# SC PRODUCT FAMILY

## TECHNICAL OVERVIEW

VeriFone®

**Table of Contents**

## 1. Introduction

The smart card (SC) family of VeriFone products is a series of hand-held smart card reader/writers that supports multiple options for secure PINpad and smart card applications.

The Family consists of the SC 450, SC 455, SC 550 and SC 552 products. Each of these products offers a different range of capabilities and options, yet all share the same basic design architecture. The family therefore meets current market requirements and configuration options while anticipating a planned growth path.

This document describes each product in detail and gives an overview of each of the major physical components.

## 2. Product Descriptions

*SC 450*

The SC 450 is a hand-held PINpad with a single smart card reader/writer. The reader/writer supports a wide range of smart cards and its design offers significant flexibility and control.

The SC 450 has a high level of physical security and supports various options for logical security, encryption and encryption key management. The security functions are performed by the internal Security Access Module (SAM). The SAM uses a custom-developed security chip to perform data encryption and secure storage. The SAM can execute individual key management schemes such as Master/Session Key. In applications where smart card-only support is required and encryption is not necessary, the SC 450 may be manufactured without the security chip.

*SC 455*

The SC 455 has the same look, size and functions as the SC 450; in addition, it supports options for a graphic display and a very high level of physical security. The SC 455 can support multiple key management schemes simultaneously, including Master/Session key and Derived Unique Key (DUKPT). Like the SC 450, the SC 455 may be supplied without the security chip.

*SC 550*

The SC 550 is also a hand-held PINpad with integrated smart card reader/writer, but with an additional feature: an integrated dual track magnetic-stripe card reader. The SC 550 has a slightly different look than the SC 4xx products but it supports the same range of features.

*SC 552*

The SC 552 offers the same functions and options as the SC 550, but it adds a second smart card reader/writer, which can be used as a a removable encryption module or a data storage device.

## 3. Main Features

The features described in this section apply to all products within the SC family unless otherwise stated.

### *3.1 Memory*

All SC products offer two options for application and data storage memory: 32K RAM and 128K RAM. This memory is battery backed and the design enables applications to be downloaded either by direct connection or by remote connection i.e. a telephone line, using the modem of an external device such as a terminal or ECR.

### *3.2 Keypad*

All keypads are arranged in a 4x4 format with 10 numeric keys, ENTER and CLEAR keys plus 4 soft function keys.

The SC 4xx products have a 4x4 membrane keypad. The keypad is made of a strong plastic with a chemical resistant surface enabling the products to operate in a variety of retail and service locations. Each key has a raised dome profile, which gives the user a tactile response when the key is pressed. For security, the electrical connections from the keypad are integrated directly into the security module, which protects against keypad tapping.

The legends and colors of the keys may be tailored to the customer's requirements. Custom keypads take about four weeks for samples and 10 weeks for production volumes. However a number of standard keypads are available with legends in a variety of languages.

The SC 5xx products have a 4x4 rubber mat keypad with the keys covered by a hard plastic cap. The colors and legends of the SC 5xx keypads can be tailored to customer requirements.

### *3.3 Display*

The standard display is a 2-line-by-16-character LCD display. Eight custom characters can be created by the application at any time to allow non-standard characters.

The display, as well as the keypad, is directly controlled from the security module; this allows the customer to enhance overall security by restricting display access to legitimate commands and processes.

On the SC 455, SC 550 and SC 552 products, an enhanced graphic display is an option. A matrix of 120x32 dots lets the programmer choose between 4-lines-by-20-character, 2- lines-by-16-character, or 2-lines-by-seven-Chinese-character displays (or a mixture of the above).

This display also supports a variety of character languages, such as Arabic, Cyrillic, Chinese, Japanese, etc. The fonts can be selected from existing VeriFone-provided fonts, or they can be created by the programmer using a VeriFone Font Designer tool. Fonts are stored in the application area and can be field-updated at any time by an application download.

### *3.4 Processor*

All SC products use the same Motorola 68HC11 processor and application development system, which ensures software compatibility across the product range.

### *3.5 Smart Card Reader/Writer*

All SC products contain a smart card reader/ writer. Designed with maximum flexibility, reader/ writers support all cards conforming to ISO Standard 7816 parts 1, 2 and 3.

The smart card is normally inserted by the cardholder into the slot at the front edge of the product. A plastic lip at the slot's edge assists card entry.

The reader/ writers read smart cards which have either the ISO standard contact positions or the slightly higher AFNOR (French) contact positions. Some applications support both positions.

The reader/ writers support cards with the protocol T=0 and/or T=1. Some applications support both protocols.

The reader/ writers support simple memory cards, protected-memory cards and processor cards. As with the other features, a single application may support all types or a combination.

Also, the reader/ writers support program voltages from 5 to 21 volts. Some applications might support all voltage types.

The software drivers that support all these options are stored in the downloadable area of application memory; this allows new card support to be added or amended via an application download.

The highly reliable reader supports more than 100,000 card insertions/removals.

### *3.6 Second Smart Card Reader/Writer*

Only the SC552 model offers a second smart card reader/ writer. The second smart card is inserted into a reader slot on the side of the unit. The card can be removed by pressing on a button at the opposite side of the unit; alternatively, the SC552 may be configured so that a special tool is required to eject the smart card. The second reader supports full-size smart cards; however, an option is available to support GSM-size SIM modules.

This reader/ writer is included for two main purposes:

1. *To act as a removable security module.*

   If the smart card inserted into the second reader contains an encryption capability, then this card may be used to perform the cryptographic functions of the PINpad. This enables the customer to maintain their level of physical security and gain flexibility not offered by an integrated security module. The smart card can also enhance the functionality of the PINpad by adding alternative encryption algorithms such as public key, or it can be used as the transport for new or upgraded encryption keys.

2. *To act as a removable storage device.*

   The second smart card reader/ writer can store extra data, such as transactions or retailer configuration information.

   The second smart card reader/ writer supports microprocessor cards adhering to ISO standard 7816 parts 1, 2 and 3. It only supports the ISO contact positions.

### *3.7 Magnetic-Stripe Card Reader*

A magnetic-stripe card reader is supported by the SC 5xx product family. The magnetic-stripe card reader is available for either Track 1 & 2 or Track 2 & 3 reading. The reader supports all cards that comply with ISO standard 7813. Additionally, the reader is bi-directional and supports a wide range of swipe speeds.

### *3.8 Security Module*

The security module performs all security functions, encryption and storage of secret data.

The security module is a separate component and acts independently from the main application area. This enables different functions to be performed simultaneously. It also enhances the overall security of the products, because the application area cannot access the security chip, the display or the keyboard. These areas can be accessed only by issuing valid commands to the security module and supplying the appropriate data, i.e., a prompt to be displayed.

At the heart of the security module is the Philips 83C852 security chip, a specially developed microcomputer designed to perform encryption operations. The security chip has the computational and mathematical capabilities to perform standard encryption algorithms such as DES and RSA. The chip also has storage space for 32 encryption keys and other sensitive data. Depending upon product configuration, selected keys and data may be stored in EEPROM or in battery-backed RAM.

VeriFone has taken this encryption chip and programmed it via the development of a custom mask. The mask is the name given to the fixed programming code for a microcomputer chip. The VeriFone mask implements the commands necessary to do such functions as initial key loading and key management.

In addition to the mask, the chip can run custom code from its internal EEPROM and can thus be individually programmed to specific customer requirements. The EEPROM code is loaded during manufacturing and can be changed only within a controlled environment using strict security procedures.

### *3.9 Security Chip Mask*

Two versions of the security chip mask are available. Each mask supports a different set of functions, which are described in detail in the application programming manual. The basic differences are:

- Mask 08 supports DES and other related encryption; key management functions, the encryption keys and other secret data are stored within the EEPROM area of the security chip.
- Mask 25 stores keys within the battery-backed RAM of the security chip giving greater functionality such as the Derived Unique Key (DUKPT) management system.

### *3.10 Physical Protection*

Physical protection is designed into the SC product family to further secure the functions and data stored in the security chip. Sensitive areas-such as the cable between the keypad and the security module-are protected from illegal attack.

Because different systems and requirements for security exist around the world, SC products offer two levels of physical protection:

1. The High Security version has a sensor on the casing that detects if the plastic is opened. In the event of tampering, the stored application and secret data are automatically erased. The security module itself is potted in epoxy resin that protects the components from examination and attack.
2. In addition to the security features of the High Security version, the Very High Security version offers the additional protection of automatically erasing stored secret data if the security module is subject to attacks, such as chemical attack, sawing, drilling, freezing, etc.

The security of the SC product family has been evaluated by the TNO and GEI test houses, which validate security components on behalf of the EFT system of countries such as Holland and Germany. The SC products have been approved for operation in both of these countries.

### *3.11 Serial Port*

All SC products have a serial port (RS232 / V.24) for connecting to external equipment. The port acts as a data interface to any external device and also as a power source. The products accept input power from 7.5 to 14 Volts DC and can therefore be powered by any VeriFone POS terminal or by external sources such as a battery or an alternate power source.

Data communication is controlled by the application and is therefore very flexible. The port operates at speeds from 300 to 19.2 Kbps. Messages to be transferred on the link may use the VeriFone standard protocol for PINpads or may be programmed to recognize the protocol and messages of any external device.

A number of standard cables connect the unit to a VeriFone terminal or an external device such as a PC. Alternate cables are available into which any 7.5–14 Volt DC power supply can be connected.

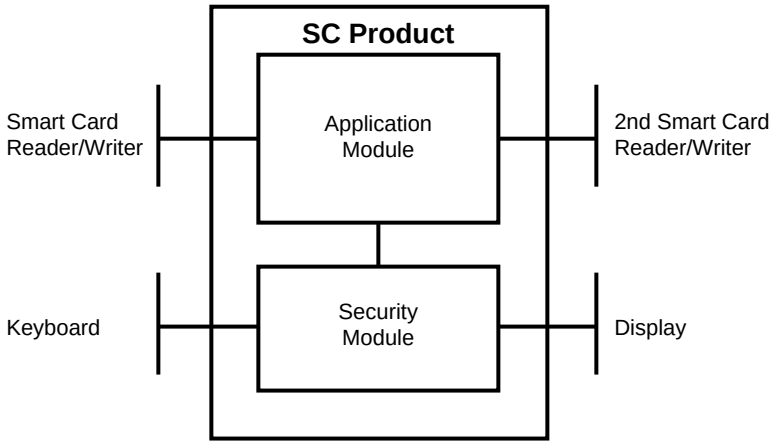
### *3.12 Feature Matrix*

| | | SC450 | SC455 | SC550 | SC552 |
|---|---|---|---|---|---|
| Memory | 32K | Yes | Yes | Yes | Yes |
| | 128K | Yes | Yes | Yes | Yes |
| Display | LCD | Yes | Yes | Yes | Yes |
| | Graphic | N/A | Option | Option | Option |
| Magnetic Card | | N/A | N/A | T1/2 or T2/3 | T1/2 or T2/3 |
| Smart Card | | Yes | Yes | Yes | Yes |
| 2nd Smart Card | | N/A | N/A | N/A | Yes |
| Keypad | | | | | |
| Membrane | | Yes | Yes | N/A | N/A |
| Rubber Mat | | N/A | N/A | Yes | Yes |
| Security Level | | | | | |
| No Security Chip | | Option | Option | Option | Option |
| High Security | | Yes | Yes | Yes | Yes |
| Very High Sec. | | N/A | Option | Option | Option |
| Sec. Chip Mask | | | | | |
| Version 8 | | Yes | Option | Option | Option |
| Version 25 | | N/A | Option | Option | Option |

## 4. Common Architecture

The SC product family uses a common electronic architecture. This enables the products to share applications and gives customers an expanded choice and a development growth path.

### *4.1 Architecture Overview*




The products are divided into two distinct modules: the application area and the security module. Each has its own microcontroller, storage memory and operating programs. There is a single, fixed, high-speed interface between the two modules.

### *4.2 Application Area*

This area contains all of the application programming, the code that controls the interface to the external device, the smart card interface and the interface to the Security module.

The application area consists of a main processor, a small amount of fixed ROM code, and 32K or 128K of battery-backed RAM.

The function of the ROM code is primarily to provide self tests when no main application has been loaded and to facilitate the loading of applications into RAM.

The RAM stores the application code and any data created by the application. Because the RAM is battery backed, the code and data are maintained even when the unit is powered off.

Applications are written in the ‘C’ programming language under the development environment provided by VeriFone for these products.

The application code has a number of functions. It controls the serial port interface to external devices sending messages and receiving responses. It is also responsible for the magnetic card and smart card interfaces, reading and processing data from each of these mediums.

For smart cards-because there are a number of different protocols, dependent on the card type and manufacturer-program code is required for each card type. This code is stored in the form of a special routine or driver for that card. By loading multiple drivers, different card types can be supported within a single application. As the application code can be downloaded remotely, card types supported within an application may be updated in the field.

Lastly, the application area controls the interface to the security module. Through this interface, the application can display messages/prompts, get data from the keyboard and request the required security function to be performed. This is achieved by sending a number of structured commands, which are recognized by the security module. Security is maintained because the application can only make requests, not obtain true access. For example, the application can request that a PIN be entered and encrypted by a stored key. The functions are then actually performed by the security module, which puts the correct prompts on the display, accepts the keyboard input, encrypts the data and passes the encrypted result to the application.

### *4.3 Security Module*

The security module performs all of the security functions of the products as well as interfacing to the display and keyboard. The security module is also the home of the security chip, which is the physical device that performs the encryption and storage of secret/sensitive data. The programming of the security module is loaded when the unit is manufactured. Although it may be tailored to the customer's exact requirements, it cannot be upgraded in the field. This restriction is to maintain the high security of the module. However since the operation of the security module is by a series of simple command requests, most changes can be accommodated by changes in the downloadable application area.

## 5. Development Environment

All products in the SC family are programmed using the same development environment and the 'C' programming language.

VeriFone has taken an existing 'C' compiler product, which is readily available worldwide, and has built a complete development environment around it.

The development environment includes the compiler and various tools for the programmer as well as a series of previously developed library routines for specific functions. These library routines include functions such as the interface commands to the security module for displaying data and driving the security chip. The smart card and magnetic card drivers are also included within these libraries. The aim of the libraries is to save each programmer from developing the standard functions required within each application.

More details on library functions and programming are provided within the Reference and Programming Manual for the SC family.