 1.Disable Keyboard
- 2.Disable Protect Zone protect
- 3.Copy/List files to Protect Zone
- 4.Enable Protect Zone protect
- 5.Enable Keyboard

Put Secured DiskOnModule into Primary Master IDE socket

Under Linux operation system:

Step1: Divide Partitions into three parts, Hda1 is User Zone, Hda2 is ROM Zone, Hda3 is Protect Zone,

Step2: Reboot Computer

Under DOS operation system:

Step3: Use Utility SDOM_VKY.EXE to set Vendor Key as 0xCDEF

Step4: Use Utility SDOM_PWD.EXE to set Protect Password as 0x5678, Protcet Password Key1 as 100,
Protect Password Key2 as 200

Under Linux operation system:

Step5:

)Mke2fs /dev/hda1

)Use Utility PASSWORD_LINUX.EXE to Open ROM Zone(Hda2),
then Mke2fs /dev/hda2, after that use Utility PASSWORD.EXE to disable ROM Zone protect

)Use Utility PASSWORD.EXE to Open Protect Zone(Hda3),
then Mke2fs /dev/hda3, after that use Utility PASSWORD.EXE to disable Protect Zone protect

Step6:Linking main program (PQI.C) with Driver (SDOM_LIB_LINUX.O)

Use GCC(Or Other Complete Program) to link PQI.C and SDOM_LIB.LIB, then will be able to access Protect Zone.

GCC LINK Command: GCC -o ./PROJECT -g ./PQI.C ./SDOM_LIB_LINUX.O

/*Program Name: PQI.C*/

```

#include<PQI.H>      // Attach this head file is essential
#include<stdlib.h>
Void main ( )
{
Keyboard ( 0 );      //Disable the Keyboard
SDOM_P_PASSWORD (0x1F0, 0xCDEF, 0x5678, 100, 200); //Disable Protect
Zone protect
System ("mount /dev/hda3 /mnt/hda3"); //Mount Protect Zone to /mnt/hda3
System ("cp *.* /mnt/hda3"); //Copy files to Protect Zone
System ("ls /mnt/hda3"); //List Protect Zone files
SDOM_P_PASSWORD (0x1F0, 0, 0, 0, 0); //Enable Protect Zone protect
Keyboard ( 1 );      //Enable the Keyboard
}

```

4.) The Secured DiskOnModule Mass Production

PQI offers two mass production solutions for Secured DOM' s customers.

Solution 1: Use PQI Duplicator

Step 1:

PQI will follow the “Setup Secured DiskOnModule Step” to built customer’ s own system into the proper area of Secured DiskOnModule, makes it become one piece of “Source DOM”

Step 2:

Use PQI s duplicator to make 1 to 7 DOM copy process.

Step 3:

Use PC DOS system to set Vendor Key, ROM Zone Password, and Protect Zone Password

Solution 2: Use PC Platform

Step 1:

PQI will follow the “Setup Secured DiskOnModule Step” to built customer’ s own system into the proper area of Secured DiskOnModule, makes it become one piece of “Source DOM”

Step 2:

Use Image File catching tool to get Source Image

Step 3:

Use PC' s own system to make 1 to 1 DOM copy process.

Step 4:

Use PC DOS system to set Vendor Key, ROM Zone Password, and Protect Zone Password