Clarista GemClub-*Memo*

Technical Specifications

V 2.1

GEMALTO, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.

Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90

Printed in France. Document Reference: D1072568

January 28, 2008

Contents

List of Figures

List of Tables

Introduction

This document describes the Clarista GemClub-Memo smart card. It provides electrical, functional and physical information.

This Technical Specifications has been updated to describe the changes and improvements made on Clarista GemClub-*Memo* with the introduction of a new chip in replacement of the ST M37002B.

This new chip is the Theseus ® Titanium 40 from SST.

In the specification hereafter, when necessary, the distinction between the 2 Clarista GemClub-*Memo* versions will be as follow:

- Clarista GemClub-Memo V1 (or 'Clarista GCM v1') will be mentioned for the one using the chip M37002B (stopped in Q4 2007)
- Clarista GemClub-Memo V2 (or 'Clarista GCM v2') will be mentioned for the one using the chip Theseus ® Titanium 40, introduced in Q4 2007.

Who Should Read This Book

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

Conventions

The following conventions are used in this document:

Numeric Values

By default, numeric values are expressed in decimal notation.

- Binary numbers are followed by the 'b' character. For example, the decimal value 13 is expressed in binary as **1101b**.
- Hexadecimal numbers are followed by the 'h' character. For example, the decimal value 13 is expressed in hexadecimal as **0Dh**.

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:

One byte	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0

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 Clarista GemClub - *Memo,* the following document exists:

- Clarista GemClub - *Memo* Application Note

Contact Our Hotline

If you do not find the information you need in this manual, or if you find errors, contact the Gemalto hotline at http://support.gemalto.com/.

Please note the document reference number, your job function, and the name of your company. (You will find the document reference number at the bottom of the legal notice on the inside front cover.)

1

Overview

Clarista GemClub- *Memo* was initially based on a memory chip (ST M37002B). This chip is now replaced by the Theseus ® Titanium 40 from SST.

This new version ensures a full backwards compatibility with original Clarista GemClub- *Memo* (based on M37002B) except on 2 points:

- Forbidden values notified on previous version are now removed: 00h 00h 00h 00h, 80h 00h 00h 00h, 7Fh FFh FFh FFh and FFh FFh FFh FFh for CSC0, CSC1 and CSC2.
- The 'Rapid Communication Mode' described in the Technical Specifications v1.0 is no more available. It has been replaced by a Switch Speed command described in chapter 6.

Note: gemalto does not ensure this compatbility if cards are used under conditions that are not compliant with ISO standards or as defined in chapters 7 & 8.

Clarista GCM V2 provides some improvements compared to Clarista GCM V1, notified here-after:

- Increase the communication speed to an equivalent of PPS 94h or PPS 95h (115 000 bauds) in issuer and user mode.
- Read or Write several words of 4 bytes in one command.
- Back-up of sensitive data is strengthened.
- Processing performance of the chip is increased with a positive impact on the transaction time.

Clarista GemClub-*Memo* has a memory of two kilobits and offers features such as:

- Easier implementation: the cards use the T=0 protocol that provides many advantages:
  - ⇨ 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) allows the terminal to recognize the card
  - ⇨ It uses APDU commands
- Security (three Card Secret Codes, Access Conditions Area, Card Transaction Counter, Balance Area, specific back-up of sensitive area)

Clarista GemClub-*Memo* is compatible with the PC/SC standard.

Clarista 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

2

Operating Modes

Clarista GemClub-*Memo* cards can be delivered in 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, "Clarista GemClub-*Memo* Card Mapping".

3

Clarista GemClub-*Memo* Card Mapping

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

The structure of the Clarista GemClub-*Memo* memory is shown in the *Clarista GemClub-Memo Card Mapping* in the page here-after:

Address (Word)	Area	
00h	Manufacturer Area	
01h-04h	Issuer Area 31 | 30	
05h	31 Access 24 Conditions Area	23 Protected Area 00
06h	Card Secret Code 0	
07h	CSC 0 Ratification Counter	
08h-0Ah	CTC 1 CTC 1 Backup	
0Bh-0Fh	Balance 1 Balance 1 Backup	
10h-1Fh	User Area 1	
20h-22h	CTC 2 CTC 2 Backup	
23h-27h	Balance 2 Balance 2 Backup	
28h-37h	User Area 2	
38h	Card Secret Code 1	
39h	CSC 1 Ratification Counter	
3Ah	Card Secret Code 2	
3Bh	CSC 2 Ratification Counter	
3Ch-3Fh	Protected Area	

Figure 1 - Clarista 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.

Secret code size is 32 bits (four bytes). For sample cards, CSC 0 value is AAh AAh AAh AAh.

Warning: restriction for Clarista GemClub-Memo V1 (based on chip M37002B) only.

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

This restriction is not valid on Clarista GemClub-*Memo* V2 (based on the chip Theseus ® Titanium 40).

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 (CTC)

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

Table 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)
- 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

Table 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 (CSC 1 and CSC 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.

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.

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

Warning: restriction for Clarista GemClub-Memo V1 (based on chip M37002B) only.

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

This restriction is not valid on Clarista GemClub-*Memo* V2 (based on the chip Theseus ® Titanium 40).

CSC 1 and CSC 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 Mode		User Mode	
	Read	Update	Read	Update
Manufacturer	Free	CSC0	Free	Never
Issuer	Free	CSC0	Free	Never
AAC + Protected	Free	CSC0	Free	CSC0
Card Secret Code 0	CSC0	CSC0	Never	CSC0
Card Ratification Counter 0	Free	Automatic	Free	Automatic
Card Transaction Counter 1	Free	CSC0	Free (Rb1=0) CSC1 (Rb1=1)	Automatic
BAL1	Free	CSC0	Free (Rb1=0) CSC1 (Rb1=1)	CSC1 (Ub1=0) Never (Ub1=1)
USER 1	Free	CSC0	Free (Ru1=0) CSC1 (Ru1=1)	CSC1 (Uu1=0) Never (Uu1=1)
Card Transaction Counter 2	Free	CSC0	Free (Rb2=0) CSC2 (Rb2=1)	Automatic
BAL2	Free	CSC0	Free (Rb2=0) CSC2 (Rb2=1)	CSC2 (Ub2=0) Never (Ub2=1)
USER 2	Free	CSC0	Free (Ru2=0) CSC2 (Ru2=1)	CSC2 (Uu2=0) Never (Uu2=1)
Card Secret Code 1	CSC1	CSC0	Never	CSC1
Card Ratification Counter 1	Free	Automatic	Free	Automatic
Card Secret Code 2	CSC2	CSC0	Never	CSC2
Card Ratification Counter 2	Free	Automatic	Free	Automatic
Protected	Free	CSC0	Free	CSC0

Table 4 - Area Access Conditions

4

Commands

Clarista GemClub-Memo only uses three applicative commands:

- Read
- Update
- Verify

These commands are described in this chapter.

READ Command

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	Length of the data to read: 04h or multiple of 04h

Parameters

P2: Address of the word to be read or to start the read.

Le: Value is variable, depending on area to **Read** and P2 value, Le can take the value 04h or multiple of 04h (08h, 0Ch, 10h, …), as described in the tables 5 and 6.

Warning: Le parameter value is fixed to '04h' only on Clarista GCM V1 (with the chip M37002B).

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

Response

Data	SW1, SW2
Word1 (D0, D1, D2, D3) if Le=04h Word1, Word2 if Le=08h, … => See tables 5 and 6.	90h 00h

Where:

Data: Is the content of the word(s) read.

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

SW1	SW2	Description / ALIAS
65h	81h	Unknown mode / PB_MEM
67h	00h	Invalid length of expected data / PB_LONG as described in Tables n° 8 & 9.
69h	82h	Security not satisfied / PB_SECUR
6Bh	00h	Invalid P2 parameter / PB_PARAM
6Dh	00h	Invalid instruction byte (INS) / PB_INS
90h	00h	Command successfully executed / CODE_OK

Area		**P2 (hexadecimal)**		**Le: allowed values (hexadecimal)**	**Number of words returned by Read command**
Manufacturer		00		04	1
Issuer		01 02 03 04		04, 08, 0C, 10 04, 08, 0C 04, 08 04	1, 2, 3, 4 1, 2, 3 1, 2 1
AAC		05		04	1
CSC0 (1)		06		04	1
CL0		07		04	1
CTC1	**CTC2**	08 09 0A	20 21 22	04, 08, 0C 04, 08 04	1, 2, 3 1, 2 1
BAL1	**BAL2**	0B 0C 0D 0E 0F	23 24 25 26 27	04, 08, 0C, 10, 14 04, 08, 0C, 10 04, 08, 0C 04, 08 04	1, 2, 3, 4, 5 1, 2, 3, 4 1, 2, 3 1, 2 1
User 1	**User 2**	10 11 12 . . . 1D 1E 1F	28 29 2A . . . 35 36 37	04, 08, 0C, val-1 + 04h, .., 40h 04, 08, 0C, … 3Ch 04, 08, 0C, … 38h . . . 04, 08, 0C 04, 08 04	1, 2, 3, …, 16 1, 2, 3, …, 15 1, 2, 3, …, 14 . . . 1, 2, 3 1, 2 1
CSC1 (1)	**CSC2** (1)	38	3A	04	1
CL1 (1)	**CL2** (1)	39	3B	04	1
Protected		3C 3D 3E 3F		04, 08, 0C, 10 04, 08, 0C 04, 08 04	1, 2, 3, 4 1, 2, 3 1, 2 1

(1): depending on access conditions defined in table 4 for issuer mode.

Table 5 - 'Le' possible values on Read Command in Issuer Mode

Area		**P2: value (hexadecimal)**		**Le: Value (hexadecimal)**	**Number of words returned**
Manufacturer		00		04	1
Issuer		01 02 03 04		04, 08, 0C, 10 04, 08, 0C 04, 08 04	1, 2, 3, 4 1, 2, 3 1, 2 1
AAC		05		04	1
CL0		07		04	1
CTC1 (2)	**CTC2** (2)	08 09 0A	20 21 22	04, 08, 0C 04, 08 04	1, 2, 3 1, 2 1
BAL1 (2)	**BAL2** (2)	0B 0C 0D 0E 0F	23 24 25 26 27	04, 08, 0C, 10, 14 04, 08, 0C, 10 04, 08, 0C 04, 08 04	1, 2, 3, 4, 5 1, 2, 3, 4 1, 2, 3 1, 2 1
User 1 (2)	**User 2** (2)	10 11 12 . . . 1D 1E 1F	28 29 2A . . . 35 36 37	04, 08, 0C, val-1 + 04h, **..**, 40h 04, 08, 0C, … 3Ch 04, 08, 0C, … 38h . . . 04, 08, 0C 04, 08 04	1, 2, 3, …, 16 1, 2, 3, …, 15 1, 2, 3, …, 14 . . . 1, 2, 3 1, 2 1
CL1 (2)	**CL2** (2)	39	3B	04	1
Protected		3C 3D 3E 3F		04, 08, 0C, 10 04, 08, 0C 04, 08 04	1, 2, 3, 4 1, 2, 3 1, 2 1

(2): depending on access conditions defined in table 4 for user mode.

Table 6 - 'Le' possible values on Read Command in User Mode

UPDATE Command

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

Note about Balance Update:

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.

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	Lc	Data
80h	DEh	00h	Ad	XXh	Data

Parameters

P2: Address of the word to be updated or to start the Update.

Lc: Depending of GemClub Memo area and P2 value, Lc can take the value 04h or multiple of 04h (08h, 0Ch, 10h), as described in the tables 7 and 8.

Data: Is the value of the data to be written to the card, Least Significant Byte (D0) first, Most Significant Byte (D3) last.

Warning: Le parameter value is fixed to '04h' only on Clarista GCM V1 (with the chip M37002B).

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

Response

SW1, SW2

Where:

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

SW1	SW2	Description / ALIAS
65h	81h	Memory error: unknown flag, unknown mode or CTC reached maximum allowed value / PB_MEM
67h	00h	Invalid Lc value / PB_LONG (see tables 7 and 8).
69h	82h	Security not satisfied, words in balance updated in wrong order or attempt to update flag word / PB_SECUR
6Bh	00h	Invalid P2 parameter / PB_PARAM
6Dh	00h	Invalid instruction byte (INS) / PB_INS
90h	00h	Command successfully executed / CODE_OK

Area		**P2 (hexadecimal)**		**Lc: allowed values (hexadecimal)**	**Number of words to be updated** (1)
Manufacturer		00		04	1
Issuer		01 02 03 04		04, 08, 0C, 10 04, 08, 0C 04, 08 04	1, 2, 3, 4 1, 2, 3 1, 2, 1
AAC		05		04	1
CSC0		06		04	1
CTC1	**CTC2**	08 09 0A	20 21 22	04, 08, 0C 04, 08 04	1, 2, 3 1, 2, 1
BAL1	**BAL2**	0B 0C 0D 0E 0F	23 24 25 26 27	04, 08, 0C, 10, 14 04, 08, 0C, 10 04, 08, 0C 04, 08 04	1, 2, 3, 4, 5 1, 2, 3, 4 1, 2, 3 1, 2 1
User 1	**User 2**	10 11 12 . . . 1D 1E 1F	28 29 2A . . . 35 36 37	04, 08, 0C, val-1 + 04h, .., 40h 04, 08, 0C, … 3Ch 04, 08, 0C, … 38h . . . 04, 08, 0C 04, 08 04	1, 2, 3, … ,16 1, 2, 3, … ,15 1, 2, 3, … ,14 . . . 1, 2, 3 1, 2 1
CSC1	**CSC2**	38	3A	04	1
Protected		3C 3D 3E 3F		04, 08, 0C, 10 04, 08, 0C 04, 08 04	1, 2, 3, 4 1, 2, 3 1, 2, 1

(1): depending on access conditions defined in table 4 for issuer mode.

Table 7 - ‘Le’ possible values on Update Command in Issuer Mode

<table>
<tr><th colspan="2">Area</th><th colspan="2">P2 (hexadecimal)</th><th>Lc: allowed values (hexadecimal)</th><th>Number of words to be updated [(1)]</th></tr>
<tr><td colspan="2">AAC</td><td colspan="2">05</td><td>04</td><td>1</td></tr>
<tr><td colspan="2">CSC0</td><td colspan="2">06</td><td>04</td><td>1</td></tr>
<tr><td>BAL1</td><td>BAL2</td><td>0C
0D
0E
0F</td><td>24
25
26
27</td><td>04
04
04
04</td><td>1
1
1
1</td></tr>
<tr><td>User 1</td><td>User 2</td><td>10
11
12
.
.
.
1D
1E
1F</td><td>28
29
2A
.
.
.
35
36
37</td><td>04, 08, 0C, val-1 + 04h, .., 40h
04, 08, 0C, … 3Ch
04, 08, 0C, … 38h
.
.
.
04, 08, 0C
04, 08
04</td><td>1, 2, 3, … ,16
1, 2, 3, … ,15
1, 2, 3, … ,14
.
.
.
1, 2, 3
1, 2
1</td></tr>
<tr><td>CSC1</td><td>CSC2</td><td>38</td><td>3A</td><td>04</td><td>1</td></tr>
<tr><td colspan="2">Protected</td><td colspan="2">3C
3D
3E
3F</td><td>04, 08, 0C, 10
04, 08, 0C
04, 08
04</td><td>1, 2, 3, 4
1, 2, 3
1, 2,
1</td></tr>
</table>

[(1)]: depending on access conditions defined in table 4 for user mode.

Table 8 - ‘Le’ possible values on Update Command in User Mode

VERIFY Command

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

Note: This command can also be used in issuer mode to emulate the card's behavior in user mode. After a Reset, the card returns to issuer mode.

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	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. (CSC0 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 content is 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 in the page here-after:

SW1	SW2	Description
63h	00h	Invalid Secret Code
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.

Warning: restriction for Clarista GemClub-Memo V1 only (based on chip M37002B).

⇨ 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.

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

This restriction is removed on Clarista GemClub-*Memo* V2 (based on the chip Theseus ® Titanium 40).

5

Anti-Withdrawal Mechanism

This mechanism is not available in issuer mode. In user mode, Clarista 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 are, 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 "*Clarista GemClub - Memo Card Mapping*" chapter.

During normal processing, (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 (assuming that a typical transaction implies the Update 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.

6

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.

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.

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 9 - ATR Structure

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.

Nevertheless, to ensure full backwards compatibility between Clarista GCM V1 and V2, T2 value is equal to 01h on Clarista GCM V2 (as for GCM V1).

A specific 'Get Chip ID info' command allows identifying the Clarista GCM V2, based on TT40 chip, as described hereafter.

Command 'Get Chip ID Info'

Format

CLA	INS	P1	P2	Le
80h	C0h	00h	00H	08h

Response

Data	SW1, SW2
8 bytes	90h 00h

Where:

Data: contains the 8 bytes unique chip ID / chip serial number

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

SW1	SW2	Description
6Dh	00h	Invalid instruction byte (INS)
6Ah	86h	Invalid P1/P2 parameter
67h	00h	Invalid length of expected data
90h	00h	Command successfully executed.

Note: This command is not implemented on GCM V1 (based on M37002B chip).

APDU / TPDU exchanges

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: Variable.

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, a parity bit and 2 stops bits.

A falling I/O edge indicates that a character is to be received.

On Clarista GCM V1 (with the chip M37002B), 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.

On Clarista GCM V2 (with the chip TT40), each bit is samples by the UART and 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 for TA1=11h). After the byte has been completely received, the card either continues to send the next byte or the card switches to reception mode to receive a byte.

The card sends the byte with the following minimum timing:

- Clarista GCM V1: **13 etu** after the falling edge of the last start bit if the card was previously in sending mode
- Clarista GCM V2: **12 etu** after the falling edge of the last start bit if the card was previously in sending mode
- Clarista GCM V1 & V2: 16 etu after the falling edge of the last start bit if the card was previously in receiving mode (conforming to the EMV standards).

With the timings above, the card is ISO-7816 compliant and requires that the reader be also ISO-7816 in order to establish error free communication.

As such, reader must follow the timings below to have error free communication with the GemClub Memo card:

During Reader Reception

- Reader must be ready to receive a byte before 12 etu if reader was previously in receiving mode.
- Reader must be ready to receive a byte before 16 etu if reader was previously in emission mode.

During Reader transmission

- If following ISO-7816 standard, reader must transmit a byte with a minimum timing of 12 etu between falling edge of previous byte.
- If following EMV standard, reader must transmit a byte with a minimum timing of 12 etu between falling edge of previous byte if previous byte was a byte transmission by the reader. However, if previous byte was a byte transmission by the card, reader must transmit the byte with a minimum of 16 etu between falling edge of previous byte.

Communication Speed

Switch Speed Command: for Clarista GCMemo V2 only

A specific 'Switch Speed Command' **is only supported by Clarista GemClub-*Memo* V2** to increase communication speed between card and reader. It allows emulating a PPS exchange of 94h and 95h.

This command is available both in Issuer and User mode.

Format

CLA	INS	P1	P2	Li/Le
80h	14h	TA1h	00h	00h

TA1 values are: 11h, 94h or 95h.

Response

SW1, SW2

Where:

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

SW1	SW2	Description
6Dh	00h	Invalid instruction byte (INS)
6Ah	86h	Invalid P2 parameter
67h	00h	Invalid length of expected data
6Bh	00h	TA1 value in P1 is not supported
90h	00h	Command successfully executed.

Rapid Communication Mode: for Clarista GCM V1 only

A specific rapid communication mode exists on Clarista GemClub-Memo V1 (based on M37002B chip), 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 10 - Rapid Communication Mode – Breakdown of characters

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 bytes. The possible values are shown in the table here-after:

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.

7

Electrical Characteristics

This chapter describes the electrical characteristics of Clarista GemClub-Memo product based on Theseus® Titanium 40 chip.

Common Specifications

Absolute Maximum Ratings	**Min.**	**Typical**	**Max.**	**Unit**
External Power Supply (VCC EXT to GND)	-0.3		+6.0	V
All Pins to GND	-0.3			V
All Pins to VCC			+0.3	V
Storage Temperature, at R.H.<60%	-15		+30	°C
Recommended Usage Ranges	**Min.**	**Typical**	**Max.**	**Unit**
External Power Supply (VCC EXT)	2.7	3.0, 5.0	5.5	V
Operating Temperature	-20	+25	+85	°C

Table 11 - TT40 Common Specifications

Note: Operation or storage of the product beyond Absolute Maximum Ratings may damage the product and voids any product warrantees.

DC Characteristics

Parameter	Symbol	Conditions*	Min.	Max.	Unit
High Output Voltage	VIH	I/O@3V&5V IIHmax =+ 20uA	0.7 x VCC	Vcc+0.3	V
	VIL	I/O@3V IIL = +1mA	-0.3	0.2 VCC	
		I/O@5V IIL = + 1mA	-0.3	0.8	
	VOH	Clock @ 3V IOH max = +20 µA	0.7 x VCC	Vcc	
		Clock @ 5V IOH max = +20 µA	0.7 x VCC		
		RST@ 3V IOH max = +200 µA	0.8 x VCC		
		RST@ 5V IOH max = +20 µA	VCC -0.7		
		I/O@ 3V IOHmax = +1mA	0.7 x VCC		
		I/O@ 5V IOHmax = +1mA	0.7 x VCC		
Low Output Voltage	VOL	Clock @ 3V IOL max = -200 µA	0	0.2 VCC	V
		Clock @ 5V IOL max = -200 µA	0	0.5	
		RST@ 3V IOL max = -200 µA	0	0.2 VCC	
		RST@ 5V IOL max = -200 µA	0	0.6	
		I/O@ 3V IOLmax = -1mA	0	0.4	
		I/O@ 5V IOLmax = -1mA	0	0.4	
Rise/Fall Time	tR and tF	Clk Cin = Cout = 30pF		50	nS
		Rst Cin = Cout = 30pF		400	uS
		O Cin = Cout = 30pF		1	
Supply Current Active	Icc	2.7 to 3.3V, ISO_CLK 4MHz, 30MHz Internal, Vih = VCC +/- 0.3V, Vil = VSS +/- 0.3V		6	mA
Supply Current Active	Icc	4.5 to 5.5V, ISO_CLK 4MHz, 60MHz Internal Vih = VCC +/- 0.3V, Vil = VSS +/- 0.3V		10	mA
Supply Current Idle	Icci	2.7 to 5.5V, ISO_CLK 1MHz, 25°C Vih = VCC +/- 0.3V, Vil = VSS +/- 0.3V		200	uA
Stop Clock Mode	Icci	1MHz, 25°C <100uA at 3V and <200uA at 5V		100 200	uA

*The programmable pull-up resistor is in the default OFF condition.

Table 12 - TT40 DC Characteristics

8

Physical Characteristics

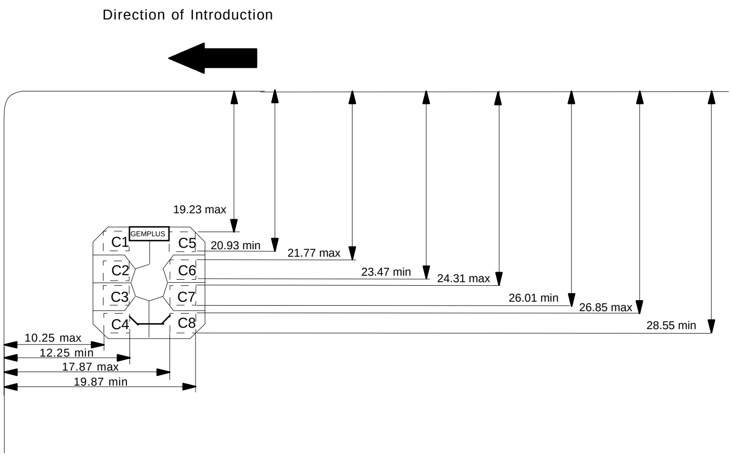
The Clarista GemClub-Memo card's physical characteristics comply with the ISO 7816-1 specification.

The card dimensions are as follows:

- Length / Width = 85.6 mm
- Width / Height = 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:



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.

Figure 2 - Card Contact Positions and Assignments

Operating Temperatures

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 50ºC
ABS	-20ºC to 70ºC
PVC HT	-20ºC to 70ºC
PET	-20ºC to 85ºC

Card Reliability

GemClub-Memo card reliability data is as follows:

	Test	Standard Ref.	Conditions	Test Success Criteria
1	Card dimensions	ISO 7810	85.47<length /width <85.72mm 53.92<width / Height <54.03mm 0.76<thickness<0.84mm	Nominal functionality
2	Contact location	ISO 7816-2	See contact chapter	Nominal functionality
3	Surface profile of contact	ISO 7816-1	-100 µm; +100 µm	Nominal functionality
4	Dynamic bending torsional stress	ISO 7810	1 ISO cycle = 500 bends (width) (250 front + 250 back) 500 bends (length) (250 front +250 back) 500 torsions	Nominal functionality Visual
5	Salt atmosphere	ISO 7810 ISO 9227	24 h at 35ºC, 45% RH, 5% NaCl	Nominal functionality
6	Temperature & Humitidy	CQM 1.9D § durability	168 h at 85ºC / 85 %RH	Nominal functionality
9	Card stability with temperature	Internal	168h at 70ºC (dry Tº) (depending on the card body - see *Operating Temperatures*)	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	Nominal functionality
13	ESD protection	MIL STD -883 Method 3015-6	Class A : 4Kv	Nominal functionality
14	EEPROM ENDURANCE		100,000 write / erase cycles at 25°C	Nominal functionality

Table 13 - Card Reliability Data

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

Terminology

Abbreviations

APDU	Application Protocol Data Unit
ATR	Answer To Reset
CLK	Clock signal
CSC	Card Secret Code
CTC	Card Transaction Counter
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
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
GCM or GCMemo	GemClub-*Memo*