

Memory Card Support For ASEDrive IIIe Smart Card Readers

Application Note
Version 1.02
Oct. 19, 2003

Copyright © 2002
Athena Smartcard Solutions, Inc.

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Athena Smartcard Solutions, Inc.

ASE is a registered trademark of Athena Smartcard Solutions, Inc.

Revisions

Rev Number	Date	Notes
1	25 Dec 2002	Initial Release Version 1.0
2	29 Dec. 2002	Updating of 2 and 3 bus section

CONTENTS

Introduction	1
Non-Protected Memory Cards	1
I ² C	1
Extended I2C Family	1
Protected Memory Cards	2
2-bus Family	2
3-bus Family	3
Protected Memory Cards Selection Considerations:	4
ATR Values of 2-bus and 3-bus Cards	5
2-bus and 3-bus Cards Protected Area Memory Map.....	5
Working with memory cards in ASEDrive IIIe	6
Supported Memory Cards	6
Protected Memory Card in ASEDrive IIIe	6
Free Memory Cards in ASEDrive IIIe.....	6
Card Command Samples	8
All Memory cards	8
Protected Memory Cards (2-bus, 3-bus).....	8

Introduction

Memory cards use a synchronous communication protocol. They have no processing or file management capabilities, just simple data storage. There are several memory card product families. Each family of memory cards uses its own proprietary protocol and offers different level of protection, features and memory size. ASE distinguishes between 2 main families of memory cards:

- **Non-Protected Memory Cards** - Cards which do not offer any level of protection. They allow reading and updating data on the card freely.
- **Protected Memory Cards** – Cards which employ a protection mechanism, such as enabling to alter memory only after a successful password verification process.

Each family of ASECard memory cards is further broken down into two sub-categories. **I2C** and **Extended I2C** for non-protected memory cards and **2-bus** and **3-bus** for protected memory cards.

Non-Protected Memory Cards

ASECard memory cards offer an easy-to-implement solution for applications that require low-cost, free-access storage capabilities. Such applications include leisure, health care, and vehicle maintenance. In their functionality, memory cards are like floppy disks, with no security or file management capabilities.

I²C

This family includes the ASE M2 and M4 cards. The number after the “M” indicates the size of the card’s EEPROM, in kilobits. For example, an M2 card has 2Kbits of memory, i.e. 256 bytes.

Extended I2C Family

Extended I²C cards contain up to 128 kilobits of EEPROM. These are the ASE M64 and M128. The number after the “M” indicates the size of the card EEPROM, in kilobits. An M64 card has a capacity of 8K bytes.

Protected Memory Cards

Protected memory cards use wired logic to control reading, updating, and access rights to the card memory. Some protected memory cards, such as 2-Bus or 3-Bus cards, conform to the card powering and Answer To Reset (ATR) standards ISO 7816-10.

Protected memory cards are best suited to applications in which data must be stored in write protected zones, but do not contain confidential data and do not require a complex and secure file structure.

In both 2-bus and 3-bus cards, all the memory area (except the password/PSC and counter) can be read freely. Cards that do not contain a password can be written to freely. For cards with a password, the password must be verified before data can be written. The number of maximum invalid password attempts is limited. Once this limit has been reached, the card can be read but writing to the card is permanently blocked. Resetting the card or turning power off to the card will not reset its password attempts counter. However, successful password verification resets the counter to 0.

ASE offers two sub-categories of protected memory cards:

2-bus Family

This family includes the **MP32** and **MP42** cards. 32 of the 256 bytes of 2-bus cards support a protection bit which enables locking of the data in the respective memory byte. This protects the specific data for rewriting. (For example, this area can be useful for keeping a card serial number or a card holder ID that must not be changed).

In addition to the protection bit, MP42 cards contain a password for writing (PSC), thus offering data writing security.

☞ **Note:** A common source of confusion is the difference between protection bits and the PSC. Many confuse between the two, but they are quite different:

In MP42 for example, The **entire** card content is protected by the password (PSC), but only the first 32 bytes can be locked for writing. When an individual memory location is locked for writing, it cannot be updated anymore even after a successful password verification!

The following diagram describes the structure of 2-bus protected memory cards (MP32 and MP42):

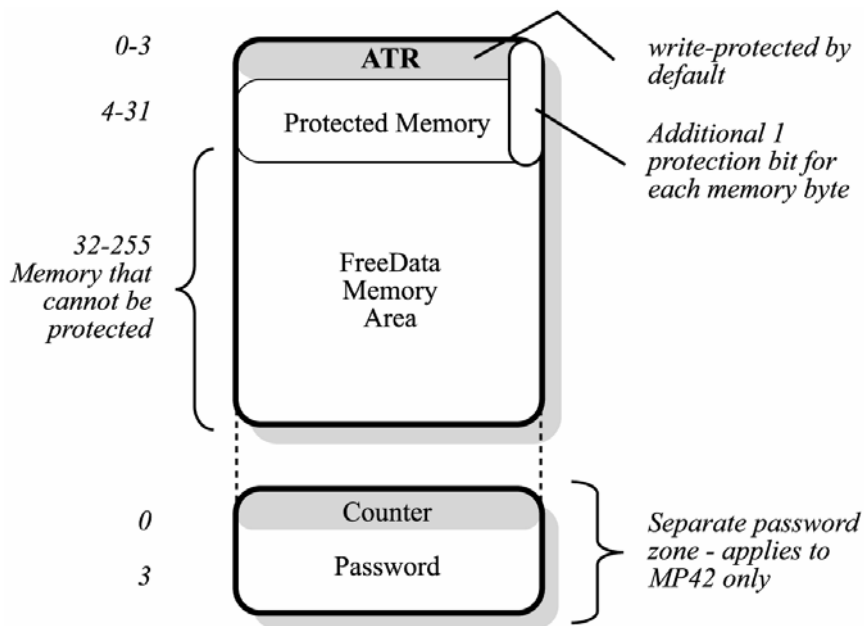


Figure 1 – 2-bus data and security structure map

2-bus protected memory cards contain 256 bytes of memory of which 32 bytes are protected. All 32 protected bytes have an additional protection bit for data locking.

Note: Some bytes, in the protected memory area, are already initialized at the factory and are write-protected by default.

MP42 contains a 4-byte zone for the PSC (password) which should be presented prior to writing data to the card. **The default PSC for MP42 cards is 0xFFFFF.**

3-bus Family

This family includes the **MP18** and **MP28** cards. Each of the 1021 bytes of M28 and 1024 bytes of MP18 cards supports a protection bit, which enables locking of the data in the respective memory byte for rewriting.

MP28 cards contain a password for writing (PSC), thus offering additional data security.

The following diagram describes the structure of 3-bus protected memory cards (MP18 and MP28):

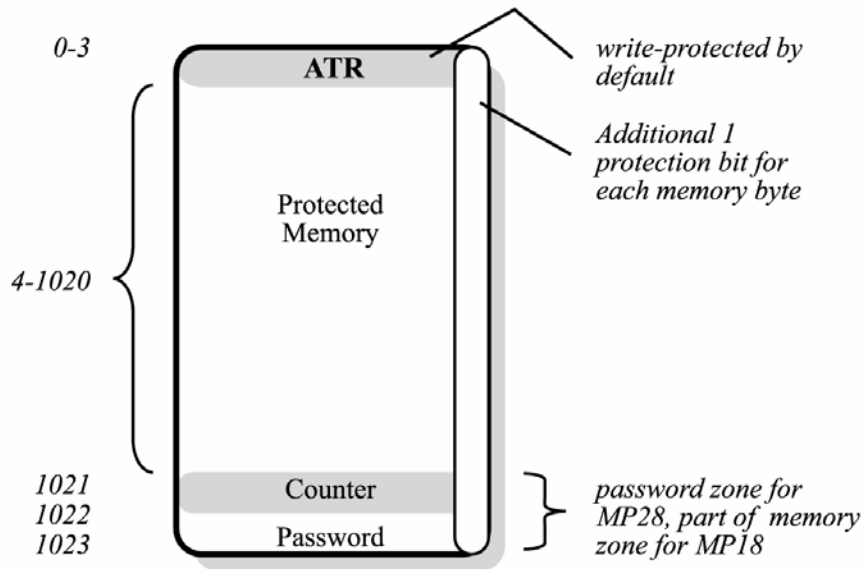


Figure 2 – 3-bus data and security structure map

3-bus protected memory cards contain 1021 (in MP28) or 1024 (in MP18) bytes of protected memory using an additional protection bit for data locking. Of the 1024 (or 1021) bytes, 4 bytes are reserved for the ATR.

MP28 cards contain a password zone of 3 bytes for the password and password counter. You should not try to access these 3 bytes directly. **The default password for these cards is 0xFFFF.**

MP18 cards do not contain a password, so the password zone is a continuous part of the protected memory area.

Protected Memory Cards Selection Considerations:

Please take into account the following when choosing protected memory cards for your application:

- ◆ In both 2-bus and 3-bus cards, all card data can be read freely.
- ◆ Cards that do not contain a password can be written to freely, unless locked for rewriting.
- ◆ For cards with a password, it must be presented before data can be written.

- ◆ The number of maximum consecutive password failed attempts is limited; once this limit is reached, the card can be read but writing to the card is blocked

☞ *Note: Constant ATR ensures the ability to distinguish between 2 and 3-bus ASE protected memory cards. However, it is impossible to distinguish among different cards within one of these groups (such as between MP18 and MP28, or between MP32 and MP42). Therefore, you must know in advance the card that your application uses.*

ASE protected memory cards are supported by ASEDdrive IIIe under PC/SC.

ATR Values of 2-bus and 3-bus Cards

2-bus and 3-bus cards have 4 bytes of ATR with the following values:

MP32/MP42	A2, 13, 10, 91
MP18/MP28	92, 23, 10, 91

The ATR used is only a convention and can be changed upon user request. However, it is recommended to use the conventional values.

2-bus and 3-bus Cards Protected Area Memory Map

In the protected memory area of both 2-bus and 3-bus cards some of the values are protected in the initialization phase of the card. The following convention is used:

Byte 0 – 3	ATR headers
Byte 4 – 7	Chip manufacturer information
Byte 8 – 12	Card embedder information
Byte 21 – 26	Application Provider Identifier

Working with memory cards in ASEDrive IIIe

ASEDrive IIIe smart card readers can support memory cards (synchronous cards), in addition to CPU based smart cards.

Supported Memory Cards

ASEDrive IIIe supports the following types of memory cards:

- 2BUS protected memory cards
- 3BUS protected memory cards
- I2C memory cards
- XI2C (Extended I2C) memory cards

In order to simplify the programming model, ASEDrive IIIe provides the programmer with a view of an ISO7816-4 CPU smart card with Transparent Files.

Protected Memory Card in ASEDrive IIIe

The protected memory card (2BUS and 3BUS) types are logically seen as ISO7816-4 CPU smart cards with 2 binary files: 3F00 and 3F01. The file 3F00 (the Master File in CPU cards) represents the regular *data memory* of the card (usually 256 bytes in 2BUS cards and 1021 bytes in 3BUS cards) and the file 3F01 represents the protection bits (32 bits in 2BUS cards and 1021 bits in 3BUS cards). The byte in address 'addr' in file 3F01 represents the protection bit of the corresponding data byte stored in address 'addr' in the data memory in file 3F00.

Most 2BUS and 3BUS cards have a password that must be verified before writing to the card is enabled. 2BUS cards have a 3 bytes password and 3BUS cards have a 2 byte password.

Non Protected Memory Cards in ASEDrive IIIe

The I2C and XI2C memory cards contain only one logical binary file, 3F00, which contains the data memory of the card. The file is automatically selected so it is not required to send a SELECT_FILE APDU. The actual file size depends on the actual cards size.

The ASEDrive IIIe reader cannot automatically distinguish between I2C and XI2C cards. In addition, it cannot detect automatically the size of an I2C or XI2C card. Some readers do detect the size of the cards, however, by doing this, they write some data to the card and restore the

original data at the end of the detection process. ASEDrive IIIe policy is not to implicitly write on the card. It is insecure and may damage the card, if for example, the user removes the card before the process terminates or the operation does not terminate successfully. Thus, the card size should be known by advance by the programmer.

When ASEDrive IIIe detects that the inserted card is an I2C or XI2C card, it assumes that the card is of type I2C. If this is the case, no action needs to be done and the application will work properly. For the cases that the application expects XI2C cards, the programmer should add a call to SCardControl, as described in the example below:

```
#include "winsmcrd.h"
```

```
#define IOCTL_I2C_EXTENSION SCARD_CTL_CODE(2050)
```

```
SCardControl(hCard,IOCTL_I2C_EXTENSION ,NULL,0,NULL,0,&Len);
```

This informs ASEDrive IIIe to treat cards of type I2C/XI2C as an XI2C card.

Working with memory cards this way is simple and easy. The user should simply *select* the file to read using the ISO7816-4 SELECT_FILE command, and then issue a READ_BINARY or WRITE_BINARY to that file, as specified in ISO7816-4. The password of 2BUS and 3BUS cards is verified with the ISO7816-4 VERIFY command.

Sending the ISO7816-4 APDUs is using in the most natural way, using the SCardTransmit function, rather than using SCardControl . The protocol type that should be used is RAW, in both SCardConnect and SCardTransmit.

NOTE: The class byte for all APDUs is 0x0.

```
#include "winsmcrd.h"
```

```
//No In parameters No Out parameters
```

```
#define IOCTL_I2C_EXTENSION SCARD_CTL_CODE(2050)
```

```
SCardControl (hCard, IOCTL_I2C_EXTENSION, NULL, 0,NULL, 0, &Len);
```

Card Command Samples

All Memory cards

Write Command

Cla	Ins	P1	P2	Lc	Le	Data
00	D6	00	20	08		01 02 03 04 05 06 07 08

Writes 8 bytes to address 0x20

Read Command

Cla	Ins	P1	P2	Lc	Le	Data
00	B0	00	20		08	Received from card

Read 8 bytes from address 0x20

Protected Memory Cards (2-bus, 3-bus)

Select protected section

Cla	Ins	P1	P2	Lc	Le	Data
00	A4	00	00	02		3F 01

Selects protected section 3F 01 (2BUS & 3BUS only).

Select data section

Cla	Ins	P1	P2	Lc	Le	Data
00	A4	00	00	02		3F 00

Selects data section 3F 00 (2BUS & 3BUS only).

Verify password

Cla	Ins	P1	P2	Lc	Le	Data
00	20	00	00	03		FF FF FF

Verifies password - 2BUS password is: FF FF FF

Change password

Cla	Ins	P1	P2	Lc	Le	Data
00	24	00	00	06		FF FF FF 11 22 33

Changes password 2BUS – Old password is: FF FF FF changed into: 11 22 33.

Write and protect data sequence (2BUS & 3BUS)

Cla	Ins	P1	P2	Lc	Le	Data
00	A4	00	00	02		3F 00

Select data section 3F 00

Cla	Ins	P1	P2	Lc	Le	Data
00	D6	00	00	08		01 02 03 04 05 06 07 08

Write 8 bytes

Cla	Ins	P1	P2	Lc	Le	Data
00	A4	00	00	02		3F 01

Select protected section 3F 01

Cla	Ins	P1	P2	Lc	Le	Data
00	D6	00	00	08		01 02 03 04 05 06 07 08

Write 8 bytes