

**Samsung S3CC9P9 v1.3  
Technical Manual  
Version 1.2 January  
2007**



# CONTENTS

<b>1. Overview.....</b>	<b>3</b>
1.1. Revision History.....	3
1.2. References .....	3
1.3. Trademarks.....	3
<b>2. Basic specification.....</b>	<b>3</b>
2.1. Java Card Features .....	3
2.2. Visa GlobalPlatform Features.....	3
2.3. Security Features.....	4
2.3.1. Cipher.....	4
2.3.2. Signature.....	4
2.3.3. Message Digest .....	4
2.3.4. Key Builder .....	4
<b>3. Communications .....</b>	<b>4</b>
3.1. Supported protocols.....	4
3.2. Supported speeds.....	4
<b>4. Hardware Specification.....</b>	<b>5</b>
<b>5. Applets.....</b>	<b>5</b>
5.1. Issuer Security Domain.....	5
5.1.1. Supported Commands.....	5
5.1.2. Example of Secure Channel Initiation.....	6
5.2. Supplementary Security Domain .....	6
5.3. Certification Applet.....	6
5.3.1. Examples of Certificate Applet installation.....	6
5.3.2. AID Information.....	6
<b>6. Notes on Implementation.....</b>	<b>6</b>
6.1. CHANNEL.....	6
6.1.1. MANAGE CHANNEL Command .....	6
6.2. Proprietary Commands.....	7
6.2.1. GET CARD-PROFILE DATA Command .....	7
6.2.2. GET CARD-INFO DATA Command.....	7

# 1. Overview

## 1.1. Revision History

Version 1.0 Initial draft

Version 1.0.1 "6.2 Proprietary Commands" added

Version 1.1 Release draft

Version 1.2 5.1, 5.1.2 updated.

## 1.2. References

[1] GlobalPlatform Card Specification Version 2.1.1 March 2003

<http://www.globalplatform.org>

[2] Visa GlobalPlatform 2.1.1 Card Implementation Requirements Version 1.0 May 2003

[3] EMV Integrated Circuit Card Specifications for Payment System 4.1, May 2004

<http://www.emvco.com>

[4] ISO/IEC 7816, Information technology - Identification cards – Integrated circuits(s) cards with contacts – Part 4 : Interindustry commands for interchange, September 1995

## 1.3. Trademarks

Sun, Sun Microsystems, Java, Java Card and Java Card S are trademarks of Sun Microsystems, Inc.

# 2. Basic specification

Card is a "Java Card" implementation conforming to "*Visa GlobalPlatform 2.1.1 Card Implementation Requirement*" and "*Java Card 2.2.1*".

**Card** is implemented on Samsung S3CC9P9 smart card controller which has 160 Kbytes ROM and 32 Kbytes EEPROM. It has VSDC 2.5.1 and PSE 2.2 as its ROM applets.

## 2.1. Java Card Features

**Card** supports all features of "*Java Card 2.2.1*" including RMI, Multiple Logical Channels and Garbage Collection.

## 2.2. Visa GlobalPlatform Features

**Card** conforms to **Configuration 3** implementation specified in "*Visa GlobalPlatform 2.1.1 Card Implementation Requirement*".

Following features are supported.

- Public key DAP Verification
- Mandated DAP Verification
- SCP02 with implementation option '15'
- Global PIN via CVM interface
- Deprecated API of Open Platform 2.0.1
- EMV Level 1 requirements
- Delegated Management
- Optional feature. The availability of this optional feature is at the discretion of the issuer.

## 2.3. Security Features

### 2.3.1. Cipher

Following algorithms are supported.

- DES\_CBC : NOPAD, ISO9797\_M1, ISO9797\_M2
- DES\_ECB : NOPAD, ISO9797\_M1, ISO9797\_M2
- RSA : NOPAD, PKCS1 (maximum length of 1024 bits)
- RSA\_CRT : NOPAD, PKCS1 (maximum length of 2048 bits)
- SEED\_CBC : NOPAD, NRPAD (domestically used in South Korea)
- SEED\_ECB : NOPAD, NRPAD (domestically used in South Korea)

### 2.3.2. Signature

MODE\_SIGN and MODE\_VERIFY of following algorithms are supported.

- DES\_MAC8 : NOPAD, ISO9797\_1\_M2\_ALG3, ISO9797\_M1, ISO9797\_M2
- RSA\_SHA : PKCS1, ISO9796

### 2.3.3. Message Digest

Following algorithms are supported.

- MD5
- SHA-1

### 2.3.4. Key Builder

Following key types are supported.

- TYPE\_DES
- TYPE\_DES\_TRANSIENT\_DESELECT
- TYPE\_DES\_TRANSIENT\_RESET
- TYPE\_RSA\_PUBLIC (with maximum key length of 1024 bits)
- TYPE\_RSA\_PRIVATE (with maximum prime length of 1024 bits)
- TYPE\_RSA\_CRT\_PRIVATE (with maximum prime length of 1024 bits)

Keys with following key length are supported.

- LENGTH\_DES
- LENGTH\_DES3\_2KEY
- RSA key length that is a multiple of 32 bits between 512 bits and 1024 bits
- RSA CRT prime length that is a multiple of 16 bits between 256 bits and 512 bits. Also supports prime length of 1024 bits.

## 3. Communications

### 3.1. Supported protocols

- ISO7816 T=0 direct convention [default]
- ISO7816 T=1 direct convention

### 3.2. Supported speeds

At the default clock rate of 3.57 MHz, the following communication speeds can be attained:

- 9600 bit/sec [default]
- 19200 bit/sec
- 38400 bit/sec
- 115200 bit/sec

## 4. Hardware Specification

Samsung Electronics S3CC9P9  
CPU 16-bit Calm 16 series  
ROM 160 Kbytes  
EEPROM 32 Kbytes  
RAM 6 Kbytes  
Operating Temperature -25°C ~ 85°C  
Operating Voltage 2.7 V ~ 5.5 V

## 5. Applets

**Card** has the Issuer Security Domain, Supplementary Security Domain and six ROM applets (Certification Applet, eBook, ATM Applet, K-Cash, PSE and VSDC). Capabilities of the Issuer Security Domain and these ROM applets are described in this section.

- Issuer Security Domain
- Supplementary Security Domain
- Certification Applet

### 5.1. Issuer Security Domain

Issuer Security Domain (hereinafter referred to as "ISD") is an applet that is used to manage a card. The ISD is implemented based on the *GlobalPlatform Card specification 2.1.1* and the *Visa GlobalPlatform 2.1.1 Card Implementation Requirements*.

The AID of the ISD is "0xA0 0x00 0x00 0x00 0x03 0x00 0x00 0x00" and the value of initial key is '0x40 0x41 0x42 0x43 0x44 0x45 0x46 0x47 0x48 0x49 0x4A 0x4B 0x4C 0x4D 0x4E 0x4F' and the default key version number is '0x00'.

#### 5.1.1. Supported Commands

Commands supported by the ISD of **Card** are as follows.

- DELETE
- INSTALL
- LOAD
- INITIALIZE UPDATE
- EXTERNAL AUTHENTICATE
- PUT KEY
- STORE DATA
- GET DATA
- GET STATUS
- SET STATUS

##### 5.1.1.1. DELETE

All requirements specified in *Visa GlobalPlatform 2.1.1 Card Implementation Requirements version 1.0* are implemented.

**Card** does not support deletion of key. If TLV tag in command message is not '0x4F', indicating AID, card returns 0x6A80.

##### 5.1.1.2. INSTALL

All requirements specified in *Visa GlobalPlatform 2.1.1 Card Implementation Requirements version 1.0* are implemented.

##### 5.1.1.3. LOAD

All requirements specified in *Visa GlobalPlatform 2.1.1 Card Implementation Requirements version 1.0* are implemented.

#### **5.1.1.4. INITIALIZE UPDATE**

All requirements specified in *Visa GlobalPlatform 2.1.1 Card Implementation Requirements version 1.0* are implemented.

The ISD supports Secure Channel Protocol '02' and specifically implementation option '15'.

#### **5.1.1.5. EXTERNAL AUTHENTICATE**

All requirements specified in *Visa GlobalPlatform 2.1.1 Card Implementation Requirements version 1.0* are implemented.

The ISD supports Secure Channel Protocol '02' and specifically implementation option '15'.

#### **5.1.1.6. PUT KEY**

All requirements specified in *Visa GlobalPlatform 2.1.1 Card Implementation Requirements version 1.0* are implemented.

#### **5.1.1.7. STORE DATA**

All requirements specified in *Visa GlobalPlatform 2.1.1 Card Implementation Requirements version 1.0* are implemented.

#### **5.1.1.8. GET DATA**

All requirements specified in *Visa GlobalPlatform 2.1.1 Card Implementation Requirements version 1.0* are implemented.

#### **5.1.1.9. GET STATUS**

This command is used by the ISD only to retrieve Executable Load File, Executable Module, ISD and Application Life Cycle data.

All requirements specified in *Visa GlobalPlatform 2.1.1 Card Implementation Requirements version 1.0* are implemented.

**Card** does not support retrieval of data relating to Executable Load Files and their Executable Modules. Therefore, for this command with P1 value equal to '0x10', card returns 0x6A81.

And, **Card** can respond to a command with 256-byte-length of data maximally.

#### **5.1.1.10. SET STATUS**

This command is used by the ISD only to change the Life Cycle of the card and to lock or unlock an Application.

All requirements specified in *Visa GlobalPlatform 2.1.1 Card Implementation Requirements version 1.0* are implemented.

#### **5.1.2. Example of Secure Channel Initiation**

Following is an example of secure channel initiation.

Send 80 50 00 00 08

11 22 33 44 55 66 77 88 (Host challenge)

Response 61 1C (Status Word)

Send 00 C0 00 00 1C

Response 00 00 61 72 01 27 23 90 99 45 (Key diversification data)

FF 02 (Key information)

00 00 (Sequence Counter)

3D 02 9C 31 C7 89 (Card challenge)

10 91 59 B6 9D D1 E8 F7 (Card cryptogram)

90 00 (Status Word)

Send 84 82 00 00 10

6C AB F3 4A CF AA 6C CB F3 46 3E BD 51 AE 8A 55 (Host

cryptogram and MAC)  
Response 90 00 (Status Word)

## 5.2. Supplementary Security Domain

Supplementary Security Domain (hereinafter referred to as “SSD”) is an applet that is used to manage a card but has limited capability comparing to ISD. The SSD is implemented based on the *GlobalPlatform Card specification 2.1.1* and the *Visa GlobalPlatform 2.1.1 Card Implementation Requirements version 1.0*.

The package ID of the SSD is “0xA0 0x00 0x00 0x00 0x03 0x53 0x50” and needs to be installed in order to use SSD.

SSD supports following commands.

- INITIALIZED UPDATE (Section 5.1.1.4)
- EXTERNAL AUTHENTICATION (Section 5.1.1.5)
- PUT KEY (Section 5.1.1.6)
- STORE DATA (Section 5.1.1.7)
- GET DATA (Section 5.1.1.8)

For further information about commands that SSD supports, refer to related sections mentioned above. For any options of commands.

## 6. Notes on Implementation

Following section briefly describes notes on **Card** implementation.

### 6.1. CHANNEL

**Card** has two logical channels. One is used for basic logical channel and the other one is used for supplementary logical channels.

#### 6.1.1. MANAGE CHANNEL Command

The MANAGE CHANNEL command opens and closes logical channels. Further information of MANAGE CHANNEL command is described in ISO/EIC 7816-4<sup>[4]</sup>.

##### 6.1.1.1. Secure Messaging

According to ISO/EIC 7816-4<sup>[4]</sup>, four Secure Messaging (hereinafter referred to as “SM”) options exists and are indicated in lower nibble of CLA of APDU command.

**Card** only supports ‘No SM or no SM indication’ for MANAGE CHANNEL command. In other words, lower nibble of CLA of MANAGE CHANNEL command should be ‘0’.

If any other value is used for lower nibble of CLA of MANAGE CHANNEL command, **Card** will return status word indicating error or warning.

##### 6.1.1.2. Behavior of Card

Upon receiving MANAGE CHANNEL command, **Card** first checks if command requests SM by analyzing lower nibble of CLA. If MANAGE CHANNEL command requests SM, **Card** returns 0x6882 indicating “secure messaging not supported”<sup>[4]</sup>. For example, **Card** returns 0x6882 for MANAGE CHANNEL command ‘04 70 P1 P2 00’, ‘08 70 P1 P2 00’ and ‘0C 70 P1 P2 00’ with P1, P2 be combination of any value between 0x00 to 0xFF.

After checking CLA for SM, **Card** opens or closes logical channel

according to the command received.

## 6.2. Proprietary Commands

Issuer Security Domain of **Card** supports two proprietary commands. These are simple commands and supported for specific requirements of several domestic card issuers and application providers in South Korea.

### 6.2.1. GET CARD-PROFILE DATA Command

#### 6.2.1.1. Definition and Requirements

This command returns card-profile data. This command may only be issued within a Secure Channel Session and the level of security for the command is dependent on the security level defined in the EXTERNAL AUTHENTICATE command.

#### 6.2.1.2. Command Format

**CLA INS P1 P2 Lc**

D0 02 XX XX 00

(Any value between 0x00 and 0xFF can be used for 'XX'.)

#### 6.2.1.3. Response Format

Response data format of GET CARD-PROFILE DATA command is described in the following table.

##### Description Length Value

Card OS Version indicating Kona 20 2 0200

The size of available RAM segment 2 Variable

The size of available EEPROM segment 2 Variable

The size of transaction buffer 2 0EFF

The number of logical channels 2 0002

Constant value 4 00010000

### 6.2.2. GET CARD-INFO DATA Command

#### 6.2.2.1. Definition and Requirements

This command returns card-info data. This command may only be issued within a Secure Channel Session and the level of security for the command is dependent on the security level defined in the EXTERNAL AUTHENTICATE command.

#### 6.2.2.2. Command Format

**CLA INS P1 P2 Lc**

D0 06 00 00 00

#### 6.2.2.3. Response Format

Response data format of GET CARD-INFO DATA command is described in the following table. More than one set of data may be returned.

##### Description Length Value

Length of AID 1 05 to 10

AID 5~16 Variable

Life Cycle Status 1 Refer to GP spec.[1]

Privilege 1 Refer to GP spec.[1]

Constants 2 0000