FIPS 140-2 Level-3 Non-propriety Security Policy

GO-Trust SDencrypter

Version	：	v5.0
Date	：	February 05, 2014
Classification	：	Public

EDITOR

Author	Title
Sean Huang	Senior Engineer

Revision History

Version	Description	Date	By
0.1	Initial Version	2013/02/04	Sean Huang
0.2	Response for comments	2013/02/08	Sean Huang
0.3	Update	2013/02/23	Sean Huang
1.0	Final Version	2013/03/21	Sean Huang
2.0	Modify per NIST comments	2013/11/13	Sean Huang
3.0	Modify per NIST comments	2014/01/13	Sean Huang
4.0	Modify per NIST comments	2014/01/29	Sean Huang
5.0	Modify per NIST comments	2014/02/05	Sean Huang

Table of Contents

1 Introduction

1.1 Purpose

This document describes the non-proprietary security policy for ***SDencrypter*** developed by GOTrust Technology Inc., in which illustrates how the cryptographic module meets the requirements for the security level 3 validation specified in the FIPS 140-2 standard. This security policy is part of the evidence documentation package to be submitted to the testing lab.

FIPS 140-2 specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard, please visit http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

1.2 Scope

This Security Policy specifies the security rules under which the cryptographic module operates its major properties. It does not describe the requirements for the entire system, which makes use of the cryptographic module.

1.3 Security Level

The SDencrypter meets the overall requirements applicable to FIPS140-2 Security Level 3. In the individual requirement sections of FIPS 140-2 the following Security Level ratings are achieved:

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self-tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

2 Cryptographic Module Specification

The GO-Trust SDencrypter, hereafter referred to as SDencrypter, acts as a flexible platform for constructing diversified security services such as secure mobile application, which possessing high performance, streaming encryption and decryption services. The SDencrypter comprises three major components: security element, SDencrypter controller and up to 16 GB of flash memory. The module contains CPUs, ROMs, and RAMs and all these components are packaged in the form factor of microSD card. The entire encryption, decryption, key exchange processing is completed inside the module. Fast “in-chip” processing, using a high-performance, Common Criteria EAL5+ certified security element, supports streaming data encryption, file encryption, key management, secure VPN, and media right protection. High-assurance protection is provided to keys and sensitive data which are encrypted and stored inside the Secure Element.

2.1 Cryptographic Module Boundary

The boundary of SDencrypter is the edge of one microSD card. The perimeter of the module forms the cryptographic boundary of this FIPS140-2 Security Level 3 compliant multiple-chip embedded cryptographic module.

Physical cryptographic boundary of SDencrypter can be referred to Figure 1, which shows a standard form factor of microSD. SDencrypter is approximately 15mm x 11mm and provides 8 standard contact pins plus 2 extended contact pins. Block diagram of SDencrypter shows as Figure 2.

Figure 1 – Physical Boundary of SDencrypter (Top view and Bottom view)

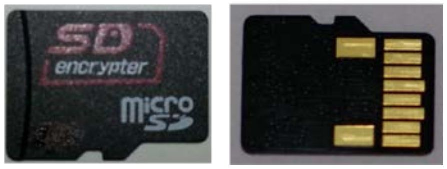
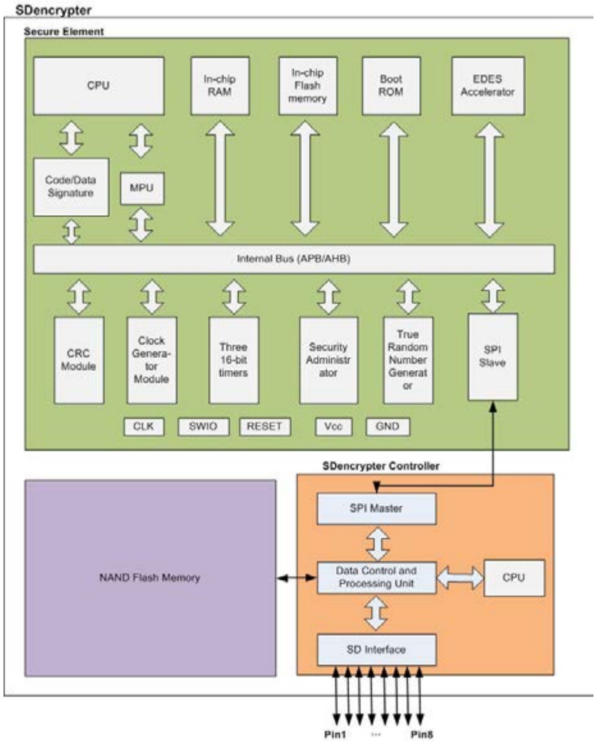
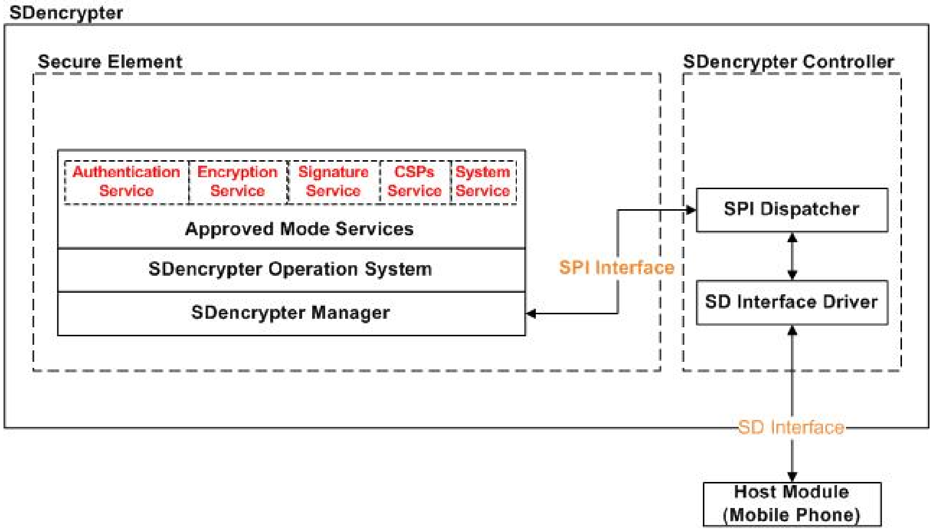


Figure 2 – Block Diagram of SDencrypter



Logical boundary of cryptographic module is shown as Figure 3, which describes firmware module on SDencrypter that provides Approved mode services.

Figure 3 – Logical Boundary Diagram



2.2 Hardware

SDencrypter is a multiple-chip embedded module that hardware boundary contains CPU, ROM, flash memory, and RAM. No components are excluded from the cryptographic boundary. Here lists important components of SDencrypter:

- Secure Element
  - 32 bit CPU
  - CPU clock frequency up to 22.5 MHz
  - 1280 KByte in-chip flash memory (include Boot ROM)
  - 30 KByte in-chip RAM
  - 1.8V, 3V, 5V supply voltage ranges
  - Hardware random number generator HRNG
  - Three hardware 16 bit timers

- Hardware security-enhanced DES accelerator EDES
- CRC module
- SPI Slave Interface
- Active shield
- Memory protection unit

▪ SDencrypter Controller

  - 8 bit CPU
  - 16 KByte flash memory
  - 36 KByte RAM

▪ NAND Flash Memory

  - Up to 16 GByte NAND flash memory

This security policy emphasizes that all FIPS Approved Mode Services of SDencrypter is performed in Secure Element; in other words, the reader should bear in mind that the processing and storage of CSPs can only happen inside the in-chip flash memory and the in-chip RAM of Secure Element, rather than flash memory of SDencrypter Controller and NANS Flash Memory.

2.3 Firmware

SDencrypter contains firmware residing in the module. The firmware is implemented using high level language (C) and comprises the two major parts, which are SDencrypter Controller firmware and Secure Element firmware.

1. SDencrypter Controller firmware:
   - SD Interface Driver: Receiving command from host module and sending response to host module via the standard SD 2.0 interface.
   - SPI Dispatcher: Sending command to Secure Element and receiving response from Secure Element via the defined SPI interface.
2. Secure Element firmware

- SDencrypter Manager: SDencrypter memory initialization and I/O control (SPI interface)
- SDencrypter Operation System: SDencrypter file system initialization and management
- Approve Mode Services and Operations: Provides all Approved mode services listing in Section 2.4.

2.4 FIPS Approved Mode Services

SDencrypter shall not contain Non-FIPS Approved mode services. The module does not implement bypass or maintenance modes. FIPS-Approved mode services includes:

- Authentication Services: authentication of roles of Crypto Officer and User
  - Authentication

- Encryption Services: FIPS validated encryption and decryption algorithms
  - Decryption
  - Encryption

- Signature Services: FIPS validated digital signature generation and verification
  - MAC
  - Signature Generation
  - Signature Verification

- CSPs Services: CSPs related operations including CSP generation, key derivation, key wrapping and CSP zeroization
  - Password Modification
  - Random Number Generation
  - Get Key Version
  - Key Generation
  - Put Key
  - Wrap Key
  - Clear Key

- System Services: system layer operation including show status and un-lock user password

- Self-Test
- Show Status

The details are shown in Table 5.

The FIPS-Approved mode services are implemented based on validated security functions shown in Table 2. According to the CAVEAT in the end of Table 2, FIPS-Approved mode of operation provides access to the services which use the security algorithms disallowed after NIST announced transition period that shall not be used.

2.5 Security Functions

The following table gives the list of security functions that are provided by the SDencrypter. These security functions can be invoked through related commands shown in Table 5. All of the security functions are included in GO-Trust Cipher Library v1.0.

Table 2 – Security Functions Implemented in Module

Security Functions	Details	CAVP Cert. #
AES	ECB (e/d; 128 , 192 , 256); CBC (e/d; 128 , 192 , 256);	#1664
HMAC	HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS, KS=BS, KS>BS) SHS (Cert. #1672 HMAC-SHA256 (Key Size Ranges Tested: KS<BS, KS=BS, KS>BS) SHS (Cert. #1672)	#1426

KDF	CTR_Mode: (Llength (Min20 Max70)
	MACSupported([HMACSHA1] [HMACSHA256])
	LocationCounter([AfterFixedData]) rlength([8]))
	RNG Val#999; HMAC Val#1426
		#7

RNG	ANSI X9.31[Triple-DES-2Key; AES-256Key]	#999

Security Functions	Details	CAVP Cert. #
RSA	FIPS186-2: ALG[RSASSA-PKCS1_V1_5]:SIG(gen), SIG(ver): 1024, 2048 ALG[RSASSA-PSS]:SIG(gen); SIG(ver); 1024, 2048 SHS: SHA-1 & SHA-256 Val#1672 FIPS186-3: 186-3KEY(gen): FIPS186-3_Fixed_e , FIPS186-3_Fixed_e_Value PGM (ProbPrimeCondition): 1024 , 2048 PPTT:(C.2) ALG[RSASSA-PKCS1_V1_5] SIG(gen): (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver): (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SHA-1 Val#1673; RNG Val#999	#976
SHS	SHA-1 (BYTE-only) SHA-256 (BYTE-only)	#1672
Triple-DES	TECB(e/d; KO 1,2); TCBC(e/d; KO 1,2)	#1237
AES Key Wrap	Compliant with SP800-38F key wrapping as an Approved key transport method indicated in [IG D.9] AES (Cert. #1664, key wrapping; key establishment methodology provides 256 bits of encryption strength)	non-Approved

CAVEAT: [SP800-131A] describes the transition associated with the use of cryptographic algorithms and key lengths; based on the information included in this publication the usage of following algorithms implemented in this cryptographic module is discouraged as they cannot be used in FIPS mode after the transition period:

- HMAC with key lengths < 112 bits, disallowed after 2013.
- RSA Key Generation and Digital Signature Generation with keys of length < 2048bits, disallowed after 2013.
- SHA-1 for digital signature generation, disallowed after 2013.
- Two-key Triple-DES Encryption: acceptable through 2010, restricted use from 2011 through 2015, disallowed after 2015.

- Two-key Triple-DES Decryption: Acceptable through 2010, legacy-use after 2010.

2.6 FIPS Approved Mode Indicator

SDencrypter provides "Show Status" in system service to indicate the module is under Approved mode.

3 Cryptographic Module Ports and Interfaces

The module's physical interfaces are composed of a set of contact pins providing data input, output, power, control in, status out and clock. No physical covers, doors, openings, physical status indicators and manual control interface are included in the module.

3.1 Physical Ports

Figure 4 – SDencrypter assigned pin number

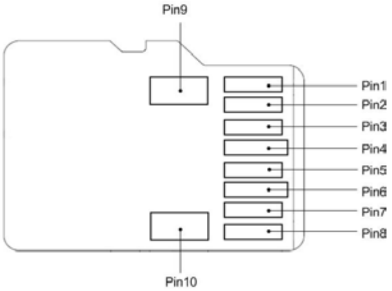


Table 3 – Physical Ports

Pin	Pin Assignment	Description
Pin1	DATA2	Data line[bit 2]
Pin2	DATA3	Data Line[bit 3]
Pin3	CMD	Command and response
Pin4	VCC	Supply voltage

Pin	Pin Assignment	Description
Pin5	CLK	Clock
Pin6	VSS	Supply voltage ground
Pin7	DATA0	Data line[bit 0]
Pin8	DATA1	Data line[bit 1]
Pin9	RFU	Reserved for future use
Pin10	RFU	Reserved for future use

3.2 Logical Interfaces

SDencrypter is configured as a slave controller to process and respond to the commands. The I/O ports of the platform provide the following logical interfaces:

Table 4 – Logical Interfaces

Logical Interface	Pin assignment
Data Input	DATA0, DATA1, DATA2, DATA3
Data Output	DATA0, DATA1, DATA2, DATA3
Control Input	CMD, CLK
Status Output	CMD
Power	VCC, VSS

The logical interfaces are kept logically separate when sharing a physical port by the protocols used. Information flows for the data input, data output, control input, and status output interfaces are encapsulated into SD 2.0 commands.

1. For logical interfaces “Data Input” and “Data Output”: They share the same physical ports (DATA0, DATA1, DATA2, DATA3). In this case the logical interfaces are kept logically separate when sharing the same physical ports by the data flow. If data goes into module, the physical ports mean “Data Input”. On the contrary data goes out module; the physical ports mean “Data Output”.

2. For logical interfaces “Control Input” and “Status Output”: They share the same physical ports (CMD). In this case the logical interfaces are kept logically separate when sharing the same physical port by the information flow. If information goes into module, the physical port means “Control Input”. On the contrary information goes out module; the physical port means “Status Output”.

4 Roles, Services and Authentication

SDencrypter supports two roles, Crypto Officer (CO) and User, and enforces the separation of these roles by restricting the services available to each one. The cryptographic module enforces the separation of operators using identity-based authentication, which can protect CSPs against unauthorized disclose, modification, and substitution by separation roles. Operator authentication is required while module is powered up, and the operator will be automatically log-out while module is powered down. Operator authentication is proceeded with the verification of operator password.

4.1 Roles

- **Crypto Officer Role**

The Crypto Officer role is responsible for initializing the module and managing the security configuration of the cryptographic module. Before issuing a module to an end user, the Crypto Officer initializes the module with keying material and private information. The cryptographic module validates the Crypto Officer identity using password verification before accepting any initialization commands. This role is also authorized to import keys, exchange keys.

- **User Role**

The User role is available after the cryptographic module has been loaded with a user personality. This role is authorized to read user data and use cryptographic services. The module allows only one operator to assume the User role, and the corresponding “User password” shall be known by one operator (i.e., the User) only.

The module does not implement any maintenance interface, thus there is no maintenance role defined.

4.2 Identification and Authentication

The module implements identity-based authentication which is accomplished by password entry by the operator. Each password phrase is at least 6 ASCII printable characters in length.

The Crypto Officer must change the default value during logon to make the module ready for initialization. During initialization the module allows the execution of only the commands required to complete the initialization process.

Before a user can access or operate the module, the Crypto Officer must initialize it with the User password. The Crypto Officer is authorized to log on to the module any time after initialization to change parameters.

Feedback of authentication data to an operator is obscured during authentication (e.g., no visible display of characters result when entering a password). The only feedback of authentication is a return code denoting success or failure of the operation. No return code or pointer to a return value that contains password.

For Crypto Officer password and User password separate retry counters are managed by the module, which are limited the default maximum number of consecutive unsuccessful password verification attempts to five, meeting the following rules:

- If the retry counter has reached zero, all further attempts to verify the corresponding password are rejected (the password is locked), i.e., no more Crypto Officer or User authentication, respectively, is possible. The module goes Error state.

- Each unsuccessful password verification attempt decreases the corresponding retry counter by one. Successful password verification resets the corresponding retry counter to 5.

The strength of the authentication mechanism conforms to the following specifications.

- Single password-entry attempt / False Acceptance Rate

  The probability that a random password-entry (using 94 printable characters) attempt will succeed or a false acceptance will occur is $1/94^{6}$=1.45×10^{-12}. The requirement for a single–attempt / false acceptance rate of no more than 1 in 1,000,000 (i.e., less than a probability of 10^{-6}) is therefore met.

- Multiple password-entry attempt in one minute

  With the module, the Crypto Officer or User password authentication takes about 0.2 second. The maximum number of tries in one minute is 60/0.2 = 300. There is also a maximum bound of 5 successive failed authentication attempts before system halt occurs. The probability of a successful attack of multiple attempts in a one minute period is no more than 7.24×10^{-12} due to the maximum of 5 attempts. This is less than one in 100,000 (i.e., 10^{-5}), as required.

4.3 Services

The services provided by the module to each role in terms of commands are specified in the table below:

Table 5 - The relation between Services and CSPs

No.	Category	Name (CO/User)	Description	Input	Output	CSPs Access (U:Use, W:Write)	SDencrypter	SDencrypter Lite
1.	hen tica	Authentication (CO/User)	User authentication	CO password	results of authentication	CO password: U	√	√

No.	Category	Name (CO/User)	Description	Input	Output	CSPs Access (U:Use, W:Write)	SDencrypter	SDencrypter Lite
			(Crypto Officer or User)	or User password		User password: U		
2.	Encryption	Decryption (CO/User)	Decrypts data via validated security function	Ciphertext	Plaintext	Secure Channel Session Key: U User AES Session Key: U User Master Key: U User Triple-DES Session Key: U	√	√
3.		Encryption (CO/User)	Encrypts data via validated security function	Plaintext	Ciphertext	Secure Channel Session Key: U User AES Session Key: U User Master Key: U User Triple-DES Session Key: U	√	√
4.	Signature	MAC (CO/User)	Calculates a message digest via hash function (SHA or HMAC)	Message	MAC value	Secure Channel Session Key: U User Master Key: U	√	
5.		Signature Generation (CO/User)	Generates a digital signature with a previously loaded RSA private key	Message	Signature	User RSA Private Key: U	√	√
6.		Signature Verification (CO/User)	Verifies a digital signature with a previously loaded RSA public key	Message and Signature	Result of verification	RSA Public Key: U	√	
7.	CSPs	Password Modification (CO/User)	Change User password	CO/ User password	Result of Modification	CO password: W User password: W	√	√

No.	Category	Name (CO/User)	Description	Input	Output	CSPs Access (U:Use, W:Write)	SDencrypter	SDencrypter Lite
						Secure Channel Session Key: U		
8.		Random Number Generation (CO/User)	Get a random value for external authentication	Seed Key and Seed	Random number	Seed Key: U Seed: U	√	√
9.		Get Key Version (CO/User)	Get the Version of CSPs	CO/User password Key ID	Key version	CO password: U User password: U	√	√
10.		Key Generation (CO)	Generate keys	CO password	User AES Session Key User RSA Private Key User RSA Public Key User Triple-DES Session Key	CO password: U User RSA Public Key: W User AES Session Key: W User RSA Private Key: W User Triple-DES Session Key: W	√	√
11.		Put Key (CO)	Put keys to the module	CO password and key to be loaded	Result of Put Key	CO password: U Key Encryption Key: U Secure Channel Master Key: W User Master Key: W User AES Session Key: W RSA Public Key: W User Triple-DES Session Key: W	√	√
12.		Wrap Key (CO)	Wrap Key that will be outputted	CO password and key to be wrapped	Result of Wrap Key	CO password: U Key Encryption Key: U Secure Channel Session Key: U User AES Session Key: U User RSA Public Key: U User Triple-DES Session Key: U	√	√

No.	Category	Name (CO/User)	Description	Input	Output	CSPs Access (U:Use, W:Write)	SDencrypter	SDencrypter Lite
13.		Clear Key (CO)	Clear all stored keys	CO password	Result of Clear Key	CO Password: U All CSPs: W	√	√
14.	System	Self-Test (CO/User)	Integrity test and know answer test of validated security function	N/A	Result of Self-Tests	N/A	√	√
15.		Show Status (CO/User)	Indicate the current status of cryptographic module	N/A	Result of current status	N/A	√	√

5 Physical Security

The cryptographic module is multiple-chip embedded module as defined by FIPS 140-2 and is designed to meet security level 3 physical security requirements. And it has following characteristics.

- The module is covered by tamper-evident molded epoxy, and no removable covers or doors are implemented to permit physical access.
- The module does not contain any ventilation holes or slits.
- The opaque coating of module deters direct observation within the visible spectrum.
- The tamper-evident hard epoxy enclosure provides evidence of tampering, with high probability of causing serious damage to the module while attempting to probe the inner circuit by removing the hard enclosure.

5.1 Physical Security mechanisms as required by FIPS 140-2

The SDencrypter is in production grade and uses a tamper-evidence epoxy microSD as a physical security mechanism. All card models are constructed identically in terms of locations of types of components, including physical security mechanisms.

The chips are covered on one side by epoxy and on the other by substrate. A non-removable, tamper evident epoxy cover that is compatible with microSD card readers surrounds the substrate underneath the chips and the epoxy on top of the chips. The epoxy cover exposes one set of contact pins.

The epoxy that covers the otherwise exposed contact pins surrounds the pins. The physical tampering of epoxy cover will result in damage to the epoxy that covers the otherwise exposed contact pins and underlying circuitry with high probability of causing serious damage to the circuitry that the module is not function anymore. The epoxy that covers the otherwise exposed contact pins must be inspected periodically to ensure that physical security is maintained.

5.2 Additional Hardware Security Mechanisms

The SDencrypter does not provide additional hardware security mechanism.

6 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements do not apply to the module in this validation because the module does not contain a modifiable operational environment.

7 Cryptographic Key Management

7.1 Critical Security Parameters and Public Keys

The cryptographic module includes system keys and passwords for card administration purposes.

The following table provides a list and description of all CSPs and public keys managed by the module.

Table 6 – Critical Security Parameters and Public Keys

CSP/ Public Key	Type	Generated/ Input	Output	Storage	Usage	Zeroization
Crypto Officer password	6 ASCII printable characters	Entered the module in encrypted form	No output	Plaintext in in-chip flash memory	Used for Crypto Officer authentication	By command or factory reset
Key Encryption Key	AES-256 Key	Hard-coded in the firmware	No output	Plaintext in in-chip flash memory	Used to wrap keys	By command or factory reset
RSA Public Key	RSA-2048	Entered the module in encrypted form	No output	Plaintext in in-chip flash memory	Used to verify signature	By command or factory reset
Secure Channel Master Key	AES-256 Key	Entered the module in encrypted form	No output	Plaintext in in-chip flash memory	Used to generate Secure Channel Session Key	By command or factory reset
Secure Channel Session Key	AES-256 Key	Generated by KDF function	No output	Plaintext in in-chip volatile memory	Used to protect communication session	By power cycle or session termination
Seed	RNG Seed 128-bit value	Generated by HRNG	No output	Plaintext in in-chip volatile memory	Used to seed ANSI X9.31 RNG	By power cycle or by command
Seed Key	RNG Seed Key 256 bit of AES	Generated by HRNG	No output	Plaintext in in-chip volatile memory	Used to seed ANSI X9.31 RNG	By power cycle or by command
User AES Session Key	AES-256 Key	1. Generate outside: Entered the module in encrypted form 2. Generate in-chip	Output in encrypted form	Plaintext in in-chip flash memory	Used to protect User data	By command or factory reset
User Master Key	AES-256 Key	Entered the module in encrypted form	No output	Plaintext in in-chip flash memory	Used to protect User data	By command or factory reset
User password	6 ASCII printable characters	Entered the module in encrypted form	No output	Plaintext in in-chip flash memory	Used for User authentication	By command or factory reset

CSP/ Public Key	Type	Generated/ Input	Output	Storage	Usage	Zeroization
User RSA Private Key	RSA-2048	Internally-generated with FIPS 186-3 key generation	No output	Plaintext in in-chip flash memory	Used to generate signature	By command or factory reset
User RSA Public Key	RSA-2048	Internally-generated with FIPS 186-3 key generation	Output in encrypted form	Plaintext in in-chip flash memory	Used to verify signature	By command or factory reset
User Triple-DES Session Key	Triple-DES-192 Key	1. Generate outside: Entered the module in encrypted form 2. Generate in-chip	Output in encrypted form	Plaintext in in-chip flash memory	Used to protect User data	By command or factory reset

7.2 Key Generation and Diversification

SDencrypter can generate Secure Channel Session Key, RSA key pair, User AES Session Key and User Triple-DES Session Key. Secure Channel Session Key is a 256-bit AES key derived from Secure Channel Master Key using key derivation function (KDF), while RSA key pair generation follows the method shown in FIPS 186-3. Moreover, User AES Session Key and User Triple-DES Session Key are generated following the method given in FIPS 140-2 Implementation Guidance based on Approved RNG.

7.3 Key Entry and Output

Input and output of Keys in SDencrypter shall always be proceeded using the service of Put Key/Wrap Key. Put Key service adopts the key wrapping process called AES key wrap with authenticated encryption (KW-AE) recommended in NIST Special Publication 800-38F. RSA public key, User AES Session Key and User Triple-DES Session Key are allowed to be outputted in encrypted form.

7.4 Key Storage

Secure Channel Session Key as well as RNG seed values are stored in volatile memory for temporarily usage. Other keys and CSPs that need to be permanently protected are stored in the in-chip flash memory of Secure Element.

7.5 Key Zeroization

Keys stored in flash memory can be zeroized by “Clear key” service. Session keys are stored in volatile memory and act as one-time key that cannot be used while the session is done. In addition, SDencrypter can also use “Clear Key” service to zeroize all CSPs.

7.6 RNG Seed Values

During power up initialization, the module uses HRNG to compute new Seed and Seed Key values. These seed values are temporarily exists in volatile memory and are zeroized by power cycling the module. These values are not accessible to any user.

7.7 Protect against unauthorized exploitation

There are secret keys, private and public keys, and CSPs internal which stored in flash memory and RAM of cryptographic module. It must have the necessary permission when these secret keys and parameters shall be output, modify, or substitute. If the user don’t log into, these secret keys and parameters shall be prohibited from unauthorized operation.

7.8 Notice about keys

Not any intermediate key generation values are output from the module upon completion of the key generation process.

8 Electromagnetic Interference/Compatibility (EMI/EMC)

SDencrypter meets the EMI/EMC requirements according to FCC 47 CFR part 15, subpart B, class B, and received the corresponding certificate of conformity.

9 Self-Tests

The module performs both power-up and conditional self-tests. These tests are conducted automatically as part of the normal functions of the SDencrypter. They do not require any additional operator intervention. All data output via the output interface is inhibited while any power-up and conditional self-test is running.

Self-Tests failure resulting in the module goes into an Error state. In the error mode, the module no longer responds to further commands, and output any data. To remove the error state you need to return the module to the vendor for servicing.

9.1 Power-up Self-Tests

Each time as the SDencrypter is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged.
Resetting the cryptographic module provides a means by which the operator can perform the power-up self-tests on demand.

These tests include:

- Cryptographic algorithm testing

  Known Answer Tests (KATs) are conducted for each cryptographic algorithm in one mode of operation. Known input data and answers are stored in flash memory. KATs include following:

  - AES
  - ANSI X9.31 RNG
  - HMAC
  - KDF
  - Key Wrapping
  - RSA

- SHA
- Triple-DES

KATs function by separate encrypting, decrypting, hashing, signing or verifying a string for which the calculated output is known and stored within SDencrypter. An encryption, hashing or signature test passes when the calculated output matches the expected (stored in flash memory) value. The test fails when the calculated output does not match the expected value.

KATs for ANSI X9.31 RNG function by seeding the ANSI X9.31 RNG with known values and checking that the output matches the pre-calculated value stored within SDencrypter. The module also performs Continuous RNG tests for HRNG and ANSI X9.31 RNG described below.

- Firmware integrity testing

Firmware of SDencrypter comprises firmware of Secure Element and firmware of SDencrypter Controller. The integrity of firmware of Secure Element is checked with 32-bit checksum is stored in flash memory. And the integrity of firmware of SDencrypter Controller is ensured with 16-bit checksum.

If and only if all power-up self-tests are passed successfully, the cryptographic module performs the command procedure according to the first command (received before or after power-up self-tests started) and returns the corresponding response and status word via the data output interface and status output interface.

9.2 Conditional Self-Tests

- Continuous RNG Tests:

A continuous RNG test is performed during each use of both ANSI X9.31 RNG and HRNG to verify that it is not generating the same value. Each subsequent generation of a 128-bit block will be compared with the previously generated block. The test will fail if any two compared blocks are equal.

- Pair-wise Consistency Tests:

  A pair-wise consistency test is performed on RSA key pair generation.

10 Design Assurance

10.1 Configuration Management

SDencrypter product family includes the following two models according to the configuration of firmware. Both of two models satisfied the requirement of FIPS 140-2 Security Level 3.

Model Name	Secure Element Model Name	Secure Element Firmware Version	Controller Model Name	Controller Firmware No.	Firmware Configuration
GO-Trust SDencrypter	GT-3001	4.1.0.8	GT-0330	80023802-33860406	Normal
GO-Trust SDencrypter-Lite	GT-3001	4.1.0.8	GT-0330	80023802-33860506	Lite

1. Firmware configuration – Normal
   - Provide full support of Approved mode services. (See Table. 5)
   - High SPI throughput
2. Firmware configuration – Lite
   - Provide partial support of Approved mode services. (See Table. 5)
   - Low SPI throughput

SDencrypter-Lite does not provide host module the capability of accessing services like message digest, HMAC and RSA verification. However, the internal operation is not restricted from this limitation. For example, the process of RSA signature generation can still internally use the service of generating message digest.

The module was designed and developed using a configuration management system “Subversion” that is clearly ruled and operated. The definition methods, mechanisms and tools that allow identifying and placing under control all the data and information are specified in the configuration management document.

10.2 Guidance Documents

The “GOTrust SDencrypter_Getting_Started” document was designed to allow a secure operation of the module by its users as defined in the “Roles, Services and Authentication” chapter and in the scope of the Security Policy boundaries. Moreover, this document also defines and describes the steps necessary to deliver and operate the module securely.

11 Mitigation of Other Attacks

The GO-Trust SDencrypter is not designed to mitigate any specific attacks outside of those required by FIPS 140-2.

12 Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

12.1 General Security Rules

- The module does not support the service that updates firmware and software.
- The module restricts all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module.
- The module logically disconnects the output data path from the circuitry and processes when performing self-tests, key generation, key zeroization, or error states.

- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

12.2 Identification and Authentication Security Rules

- The module enforces Identity-Based authentication.
- Authenticated operators are authorized to assume either supported role. The module does not allow the operator to change roles.
- The module does not support multiple concurrent operators.
- The module does not support a maintenance interface or role.
- When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
- The module re-authenticates an operator when it is powered-up after being powered-off.
- The cryptographic module clears previous authentications on power cycle.

12.3 Access Control Security Rules

- While processing a transaction, prior to returning a response, the module will ignore all other inputs to the module. No output is performed until the transaction is completed, and the only output is the transaction response.
- The module does not enter plaintext CSPs. Authentication data (e.g. passwords) are protected by Secure Channel Session Key. Authentication data is not output during entry.
- The module does not support manual key entry.
- The module does not have any external input/output devices used for entry/output of data.
- The module does not perform any cryptographic functions while key loading or in an error state.

- Power-up self-test is automatically triggered.

12.4 Physical Security Rules

- The operator shall check of epoxy package and contact plate, whether the module is physically intact.
- The epoxy cover on the same side as the covered pins must also be inspected periodically to determine if there is visible evidence of tampering or if the substrate underneath the two chips has been exposed to ensure that physical security is maintained.
- The epoxy cover on the opposite side must also be inspected periodically to determine if there is visible evidence of tampering or if the epoxy covering the top of the two chips has been exposed to ensure that physical security is maintained.
- The physical security provided from the hardness of the module's epoxy enclosure is claimed at Operating temperature range (-25°C to +85°C). No assurance of the enclosure hardness is claimed for this physical security mechanism outside of this range.

12.5 Mitigation of Other Attacks Security Rules

- The GO-Trust SDencrypter is not designed to mitigate any specific attacks outside of those required by FIPS 140-2.

13 Security Policy Check List Tables

13.1 Roles and required Identification and Authentication

Table 8 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	password verification	User password
Crypto Officer	password verification	Crypto Officer password

13.2 Strength of Authentication Mechanisms

Table 9- Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password verification	The module prevents brute-force attacks on its password by using at least 6-character password. And a limit of 5 failed authentication attempts is imposed; 5 consecutive failed authentication attempts causes system halted. According the calculation in Section 4.2. ▪ Single password-entry attempt / False Acceptance Rate The probability that at least a random 6-character password-entry attempt will succeed or a false acceptance will occur is approximately 1.45×10^{-12}. ▪ Multiple password-entry attempt in one minute The probability of a successful attack of multiple attempts in a one minute period is no more than 7.24×10^{-12}.

13.3 Services Authorized for Roles

Table 10 - Services Authorized for Roles

Role	Authorized Services
User	Section 4.3 lists authorized services for this role
Crypto Officer	Section 4.3 lists authorized services for this role

14 References

[FIPS140-2] Security Requirements for Cryptographic modules, May 25, 2001

[SP 800-131A] NIST Special Publication 800-131A: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January, 2011

[IG] Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, January 17, 2014

[SD 2.0] SD Specifications Part 1 Physical Layer Specification, Version: 2.0, May 9, 2006

15 Acronyms

AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CLK	Clock
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CRC	Cyclic Redundancy Check

CSP	Cryptographic Security Parameter
DES	Data Encryption Standard
DRNG	Deterministic Random Number Generator
EDES	Enhanced DES accelerator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standards
GND	Ground pin
HMAC	Keyed-Hash Message Authentication Code
HRNG	Hardware Random Number Generator (Non-Deterministic Random Number Generator)
KAT	Known Answer Test
KDF	Key Derivation Function
MAC	Message Authentication Code
MPU	Memory Protection Unit
NAND	Negated AND
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest Shamir and Adleman Public Key Algorithm
RST	Reset pin
SD	Secure Digital
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface
VCC	IC power supply pin
VPN	Virtual Private Network