GemClub-*Memo*

Technical Specifications

Version 1.0

GEMPLUS

December 1998

SPECIFIC WARNING NOTICE

All information herein is either public information or is the property of and owned solely by GEMPLUS who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of GEMPLUS's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:
- **the copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.**
- **this document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.**

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided « AS IS » without any warranty of any kind. Unless otherwise expressly agreed in writing, GEMPLUS makes no warranty as to the value or accuracy of information contained herein. The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, GEMPLUS reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

GEMPLUS HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION CONTAINED HEREIN, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL GEMPLUS BE LIABLE, WHETHER IN CONTRACT, TORT OR OTHERWISE, FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER INCLUDING BUT NOT LIMITED TO DAMAGES RESULTING FROM LOSS OF USE, DATA, PROFITS, REVENUES, OR CUSTOMERS, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION CONTAINED IN THIS DOCUMENT.

Smart Cards and Smart Card Readers are patent protected by Innovatron and Bull CP8 and are produced by GEMPLUS under license.

Printed in France.

GEMPLUS, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.
Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90

Document Reference: DPD10370A00

CONTENTS

List of Figures

List of Tables

PREFACE

This document describes the GemClub-*Memo* smart card. It provides both electrical and functional information about the card memory module, and physical information about the card itself.

Audience

This manual assumes that you have basic knowledge of smart card technology.

Notation

The following notation and conventions are used throughout this document.

By default, a numeric value is expressed in decimal notation.

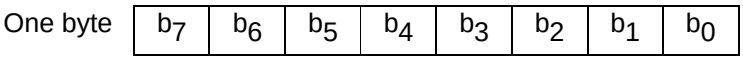
Whenever a value is expressed in binary, it will be followed by the character b. For example the decimal value 13 expressed in binary becomes **1101b**.

A hexadecimal number is followed by the character h. For example the decimal value 13 expressed in hexadecimal becomes **0Dh**.

The value 00h is assigned to each "RFU (Reserved for Future Use)" byte.

Bit Numbering

A **byte B** consists of 8 bits $b_7b_6b_5b_4b_3b_2b_1b_0$: b_7 is the most significant bit and b_0 the least significant bit:



A word consists of 32 bits (four bytes) which are numbered $b_{31}b_{30}b_{29}.....b_2b_1b_0$: b_{31} is the most significant bit and b_0 the least significant bit.

For More Information

For further information on GemClub - *Memo,* the following document exists:

- GemClub - *Memo* Application Note

OVERVIEW

With GemClub-*Memo,* a new generation of memory cards is born. It has a memory of two kilobits and offers improved features such as:

- Easier implementation: the cards use the T=0 protocol (the first memory card in the world to do so)
- Better security (three secret codes, access conditions, etc.)
- Enhanced reliability, automatic backup for sensitive data, reliable protocol

In brief, it is more like a microprocessor card than its predecessors.

The advantages of using the T=0 protocol are:

- It is present in most terminals
- It is known by developers world-wide
- It does not require the development of specific libraries or drivers
- It has an Answer to Reset (ATR) which allows the cards to be recognized by terminals
- It uses APDU commands (like microprocessor cards)

GemClub-*Memo* is the first memory card to be compatible with the PC/SC standard.

GemClub-*Memo* can be used for a variety of applications, such as:

- Loyalty programs
- Private electronic purses
- Meter applications (that is, measuring the consumption of a commodity)
- Identity

OPERATING MODES

GemClub-*Memo* cards can be delivered in one of two modes:

- Issuer mode
- User mode

These two modes define two different ways of protecting the card.

Sample cards are delivered in issuer mode for prototyping.

A logical fuse is "blown" to go from issuer mode to user mode. In practice, this fuse is two "mode" bits in the issuer area. The bits have the value 01b in issuer mode and 10b in user mode.

Warning: *The values 00b and 11b are not allowed. If they occur, (from an error during an* ***Update*** *command for example), then the card is permanently blocked and can no longer be used.*

Mode bits	Mode
00b	Not allowed - card permanently blocked.
01b	Issuer mode
10b	User mode
11b	Not allowed - card permanently blocked.

Table 1. Summary of Mode Bit Values

Note: *The change from issuer mode to user mode is irreversible.*

The user mode can be emulated in issuer mode to help prototyping.

Issuer Mode

This is the mode in which the card is initialized and personalized.

Access Rights

All the EEPROM areas (except for the manufacturer area) can be updated after presentation of Card Secret Code 0 (CSC 0). Any part of the EEPROM can be freely read, except for the card secret codes which are protected by themselves (that is, to read CSC 1, it is necessary to present CSC 1).

Ratification Counters

In this mode, these are operational and count the number of consecutive incorrect card secret code presentations. If a ratification counter reaches the value of 4, the area of EEPROM that is being protected is locked.

Backup Control & CTC Mechanism

These are not active in the issuer mode. The CTC and balance areas can be freely read and can be updated if CSC 0 has been correctly presented.

User Mode

This is the final mode of the card after it has been personalized.

Access Rights

The EEPROM areas can be accessed if the appropriate access conditions are satisfied.

Application and security mechanisms are active in this mode, see "*Access Conditions Area*" and the chapter, "*Anti-Withdrawal Mechanism*".

The user mode can be emulated in issuer mode. See the **Verify** command for further information.

Note: *For detailed information on access conditions, card secret codes and ratification counters in both modes, see the chapter, "GemClub-*Memo *Card Mapping".*

GEMCLUB-*MEMO* CARD MAPPING

The GemClub-*Memo* card has a total memory of two kilobits or 256 bytes. The memory is accessed at word level. A word is 32 bits (four bytes).

The structure of the GemClub-*Memo* memory is shown in the *GemClub-Memo Card Mapping* figure below:

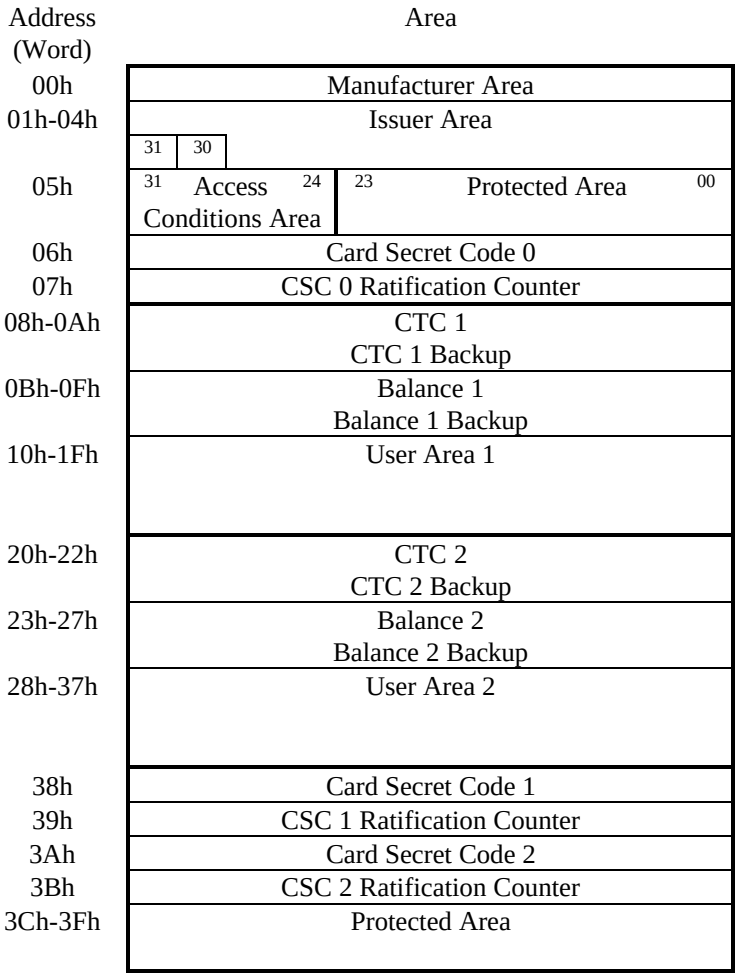


Figure 1. GemClub-*Memo* Card Mapping

Manufacturer Area

The 32 bits of the manufacturer area contain customer reference information, which is loaded by GEMPLUS at the time of manufacture. For sample cards, this value is FFh FFh FFh AAh.

Issuer Area

Two bits in this area (bits 31 and 30 in address 04h) are the mode bits. They are used to indicate whether the card is in issuer mode (01b) or user mode (10b).

Note: *If the mode bits are modified, the modification does not take effect until after a card reset.*

The remaining 126 bits contain issuer-specific information, such as serial numbers and validity dates.

This area is programmed during the personalization phase. It can always be read, but can only be updated in issuer mode if the CSC 0 is presented. Once the card is in user mode, the issuer area can no longer be modified.

Card Secret Code 0

Issuer Mode

The code is used to protect the whole card. It can be read and updated in this mode provided that it has been presented beforehand.

User Mode

The code is used to protect the access conditions area and the protected areas. It can never be read in this mode, but it can be updated provided that it has been presented beforehand.

The secret code is 32 bits (four bytes). The values 00h 00h 00h 00h, 80h 00h 00h 00h, 7Fh FFh FFh FFh and FFh FFh FFh FFh should not be used. Although it is possible to update the code with any of these values, the **Verify** command will fail when presenting them (error code 63h 00h).

Warning: *If the code is updated with any of these values, the value cannot be overwritten with another value, and effectively, CSC 0 can no longer be used.*

For sample cards, CSC 0 is AAh AAh AAh AAh.

CSC 0 Ratification Counter

The CSC 0 ratification counter is used to count the number of consecutive incorrect presentations of card secret code 0 that have been made. It allows up to three consecutive incorrect presentations. After a fourth consecutive incorrect presentation, the secret code is permanently blocked.

Although an entire word is reserved for this counter, in fact only the four msb are used (bits 31-28). Initially, these bits have the value 0000b. After the first incorrect presentation they are 1000b. For the second, third and fourth incorrect presentations, they take the values, 1100b, 1110b and 1111b respectively.

After a correct presentation of the code (assuming that the card is not blocked), the four bits are reset to the value 0000b.

In both issuer and user mode, the CSC 0 ratification counter can be freely read and it is incremented automatically.

Access Conditions Area

This area stores the access conditions for the CTCs, the balances and the user areas. The access conditions are active only in user mode and are coded on just the first byte (bits 31 - 24) of the word at address 05h.

The access conditions byte is coded as follows:

Rb1	Ub1	Ru1	Uu1	Rb2	Ub2	Ru2	Uu2

Where:

Rb1 controls the read access to CTC 1 and balance 1 (0 = free access; 1 = protected by CSC 1).

Ub1 controls the update access to balance 1 (0 = protected by CSC 1, 1 = forbidden).

Ru1 controls the read access to user area 1 (0 = free access, 1 = protected by CSC 1).

Uu1 controls the update access to user area 1 (0 = protected by CSC 1, 1 = forbidden).

Rb2 controls the read access to CTC 2 and balance 2 (0 = free access, 1 = protected by CSC 2).

Ub2 controls the update access to balance 2 (0 = protected by CSC 2, 1 = forbidden).

Ru2 controls the read access to user area 2 (0 = free access, 1 = protected by CSC 2).

Uu2 controls the update access to user area 2 (0 = protected by CSC 2, 1 = forbidden).

The access conditions can always be read, but require the presentation of CSC 0 in order to be updated (this is the same for both issuer mode and user mode).

Note: *Any modifications to the access conditions do not take effect until after a reset.*

Protected Areas

There are two of these, bits 23-0 in address 05h, and the four words at the end of the EEPROM (addresses 3Ch - 3Fh). The two protected areas share the same access conditions.

The protected areas can be used for data like the two user areas.

The protected areas can always be read, but require the presentation of CSC 0 in order to be updated (this is the same for both issuer mode and user mode).

Card Transaction Counter

There are two of these counters, CTC 1 and CTC 2. CTC 1 is incremented each time that balance 1 is updated and CTC 2 is incremented each time that balance 2 is updated. The CTCs are coded on three words. The structure is shown in the figure "*CTC Structure*". The first word is the current CTC value (A), the second word is the backup value, (B, which is equal to the previous value of the CTC) and the third word is used as an anti-withdrawal flag (F). See the chapter, "*Anti-withdrawal Mechanism*" for further details.

Field		Address	
		CTC 1	CTC 2
Current value	A	08h	20h
Backup value	B	09h	21h
Anti-Withdrawal Flag	F	0Ah	22h

Figure 2. CTC Structure

Issuer Mode

In issuer mode, the three CTC fields can be read freely, but can only be updated if the CSC 0 has been correctly presented. The three fields are accessed independently of each other.

The CTC backup mechanism is not active in this mode and the CTCs are not automatically incremented when the balance is updated.

User Mode

In user mode, the three CTC fields can be read freely if Rb1/Rb2 = 0, otherwise, if Rb1/Rb2 = 1, the appropriate CSC (1 or 2) must be presented. They can never be updated in user mode (because they are incremented automatically).

The counters are automatically incremented each time that the first word in the corresponding balance is written to. The counter is stored in the 31 lsb of the word (the msb is not used). Once the counter reaches its maximum value of 7Fh FFh FFh FFh or FFh FFh FFh FFh (depending on the value of the msb), then the corresponding balance can no longer be written to.

It must therefore be initialized in issuer mode to FFh FFh FFh FFh (or 7Fh FFh FFh FFh) minus the maximum number of transactions that are to be allowed. For example, if the CTC is to be limited to 1,000 transactions (3E8h), then the CTC must be initialized as FFh FFh FFh FFh - 03E8h = FFh FFh FCh 17h (or 7Fh FFh FFh FFh - 03E8h = 7Fh FFh FCh 17h).

If an attempt is made to update the CTC, an error message (69h 82h) is returned. If the anti-withdrawal flag is corrupted, or the maximum value of the CTC is reached, then a different error message (65h 81h) is returned.

Balance

As stated earlier, there are two balances, balance 1 and balance 2. Each has three fields: the balance value (two words, A1, A2), the backup value (two words, B1, B2) and an anti-withdrawal flag (one word, F, see the section, "*Anti-withdrawal Mechanism*" for further details). For each balance, these fields are stored in the following order: F, A1, B1, A2, B2. Thus to update balance 1, for example, it is necessary to update A1 (address 0Ch), followed by A2 (address 0Eh).

Field		Address	
		Balance 1	Balance 2
Anti-Withdrawal Flag	F	0Bh	23h
Current value	A1	0Ch	24h
Backup value	B1	0Dh	25h
Current value	A2	0Eh	26h
Backup value	B2	0Fh	27h

Figure 3. Balance Structure

Issuer Mode

In issuer mode, the three balance fields can be read freely, but can only be updated if CSC 0 has been correctly presented. The three fields (five words) are accessed independently of each other.

The balance backup mechanism is not active in this mode.

User Mode

In user mode, the three balance fields can be read freely if Rb1/Rb2 = 0, otherwise, if Rb1/Rb2 = 1, the appropriate CSC (1 or 2) must be presented. If Ub1/Ub2 = 0, the balances can be updated after presenting the appropriate CSC (1 or 2), otherwise, if Ub1/Ub2 = 1, they can never be updated.

Balances are used to store sensitive data. Each time that a balance is written to, the corresponding CTC is incremented.

Notes: *The **Update** command updates the balance one word at a time. Consequently two **Update** commands are necessary to update the balance. The first word must be updated before the second word, otherwise an error (69h 82h) is returned.*

*The new balance is only updated after the second word has been updated. If a **Reset** is executed after the update of the first word but before the update of the second word, then the previous value of the balance is restored.*

It is the update of the first word which increments the CTC.

User Area

There are two user areas, called 1 and 2, which can be used to store application data. Each area is 16 words (64 bytes) long.

Issuer Mode

In issuer mode, this area can be read freely, but CSC 0 is necessary to update it.

User Mode

In user mode, access to each area is governed by the conditions set in the access conditions area. The areas can be read freely if Ru1/Ru2 = 0, otherwise, if Ru1/Ru2 = 1, the appropriate CSC (1 or 2) must be presented. If Uu1/Uu2 = 0, the areas can be updated after presenting the appropriate CSC (1 or 2), otherwise, if Uu1/Uu2 = 1, they can never be updated.

Card Secret Codes 1 and 2

These are secret codes which can be used to protect the two CTCs, the two balances and the two user areas. Like CSC 0, they are 32 bits (four bytes) each. The values 00h 00h 00h 00h, 80h 00h 00h 00h, 7Fh FFh FFh FFh and FFh FFh FFh FFh should not be used. Although it is possible to update the code with any of these values, the **Verify** command will fail when presenting them (error code 63h 00h).

These codes cannot be read once the card is in user mode. They can be updated, but only if they have first been correctly presented.

Warning: *If the code is updated with any of these values, the value cannot be overwritten with another value, and effectively, the code can no longer be used.*

For sample cards, CSC 1 is 11h 11h 11h 11h and CSC 2 is 22h 22h 22h 22h.

CSC 1 and 2 Ratification Counters

CSC 1 and CSC 2 each have a corresponding ratification counter which is used to count the number of consecutive incorrect presentations of that secret code. The two counters function in exactly the same way as the ratification counter for CSC 0.

Note: *A maximum of three consecutive incorrect presentations are allowed. After a fourth consecutive incorrect presentation, the secret code is permanently blocked.*

Area Access Conditions

AREA	ISSUER ACCESS		USER ACCESS	
	Read	Update	Read	Update
Manufacturer	Free	Never	Free	Never
Issuer	Free	CSC 0	Free	Never
Access Conditions	Free	CSC 0	Free	CSC 0
Protected	Free	CSC 0	Free	CSC 0
Card Secret Code 0	CSC 0	CSC 0	Never	CSC 0
CSC 0 Ratification Counter	Free	Automatic	Free	Automatic
CTC 1	Free	CSC 0	Free or CSC 1	Automatic
Balance 1	Free	CSC 0	Free or CSC 1	CSC 1 or Never
User Area 1	Free	CSC 0	Free or CSC 1	CSC 1 or Never
CTC 2	Free	CSC 0	Free or CSC 2	Automatic
Balance 2	Free	CSC 0	Free or CSC 2	CSC 2 Or Never
User Area 2	Free	CSC 0	Free or CSC 2	CSC 2 or Never
Card Secret Code 1	CSC 1	CSC 0	Never	CSC 1
CSC 1 Ratification Counter	Free	Automatic	Free	Automatic
Card Secret Code 2	CSC 2	CSC 0	Never	CSC 2
CSC 2 Ratification Counter	Free	Automatic	Free	Automatic
Protected	Free	CSC 0	Free	CSC 0

Table 2. Area Access Conditions

COMMANDS

GemClub-*Memo* only uses three commands. These are:

- Read
- Update
- Verify

These commands are described individually in this chapter.

READ

This command is used to read a single word (four bytes) from the memory.

Warning: *The data is stored in the card MSB first, that is, D3, D2, D1, D0, but the response for this command has the LSB first, (that is, D0, D1, D2, D3).*

Format

CLA	INS	P1	P2	Le
80h	BEh	00h	P2	04h

Parameters

P2 — Address of the word to be read. This address is the word number. See the chapter, "*GemClub*-Memo *Card Mapping*" to find the correct addresses.

Note: *The CLA and P1 bytes are not tested by the card, so can take any values.*

Response

Data (D0, D1, D2, D3)	SW1, SW2

Where:

Data — is the contents of the word that has been read.

Note: *Remember that the data is read in the inverse order to which it is stored in the card, that is, Least Significant Byte (D0) first, Most Significant Byte (D3) last.*

SW1 and SW2 — are the status bytes. The possible values are shown in the table below:

SW1	SW2	Description
65h	81h	Unknown mode.
67h	00h	Invalid length of expected data.
69h	82h	Security not satisfied.
6Bh	00h	Invalid P2 parameter.
6Dh	00h	Invalid instruction byte (INS).
90h	00h	Command successfully executed.

UPDATE

This command is used to update a single word (four bytes) in the memory. The command automatically erases the word before writing the new value.

Notes: *The **Update** command updates the balance one word at a time. Consequently two **Update** commands are necessary to update the balance. The first word must be updated before the second word, otherwise an error code (69h 82h) is returned.*

*The new balance is only updated after the second word has been updated. If a **Reset** is executed after the update of the first word but before the update of the second word, then the previous value of the balance is restored.*

When updating the word of a balance in user mode, the address to be specified in the command can be either the address of the active value, or of the corresponding backup value.

Caution: *The data is stored in the card MSB first, that is, D3, D2, D1, D0, but the data in this command must be LSB first, (that is, D0, D1, D2, D3).*

It is the update of the first word of the balance which increments the CTC.

Format

CLA	INS	P1	P2	Lc	Data
80h	DEh	00h	Ad	04h	Data

Parameters

P2	Address of the word to be updated. This address is the word number. See the chapter, "*GemClub*-Memo *Card Mapping*" to find the correct addresses.
Data	Is the value of the data (four bytes, 32 bits) to be written to the card, Least Significant Byte (D0) first, Most Significant Byte (D3) last.

Note: *The CLA and P1 bytes are not tested by the card, so can take any values.*

Response

SW1, SW2

Where:

SW1 and SW2 are the status bytes. The possible values are shown in the table below:

SW1	SW2	Description
65h	81h	Memory error: unknown flag, unknown mode or CTC reached maximum allowed value.
67h	00h	Invalid Lc value.
69h	82h	Security not satisfied, words in balance updated in wrong order or attempt to update flag word.
6Bh	00h	Invalid P2 parameter
6Dh	00h	Invalid instruction byte (INS)
90h	00h	Command successfully executed.

VERIFY

This command is used to present (verify) a card secret code. The choice of card secret code is defined by the value of P2. In effect, P2 is the start address (the word number) of the ratification counter for the card secret code which is to be verified.

Caution: *The data is stored in the card MSB first, D3, D2, D1, D0, but the code in this command must be presented LSB first, that is, D0, D1, D2, D3.*

This command can also be used in issuer mode to emulate the card in user mode.

Note: *Emulating the user mode allows the user to test the card's behavior in user mode. After a* ***Reset,*** *the card returns to issuer mode.*

Format

CLA	INS	P1	P2	Lc	Data
00h	20h	00h	P2	04h	Data

Parameters

P2 — Address of the ratification counter for the card secret code to be verified, or value specifying that the card is to emulate user mode.

Value	Meaning
07h	CSC 0 is presented
39h	CSC 1 is presented
3Bh	CSC 2 is presented
3Ah	Card is to emulate user mode. (CSC 0 must already have been correctly presented.)

Data — Is the value of the secret code (four bytes, 32 bits) to be presented.

For user mode emulation, data is mandatory but its contents are not tested.

Note: *The CLA and P1 bytes are not tested by the card, so can take any values.*

Response

SW1, SW2

Where:

SW1 and SW2 are the status bytes. The possible values are shown in the table below:

SW1	SW2	Description
63h	00h	Invalid secret code or forbidden value (00h 00h 00h 00h, 80h 00h 00h 00h, 7Fh FFh FFh FFh or FFh FFh FFh FFh).
65h	81h	Unknown mode.
67h	00h	Invalid Lc value.
69h	82h	Security not satisfied, maximum number of presentations exceeded.
6Bh	00h	Invalid P2 parameter.
6Dh	00h	Invalid instruction byte (INS).
90h	00h	Command successfully executed.

ANTI-WITHDRAWAL MECHANISM

This mechanism is not available in issuer mode. In user mode, GemClub-*Memo* ensures the integrity of sensitive data (balances and CTCs) by means of an anti-withdrawal mechanism. This means that if the card is withdrawn from the reader during a transaction, the card is automatically returned to its previous state, prior to the start of the next transaction.

The general principle is this: for each data item which is protected (that is, CTCs, balances), the card stores the current value (A), the previous value (B) and a flag (F).

In the case of data items of one word, for example the CTCs, the card stores A, B and F. For data items of two words (balances), the current value is A1, A2, the backup value is B1, B2 and the flag is still one word, F. See the figures "*CTC Structure*" and "*Balance Structure*" in the "*GemClub - Memo Card Mapping*" chapter.

During normal processing, (that is, a transaction without a card withdrawal), the new value is written to A (or A1, A2), the previous value is written to B (or B1, B2) and the flag F is re-initialized.

If the card is withdrawn while the backup data is being written, the card knows this because the flag is not re-initialized, (that is, the flag does not have the value of 00h 00h 00h 00h). The value of the flag therefore is used to know when the card was withdrawn, and whether A (or A1, A2) should be restored to their previous value. All the zones with the anti-withdrawal mechanism are automatically restored if necessary, after a **Reset**.

In user mode, any address can be written to (if the access conditions allow it), that is a current value or a backup value. The card manages the addresses internally. In issuer mode, where there is no anti-withdrawal mechanism, all the words in the CTC and balance areas are accessed independently.

Note: *Each word of the CTC or the balance can be read independently via a* ***Read*** *command.*

The transaction is not successfully completed until the card returns status bytes of 90h 00h, following the update of the second word of the balance.

Emulating User Mode

The anti-withdrawal mechanism can also be used when emulating the user mode. Suppose a transaction is partially completed (for example, the first word only of a balance is updated), and then the card is reset. The previous value of the first word of the balance can be restored by emulating the user mode again. The sequence of commands in this example is as follows:

1. Emulate the user mode using the **Verify** command.
2. **Update** the first word of a balance (the previous value is written to B1).
3. Perform a **Reset**. The card returns to issuer mode.
4. Emulate the user mode again using the **Verify** command. The value in B1 is restored to A1.

ELECTRICAL CHARACTERISTICS

The GemClub-*Memo* Card DC characteristics are as follows:

3V Operation

Parameter	Description	Unit	Minimum	Maximum
Vcc	Supply Voltage	V	2.7	3.3
ICC	Supply current consumption	mA	-	5
Frequency	Clock frequency	MHz	1	5
T°	Chip operating temperature	°C	0	70
I/O VIH	Input high-level voltage	V	0.7*Vcc	Vcc
I/O VIL	Input low-level voltage	V	0.0	0.16*Vcc
I/O IIL	Input low-level current *Where* 0<Vil<0.16*Vcc	µA	-	250
I/O IIH	Input high-level current *Where* 0.7*Vcc<Vih<Vcc	µA	-	150
I/O VOH	Output high-level voltage (*where* IOH=-20µA).	V	0.7*Vcc	Vcc
I/O VOL	Output low-level voltage (*where* IOL=1.0mA).	V	0.0	0.4
CLOCK VIH	Input high-level voltage	V	0.7*Vcc	Vcc
CLOCK VIL	Input low-level voltage	V	0.0	0.16*Vcc
CLOCK IIH/IIL	Input high-level and low-level current *Where* 0<Vil<0.16*Vcc 0.7*Vcc<Vih<Vcc	µA	-10	+10
RESET VIH	Input high-level voltage	V	0.7*Vcc	Vcc
RESET VIL	Input low-level voltage	V	0.0	0.16*Vcc
RESET IIH/IIL	Input high-level and low-level current *Where* 0<Vil<0.16*Vcc 0.7*Vcc<Vih<Vcc	µA	-10	+10

Table 3. Electrical Characteristics at 3V

Note: *There is an internal pull-up on the I/O.*

5V Operation

Parameter	Description	Unit	Minimum	Maximum
Vcc	Supply voltage	V	4.5	5.5
ICC	Supply current consumption	mA	-	10
Frequency	Clock frequency	MHz	1	5
T°	Chip operating temperature	°C	-20	85
I/O VIH	Input high-level voltage	V	0.7*Vcc	Vcc
I/O VIL	Input low-level voltage	V	0.0	0.16*Vcc
I/O IIL	Input low-level current *Where* 0<Vil<0.16*Vcc	mA	-	1
I/O IIH	Input high-level current *Where* 0.7*Vcc<Vih<Vcc	µA	-	150
I/O VOH	Output high-level voltage (*where* IOH=-20µA).	V	0.7*Vcc	Vcc
I/O VOL	Output low-level voltage (*where* IOL=1.6mA).	V	0.0	0.4
CLOCK VIH	Input high-level voltage	V	0.7*Vcc	Vcc
CLOCK VIL	Input low-level voltage	V	0.0	0.16*Vcc
CLOCK IIH/IIL	Input high-level and low-level current *Where* 0<Vil<0.16*Vcc 0.7*Vcc<Vih<Vcc	µA	-10	+10
RESET VIH	Input high-level voltage	V	0.7*Vcc	Vcc
RESET VIL	Input low-level voltage	V	0.0	0.16*Vcc
RESET IIH/IIL	Input high-level and low-level current *Where* 0<Vil<0.16*Vcc 0.7*Vcc<Vih<Vcc	µA	-10	+10

Table 4. Electrical Characteristics at 5V

The voltage on all inputs or outputs must not exceed Vcc + 0.3V or be less than Vcc - 0.3V

Notes: *GemClub*-Memo *ESD tolerance is measured according to the test specification described in MIL-STD883C, method 3015-6.*

PHYSICAL CHARACTERISTICS

The GemClub-*Memo* card's physical characteristics comply with the ISO 7816-1 specification. The card dimensions are as follows:

Length = 85.6 mm

Width = 53.97 mm

Thickness = 0.78 mm

Card Contacts

The GemClub-*Memo* card contacts are positioned according to the ISO 7816-2 specifications. GemClub-*Memo* card contact positions and assignments are as follows:

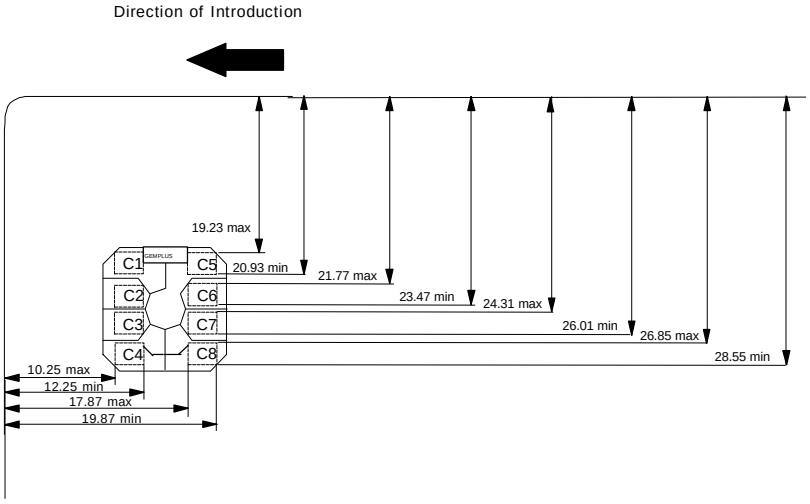


Figure 4. GemClub-*Memo* Card Contact Positions and Assignments

C1	*Vcc*	*Power Supply*
C2	*RST*	*Reset Signal*
C3	*CLK*	*Clock Signal*
C5	*Vss*	*Ground*
C7	*I/O*	*Input / Output Signal.*

Contacts C4, C6 and C8 are not used.

Operating Temperatures

The chip operating temperature range is -20ºC to 85ºC (5V).

The card body operating temperature depends upon the type of plastic that is selected when placing the order. The following temperatures apply:

Plastic	Operating Temperature
PVC	-20ºC to 55ºC
ABS	-20ºC to 60ºC
PVC HT	-20ºC to 70ºC
ABS C	-20ºC to 70ºC (peak of 85ºC)
PET	-20ºC to 85ºC

Card Reliability

GemClub-*Memo* card reliability data is as follows:

	Test	Standard Ref.	Methodology	Test Success Criteria
1	Card dimensions	ISO 7810	85.47<length<85.72mm 53.92<width<54.03mm 0.76<thickness<0.84mm	Nominal functionality
2	Contact location	ISO 7816-2	-	Nominal functionality
3	Level difference between contacts and card	ISO 7816-1	-100 µm; +100 µm	Nominal functionality
4	Dynamic bending torsional stress	ISO 10373	1 ISO cycle = 500 bends (width) 500 bends (length) 500 torsions	Nominal functionality Visual
5	Salt atmosphere	CEI68211	48 h at 35ºC, 45% RH, 5% NaCl	Nominal functionality
6	Chip Assembly Humidity	CECC 90 000	168 h at 85ºC / 85 %RH	Nominal functionality
7	Vibration	ISO 10373	3 axes, 1 hr each direction. 10g acceleration, 10 Hz - 500 Hz	Nominal functionality
8	Reader insertion for contacts		10,000 insertions	Nominal functionality
9	Card stability with temperature		48 h at 70ºC (dry Tº) (depending on the card body -see *Operating Temperatures*)	Nominal functionality Dimensions
10	Cold storage temperature		24 h at -25ºC	Nominal functionality Dimensions
11	Card stability with humidity (and temperature)	Based on 7810 § 8-1-5	168 h at 50ºC / 93%RH	Nominal functionality Dimensions
12	Data retention	Semi-conductor standard	10 years / 55ºC	Nominal functionality
13	ESD protection	MIL STD -883 Method 3015-6	Class A : 4Kv	Nominal functionality
14	EEPROM		100,000 write / erase cycles	Nominal functionality

Table 5. Card Reliability Data

Note: *Cards can be stored for one year at 25°C +/- 5°C and 60% RH +/- 20% without UV light.*

APPENDIX A. ANSWER TO RESET

When a terminal resets a GemClub-*Memo* card, it responds by returning a standard Answer To Reset (ATR).

GemClub-*Memo*'s ATR is compliant with the ISO 7816 standard.

Historical characters designate general information implemented by the card manufacturer. The specification for these characters is outside the scope of the standard specifications.

Caution: *Application software must not reject a card on the basis of a given ATR (to allow the use of future card versions). The value of T2 may be changed without prior notification.*

Character Type	Byte	Value	Description
Initial and Format	TS	3Bh	Bit synchronization and structure, direct convention: Z=1, LSB first
	T0	02h	Two historical bytes. Default parameters: F=372, D=1, Vpp generated internally, no extra guard time between two characters, T=0 protocol.
Historical	T1	53h	GemClub-*Memo* chip
	T2	XXh	Chip version

Table 6. Answer To Reset

GemClub-*Memo* can operate at 3v or 5v. At the application level, it is the reading of the T1 byte which defines the card as a GemClub-*Memo* card, and allows the card to operate at 3v.

APPENDIX B. COMMUNICATION PROTOCOL

GemClub-*Memo* cards send and receive data under the T=0 communication protocol in accordance with the ISO 7816-3 standard.

The exchanges between the reader and the card respect the ISO 7816-3 at the transport level (TPDU) as well as at the application level (APDU). The EMV specifications are also respected at the transport level.

APDU Exchanges

A command is made up of five bytes:

CLA: Class byte (not tested by the card)

INS: Proprietary instruction byte

P1: Not tested by the card (given the value 00h)

P2: Address in EEPROM (or 3A to emulate user mode)

P3: This always has the value 04h.

For the **Update** and **Verify** commands, P3 is Lc (the length in bytes of the data to be sent). For the **Read** command, P3 is Le (the length in bytes of the data to be read).

If P3 is given any value other than 04h, the command fails and an error is returned.

TPDU Exchanges

Receiving a Character

A character is made up of a start bit, followed by eight data bits and a parity bit.

A falling I/O edge indicates that a character is to be received. Each bit (start bit, data bit or parity bit) is sampled three times, after 136, 184 and 264 time periods. If the three samples are not equal, or if a parity problem is detected, the corresponding byte is refused. The card indicates that the byte has been refused by setting the I/O to zero from 10.5 to 11.5 etu after the falling edge of the start bit.

The card accepts a time gap of +/- 0.2 etu for one bit and for the total of the first ten bits.

In receiving mode, the card can receive start bits at intervals of 12 etu, regardless of whether it was previously in sending mode or receiving mode.

Sending a Character

Each bit (start bit, data bit or parity bit) lasts for exactly one etu (372 time periods). After the ten bits have been received, the card switches to reception mode at 10.5 etu and samples the I/O from 10.84 to 11.19 etu.

The card can be set to sending mode:

- 13 etu after the falling edge of the last start bit if the card was previously in sending mode
- 16 etu after the falling edge of the last start bit if the card was previously in receiving mode (conforming to the EMV standards).

Rapid Communication Mode

A rapid communication mode exists in GemClub-*Memo*, allowing rapid access to the internal logic of the card. This can be used for personalization of the card in issuer mode. In the rapid communication mode, the general interface parameters are modified, one character is broken down as follows:

Bit	Sending mode	Receiving mode
One start bit	8 time units	9 time units
Eight data bits	8 time units each	8 time units each
One parity bit	7 time units	8 time units
One waiting bit	8 time units	8 time units
One retry bit	8 time units	8 time units
Two waiting bits	8 time units each	8 time units each

Table 7. Breakdown of a Character

The interface is managed in exactly the same way as for the standard mode except for the differences concerning the character format.

No time gap is allowed for the position of the I/O edges relative to the falling edge of the start bit.

Activating the Rapid Communication Mode

The rapid communication mode is only available in issuer mode, provided that CSC 0 has been correctly presented. If an attempt is made to activate it in user mode, the error 6Dh 00h (instruction not supported) is returned.

The mode is activated by using the following command.

Format

CLA	INS	P1	P2	Lc
80h	40h	00h	3Bh	04h

Response

SW1, SW2

Where:

SW1 and SW2 are the status return bytes. The possible values are shown in the table below:

SW1	SW2	Description
65h	81h	Unknown mode.
67h	00h	Invalid length of expected data.
69h	82h	Security not satisfied, maximum number of presentations exceeded or words in balance read in wrong order.
6Dh	00h	Invalid instruction byte (INS).
90h	00h	Command successfully executed.

ABBREVIATIONS

APDU	Application Protocol Data Unit
ATR	Answer To Reset
CLK	Clock signal
CSC	Card Secret Code
CTC	Card Transaction Counter
etu	elementary time unit
EMV	Europay-Mastercard-Visa
GND	Ground
ICC	Supply current consumption
IIH	Input high-level current
IIL	Input low-level current
I/O	Input / Output signal
lsb	Least significant bit(s)
LSB	Least Significant Byte(s)
msb	Most significant bit(s)
MSB	Most Significant Byte(s)
PC/SC	Personal Computer / Smart Card
RFU	Reserved for Future Use
RH	Relative Humidity
RST	Reset Signal
TPDU	Transport Protocol Data Unit
Vcc	Supply Voltage
VIH	Input high-level voltage
VIL	Input low-level voltage
VOH	Output high-level voltage
VOL	Output low-level voltage
Vpp	Programming voltage

COMMENT FORM

GEMPLUS is always looking for ways to improve its documentation. Please help us in this by taking a minute to complete the following questionnaire:

1. In a few words, how would you describe this document?

   _____

2. How do you use this document? (Please tick the corresponding box.)
   - ❑ I read it from beginning to end.
   - ❑ I only read the sections relevant to my immediate needs.

3. When you need to find information in this guide, where is the first place you usually look? (Please tick the corresponding box.)
   - ❑ Table of contents
   - ❑ I thumb through pages until I find what I'm looking for

4. How easily can you find information in this document? (Please circle your answer.)

1	2	3	4	5
Not easily				Very easily

5. How clear is the information in this document? (Please circle your answer)

1	2	3	4	5
Not clear at all				Extremely clear

6. When you try the instructions described in this document, how easily can you follow them? (Please circle your answer.)

1	2	3	4	5
Not at all				Extremely well

7. How well did you understand the product *before* reading this document? (Please circle your answer.)

1	2	3	4	5
Not at all				Practically an expert

8. *After* reading this document? (Please circle your answer.)

1	2	3	4	5
Not at all				Practically an expert

9. The best aspect of this document is:

   _____

10. If we were to change one aspect of this document, what would you like it to be? _____

Please return this evaluation form to:
GEMPLUS Technical and On-Line Documentation Team (T.O.L.D.)
BP100
GEMENOS 13881 Cedex
FRANCE