VaultIC420™, VaultIC440™, VaultIC460™

GENERAL BUSINESS USE

FIPS 140-2 Non-proprietary Security Policy

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the INSIDE Secure VaultIC420, VaultIC440 and VaultIC460 security modules (respective ordering part numbers are ATVaultIC420, ATVaultIC440 and ATVaultIC460). This Security Policy describes how the VaultIC security module meets the security requirements of Federal Information Processing Standard (FIPS) Publication 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the FIPS 140-2 level 3 validation of the module.

FIPS 140-2 details the U.S. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at: http://csrc.nist.gov/groups/STM/index.html.

The VaultIC security module is referred to in this document as cryptographic module, security module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Inside Secure website (http://www.insidesecure.com) contains information on the full line of products from Inside Secure.
- The CMVP website (http://csrc.nist.gov/groups/STM/index.html) contains contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Module Technical Datasheet
- Algorithm Test Form
- Finite State Machine
- Other supporting documentation as additional references

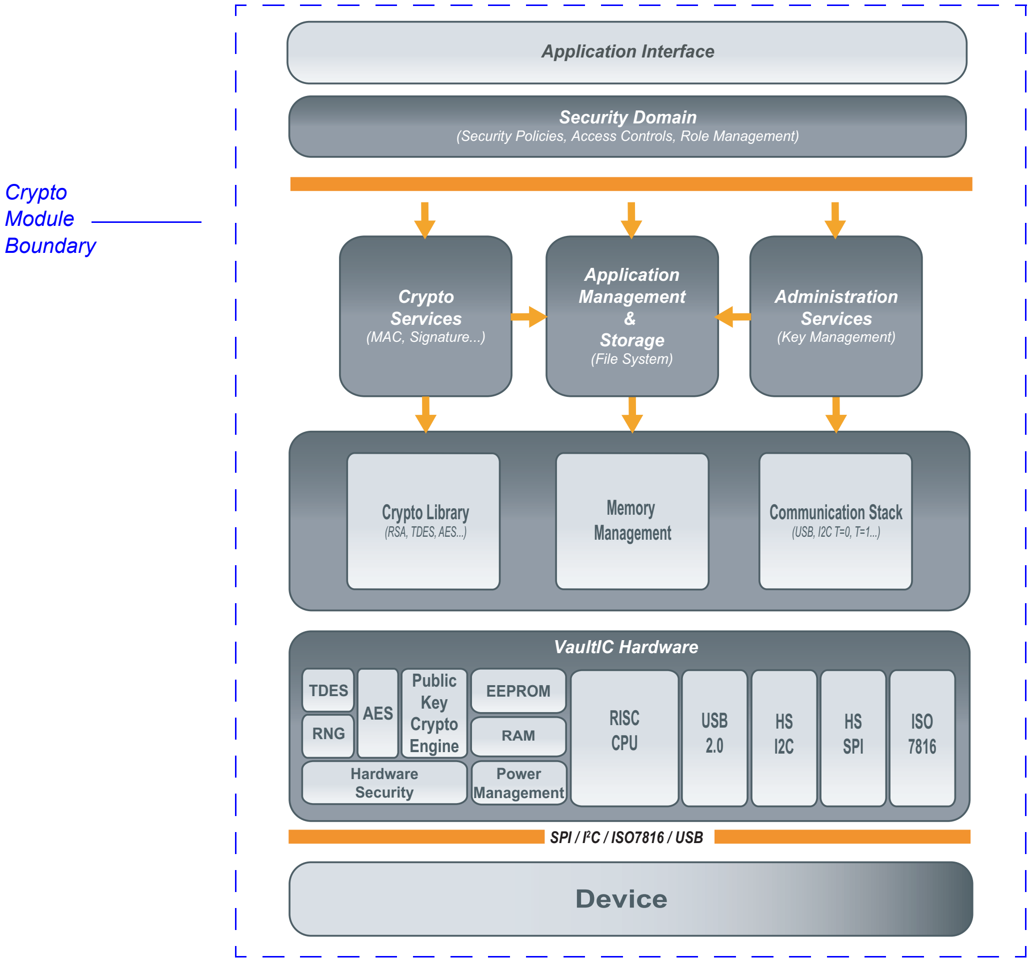
2. VaultIC Module Overview

The VaultIC420, VaultIC440 or VaultIC460 is an ASSP designed to secure various systems against counterfeiting, cloning or identity theft. It is a hardware security module that can be used in many applications such as IP protection, access control or hardware protection.

The proven technology used in the security module is already widespread and used in national ID/health cards, e-passports, bank cards (storing user Personal Identification Number, account numbers and authentication keys among others), pay-TV access control and cell phone SIM cards (allowing the storage of subscribers' unique ID, PIN code, and authentication to the network), where cloning must definitely be prevented.

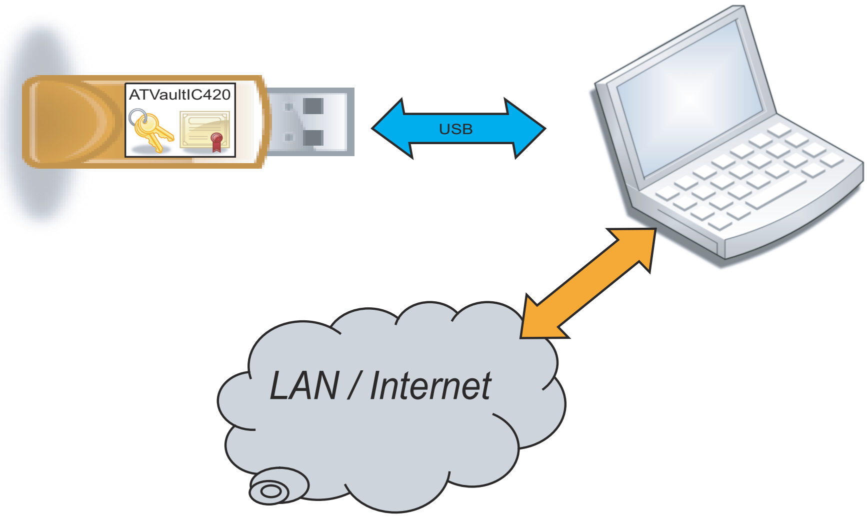
Designed to keep contents secure and avoid leaking information during code execution, the security module includes voltage, frequency and temperature detectors, illegal code execution prevention, tampering monitors and protection against side channel attacks and probing. The chips can detect tampering attempts and destroy sensitive data on such events, thus avoiding data confidentiality being compromised. Strong Authentication capability, secure storage and flexibility thanks to its various interfaces (USB, SPI, I^2C, ISO7816), low pin count and low power consumption are main features of the VaultIC. Its embedded firmware provided advanced functions such as Identity-based authentication, large Cryptographic command set, various Public domain cryptographic algorithms, Cryptographic protocols, Secure Channel Protocols, Robust communication protocol

Figure 2-1. Security Module block diagram



Below is described an example of VaultIC 4xx product in the typical USB eToken application.

Figure 2-2. USB eToken application



The module contains a cryptographic toolbox, providing basic FIPS Approved security functions to support SCP protocols and secure key storage.

Table 2-1 describes the configuration of hardware and firmware for the FIPS 140-2 validation.

Table 2-1. Versioning Information

	VaultIC420	**VaultIC440**	**VaultIC460**
Commercial Part Number	ATVaultIC420	ATVaultIC440	ATVaultIC460
Hardware Platform	AT90SO128 - Silicon Rev C		
Firmware Version	**1.2.1**		

Note

VaultIC420, VaultIC440 and VaultIC460 modules are all the same physically and offer the same functionnalities. They only differ in the size of the file system.

3. Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 3-1. Module Security Level Specification

Security Requirements Section	**Level**
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	4
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

4. Modes of Operation

VaultIC operates in different modes of operation, given different conditions of use of keys and cryptographic services. The mode of operation is automatically selected according to the device state and the authenticated operator. The selected mode of operation remains activated while the operator is authenticated. The mode of operation is discarded when the authentication is cancelled or the secure channel is terminated.

FIPS Approved Mode of Operation and Non-Approved Mode of Operation specify the conditions of use when the product is in the field.

In addition, for performance reasons, FIPS Approved Mode of Operation can be disabled at personalization time. *FIPS mode* capability can be turned off and on by logging in as the Manufacturer role and using the *Set Config* command. The module is zeroized when switching between FIPS and non-FIPS mode, including the file system and cryptographic keys being wiped.

Note

By default, the module is configured in FIPS mode.

4.1 FIPS Approved Mode of Operation

This mode is automatically selected when the device is in ACTIVATED state and an approved user or an approved administrator is successfully authenticated. While in an approved mode of operation, only Approved and Allowed Algorithms are allowed. Additional security restrictions may apply.

Note

The module will indicate that it is running in the FIPS Approved mode of operation by indicating *Mode of Operation: Approved* in the response of a *Get Info command*.

4.2 Non-Approved Mode of Operation

This mode is automatically selected when the device is in ACTIVATED state and a non-approved user, a non-approved administrator or a manufacturer is successfully authenticated. While in a non-approved mode of operation, the VaultIC™ usage is not restricted and both Approved and Allowed Algorithms and Non-Approved, Non-Allowed Algorithms are allowed.

Note

The module will indicate that it is running in the non-FIPS Approved mode of operation by indicating *Mode of Operation: non-approved mode* in the response of a *Get Info command*.

CSPs are not shared between the non-Approved and Approved modes of operation.

4.3 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 4-1. FIPS Approved Algorithms used in VaultIC Module

FIPS Approved Algorithm
AES as per FIPS 197: ECB, CBC, CFB, OFB and CTR modes 128, 192 and 256 bits
Triple-DES 3-Key: ECB, CBC, CFB, OFB modes EDE and EEE schemes Triple-DES 2-Key: Decrypt only for legacy use
AES CMAC as per NIST SP 800-38B: 128, 192 and 256 bits
SHA-1, -224, -256, -384, -512 as per FIPS 180-3
HMAC as per FIPS 198: With SHA-1, -224, -256, -384, -512
RSA 1024 bits as per FIPS 186-3: Signature verification only for legacy use RSA 2048 and 3072 bits: Signature generation and verification Keypair generation
DSA 1024 bits as per FIPS 186-3: Signature verification only for legacy use DSA 2048 bits: Signature generation and verification Keypair generation
ECDSA as per FIPS 186-3: Minimum 224 bits, up to 576 bits Signature generation and verification Keypair generation
DRBG as per NIST SP800-90: Using CTR_DRBG_AES_256

The cryptographic module supports the following non-FIPS Approved algorithms which are allowed for use in FIPS mode.

Table 4-2. FIPS Allowed Algorithms used in VaultIC Module

FIPS Allowed Algorithm
Hardware NDRNG: Used to seed the Approved DRBG
AES Key Wrap - Key establishment methodology provides 128, 192 or 256 bits of security strength

4.4 Non-Approved, Non-Allowed Algorithms

The cryptographic module supports the following non-Approved algorithms to be used only in a non-Approved mode of operation. No security claim is made in the current module for any of the following non-Approved algorithms.

Table 4-3. Non-Approved, Non-Allowed Algorithms used in VaultIC Module

Non-FIPS Allowed Algorithm
HOTP as per RFC 4226
TOTP as per OATH Draft v5
DES as per FIPS 46-3
2-Key Triple-DES Encrypt of bulk data
RSA Encrypt/Decrypt of bulk data as per PKCS#1 v2.1
ISO 9797 security functions: DES, DES MAC, 2-Key Triple-DES, Triple-DES MAC (non-compliant)

5. Ports and Interfaces

The module is a single-chip module with ports and interfaces as shown below.

Table 5-1. VaultIC Pins and FIPS 140-2 Ports and Interfaces

Pin	FIPS 140-2 Designation	Name and Description
SPI_SCK	Control Input	SPI Clock
ISO_CLK	Control Input	ISO7816 Clock
USB_XIN	Control Input	USB 2.0 Resonator Input
USB_XOUT	Status Output	USB 2.0 Resonator Output
RST	Control Input	CPU Reset
VCC	Power	Power Supply
GND	N/A	Ground
SPI_MISO	Status Output, Data Output	SPI Master In Slave Out
SPI_MOSI	Control Input, Data Input	SPI Master Out Slave In
RTC_XIN	Control Input	RTC Quartz signal Input
RTC_XOUT	Status Output	RTC Quartz signal Output
VBAT	Power	RTC Power Supply
SPI_SS I2C_SCL	Control Input Control Input	SPI Slave Select I2C Clock
SPI_SEL I2C_SDA ISO_IO0	Control Input Control Input, Data Input, Data Output, Status Output Control Input, Data Input, Data Output, Status Output	SPI or I2C selection I2C Data line ISO7816 Data line
USB_DM	Control Input, Data Input, Data Output, Status Output	USB D- Differential Data

Table 5-1. VaultIC Pins and FIPS 140-2 Ports and Interfaces

Pin	FIPS 140-2 Designation	Name and Description
USB_DP	Control Input, Data Input, Data Output, Status Output	USB D+ Differential Data
GPIO#0 to #4	Control Input, Data Input, Data Output	GPIO / I2C Address
GPIO#5 to #7	Data Input, Data Output	GPIO

6. Identification and Authentication Policy

6.1 Assumption of Roles

The module supports three distinct operator roles, the *User*, the *Administrator* (Cryptographic Officer) and the *Manufacturer*. The cryptographic module enforces the separation of roles using identity based authentication mechanisms. It is identity based because the keys and passwords used for authentication are unique to each other.

Authentication is based on the following:

Table 6-1. Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
Approved-Administrator	The administrator can usually manage the approved roles authentication data and perform approved-only cryptographic operations and key sizes	Secure Channel Protocol 03 *OR* Microsoft Card Minidriver	AES S-MAC Key *OR* Triple-DES 3K Key
Approved-User	A user is assumed to perform general security services and approved-only cryptographic operations and key sizes	Secure Channel Protocol 03 *OR* Microsoft Card Minidriver	AES S-MAC Key *OR* Triple-DES 3K Key
Manufacturer	The manufacturer can personalize and configure the chip and perform maintenance operations.	Password *OR* Secure Channel Protocol 02 *OR* Secure Channel Protocol 03 *OR* Microsoft Card Minidriver	4 - 32 byte string *OR* Triple-DES S-MAC Key *OR* AES S-MAC Key *OR* Triple-DES 3K Key

Table 6-2. Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Secure Channel Protocol 03	Based on knowledge of a 128, 192 or 256 bit AES Key (S-MAC) AES CMAC provides 128 bits of security. The probability of a random attempt or a false acceptance occurring is then 1 in 2^{128} which is less than 1 in 1,000,000. For multiple attempts in a one minute period, the device will lock out after a maximum of 127 failed authentication attempts. Therefore, the probability of a random attempt succeeding within a one minute period is 127 in 2^{128} which is less than 1 in 100,000.
Microsoft Card Minidriver	Based on knowledge of a 168 bit Triple-DES Key. Triple-DES 3Keys encryption provides 112 bits of security. The probability of a random attempt or a false acceptance occurring is then 1 in 2^{112} which is less than 1 in 1,000,000. For multiple attempts in a one minute period, the device will lock out after a maximum of 127 failed authentication attempts. Therefore, the probability of a random attempt succeeding within a one minute period is 127 in 2^{112} which is less than 1 in 100,000.
Password	Based on knowledge of a hexadecimal string, between 4 and 32 bytes. The highest probability of a random attempt or a false acceptance occurring is then 1 in 2^{32} which is less than 1 in 1,000,000. For multiple attempts in a one minute period, the device will lock out after a maximum of 127 failed authentication attempts. Therefore, the probability of a random attempt succeeding within a one minute period is 127 in 2^{32} which is less than 1 in 100,000.

6.2 Authenticated Services

Table 6-3. Administrator, User and Manufacturer Services

Service	Description
Initialize Update	Used for generation of session keys to setup secure channel and authenticate its message contents
External Authenticate	Allows transmission of authentication data
Manage Users	Authenticated administrator can add, delete or modify authentication data of any approved operators.
Update Authentication Data	Authenticated operator can update its own authentication data (change password or static keyset)
Get Authentication Info	Returns authentication method, roles access, security level, number of authentication attempts remaining, sequence counter
Cancel Authentication	Returns module to un-authenticated state
Put Key	Electronically enters keys (keys always encrypted in FIPS mode)
Read Key	Electronically outputs keys (keys always encrypted in FIPS mode)
Delete Key	Zeroizes keys

Table 6-3. Administrator, User and Manufacturer Services

Service	Description
Initialize Algorithm	Initializes cryptographic algorithm with key and algorithm specific parameters
Encrypt/Decrypt Message	Performs data encryption/decryption of provided message
Generate/Verify Signature	Generates signature on incoming messages or verifies incoming message and signature
Compute Message Digest	Computes a digest of provided message
Generate Key Pair	Internally generates public/private keypair
Generate Random	Generates random data utilizing internal DRBG
GPIO command set	Provides access to General Purpose I/O pin data (no CSP access)
File System Command set	Read/ Delete/ Modify files, folder, and access permissions of internal file system (no CSP access)
Get Info (Get Status)	Provides current status of the module, and returns FIPS mode indicator
Self-Tests	Executes the suite of self-test
Set Status	Changes the Life cycle state of the module
Set Config	Changes internal parameters and settings of the module
Test Command set	Dummy commands for integration testing purposes (no CSP access)

6.3 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 6-4. Unauthenticated Services

Service	Description
Initialize Update	Used for generation of session keys to setup secure channel and authenticate its message contents
External Authenticate	Allows transmission of authentication data
Get Authentication Info	Returns authentication method, roles access, security level, number of authentication attempts remaining, sequence counter
Cancel Authentication	Returns module to un-authenticated state
Generate Random	The random data generated by this service is not used by any other internal service. It is considered to be user data. It is not CSP nor is it used in the generation of any CSP or Key
General Purpose I/O	Provides access to I/O pin data (no CSP access)
Get Info (Get Status)	Provides current status of the module, and returns FIPS mode indicator
Self-Tests	Executes the suite of self-test

6.4 Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

Table 6-5. Private Keys and CSPs

Key Name	Type	Description
SCP03 S-ENC Static Key	AES (128, 192, or 256 bits)	SCP03 static AES encryption key
SCP03 S-MAC Static Key	AES (128, 192, or 256 bits)	SCP03 static AES MAC key
SCP03 C-MAC Session Key	AES (128, 192, or 256 bits)	SCP03 AES session key for authentication of incoming data
SCP03 R-MAC Session Key	AES (128, 192, or 256 bits)	SCP03 AES session key for authentication of outgoing data
SCP03 C-ENC Session Key	AES (128, 192, or 256 bits)	SCP03 AES session key for data encryption
Microsoft Minidriver Static Key	Triple-DES 3K 168 bits	Secret Key used for operator authentication
Triple-DES Keys	Triple-DES 3K 168 bits	Used to encrypt/decrypt messages
Triple-DES Keys	Triple-DES 2K 112 bits	Used to decrypt messages
AES Keys	AES (128, 192, or 256 bits)	Used to encrypt/decrypt messages or generate C-MACs
Seed and Seed Key	Seed and Seed Key	Used to seed the FIPS Approved DRBG (CTR_DRBG_AES256)
RSA Private Key	RSA 2048 & 3072 bits	Used for RSA signature generation
DSA Private Key	DSA 2048 bits	Used for DSA signature generation
ECDSA Private Key	ECDSA 224+ curves	Used for ECDSA signature generation

6.5 Definition of Public Keys

The module contains the following public keys:

Table 6-6. Public Keys

Key Name	Type	Description
RSA Public Key	RSA 1024 bits	Used to verify RSA signatures (legacy use)
RSA Public Key	RSA 2048 & 3072 bits	Used to verify RSA signatures
DSA Public Key	DSA 1024 bits	Used to verify DSA signatures (legacy use)
DSA Public Key	DSA 2048 bits	Used to verify DSA signatures
ECDSA Public Key	ECDSA 224+ curves	Used to verify ECDSA signatures
ECDSA Public Key	ECDSA 163+ curves	Used to verify ECDSA signatures (legacy use)

6.6 Definition of CSPs Modes of Access

Table 6-7 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- **G** = Generate: the module generates the CSP.
- **R** = Read: the module reads the CSP. The read access is typically performed before the module uses the CSP.
- **W** = Write: the module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.
- **Z** = Zeroize: the module zeroizes the CSP.

Table 6-7. CSP Access Rights within Roles & Services

Role	Authorized Service	Mode	Cryptographic Key or CSP
User, CO, Manuf	Initialize Update	**R**	SCP03 S-ENC Static Key SCP03 S-MAC Static Key
User, CO, Manuf	Initialize Update	**G**	SCP03 C-MAC Session Key SCP03 R-MAC Session Key SCP03 C-ENC Session Key
User, CO, Manuf	External Authenticate	**R**	SCP03 C-MAC Session Key SCP03 R-MAC Session Key SCP03 C-ENC Session Key Microsoft Minidriver Static Key
CO	Manage Users	**W, Z**	SCP03 S-ENC Static Key SCP03 S-MAC Static Key Microsoft Minidriver Static Key
User, CO	Update Authentication Data	**W**	SCP03 S-ENC Static Key SCP03 S-MAC Static Key Microsoft Minidriver Static Key
User, CO	Put Key	**W**	RSA private keys DSA private keys ECDSA private keys AES keys Triple-DES keys HMAC Keys
User, CO	Read Key	**R**	RSA private keys DSA private keys ECDSA private keys AES keys Triple-DES keys HMAC Keys
User, CO	Delete Key	**Z**	RSA private keys DSA private keys ECDSA private keys AES keys Triple-DES keys HMAC Keys
User, CO	Encrypt / Decrypt	**R**	AES keys Triple-DES keys

Table 6-7. CSP Access Rights within Roles & Services

Role	Authorized Service	Mode	Cryptographic Key or CSP
User, CO	Generate / Verify Signature	**R**	RSA private keys DSA private keys ECDSA private keys AES keys HMAC Keys
User, CO	Compute Message Digest	**N/A**	N/A
User, CO	Generate Key Pair	**G, W**	RSA private keys DSA private keys ECDSA private keys
User, CO, Manuf	Get Info	**N/A**	N/A
User, CO, Manuf	Self-Tests	**R**	RSA private keys DSA private keys ECDSA private keys AES keys Triple-DES keys HMAC Keys
Manuf	Set Status	**Z**	RSA private keys DSA private keys ECDSA private keys AES keys Triple-DES keys HMAC Keys
User, CO, Manuf	Get Authentication Info	**N/A**	N/A
User, CO, Manuf	Cancel Authentication	**Z**	SCP03 C-MAC Session Key SCP03 R-MAC Session Key SCP03 C-ENC Session Key
User, CO	Initialize Algorithm	**R**	RSA private keys DSA private keys ECDSA private keys AES keys Triple-DES keys HMAC Keys
User, CO, Manuf	Generate Random	**N/A**	N/A
User, CO, Manuf	GPIO Command Set	**N/A**	N/A
User, CO, Manuf	File System Command Set	**N/A**	N/A
CO	Set Config	**N/A**	N/A
User, CO, Manuf	Test Command Set	**N/A**	N/A

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the Module does not contain a modifiable operational environment.

8. Security Rules

The module design corresponds to the module's 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.

1. The cryptographic module shall provide three distinct operator roles. These are the Approved User role, the Cryptographic Officer role and the Manufacturer role.
2. The cryptographic module shall provide identity-based authentication.
3. The cryptographic module shall clear previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
5. The cryptographic module shall perform the following tests

   a. Power up Self-Tests

   – Cryptographic algorithm tests

   –Triple-DES Encrypt and Decrypt Known Answer Tests

   –AES Encrypt and Decrypt Known Answer Tests

   –AES CMAC Known Answer Test

   –HMAC-SHA-1, -256 and -512 Known Answer Test

   –DRBG Known Answer Test

   –RSA Sign/Verify Known Answer Test

   –DSA Sign/Verify Known Answer Test

   –ECDSA Sign/Verify Known Answer Test

   – Firmware Integrity Test - 16 bit CRC

   b. Critical Functions Tests: N/A

   c. Conditional Self-Tests

   – Continuous Random Number Generator (RNG) test - performed on NDRNG and DRBG, 128 bits

   – DSA Pairwise Consistency Test

   – RSA Pairwise Consistency Test

   – ECDSA Pairwise Consistency Test
6. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power or resetting the module.
7. Power-up self tests do not require any operator action.
8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

10. There are no restrictions on which keys or CSPs are zeroized by the zeroization method.
11. The module does not support concurrent operators.
12. The module does not support a maintenance interface or role.
13. The module does not support manual key entry.
14. The module does not have any external input/output devices used for entry/output of data.
15. The module does not enter or output plaintext CSPs.
16. The module does not output intermediate key values.

9. Physical Security Policy

9.1 Physical Security Mechanisms

The VaultIC single-chip module has the following physical security mechanisms

- Environmental failure protection (EFP) features for temperature, voltage, internal clock frequency, and duty cycle are provided by immediate reset circuitry.
- The removal-resistant coating with hardness and adhesion characteristics covers the single-chip module, and attempts to peel or pry the coating from the module results in irreparable damage to the module
- The shield removal detection circuitry results in reset upon an attempt to remove the metal coating from the unit
- The removal-resistant coating has solvency characteristics such that dissolving the coating has a high probability of seriously damaging the module

10. Mitigation of Other Attacks Policy

The module has been designed to mitigate against UV light attacks and DPA attacks, which are outside of the scope of FIPS 140-2.

Table 10-1. Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
UV Light Attacks	The module contains a UV light detector that will trigger when the surface of the chip is submitted to a certain cumulative UV light. Once this kind of attack is detected, the device stays under infinite reset even when the light source is removed.	N/A
DPA	It is not feasible to monitor current consumption to determine the value of an algorithm's keys. Current consumption has been designed and tested to be equivalent for both a logic "0" or logic "1".	N/A

Referenced Documents

[1] RSA Laboratories. PKCS#1 v1.5: RSA Cryptography Standard. March 1998.
[2] RSA Laboratories. PKCS#1 v2.1: RSA Cryptography Standard. June 2004.
[3] RSA Laboratories. PKCS#5 v2.0: Password-based Cryptography Standard. Mar 1999
[4] RSA Laboratories. PKCS#7 v1.5: Cryptographic Message Syntax Standard. Nov 1993
[5] RSA Laboratories. PKCS#11 v2.20: Cryptographic Token Interface Standard. Jun 2004
[6] FIPS PUB 46-3. Data Encryption Standard (DES). October 1999.
[7] FIPS PUB 186-3. Digital Signature Standard. June 2009.
[8] FIPS PUB 180-3. Secure Hash Standard. October 2008.
[9] FIPS PUB 140-2. Security requirements for Cryptographic Modules. May 2001.
[10] FIPS PUB 196. Entity authentication using public key cryptography. Feb 1997.
[11] FIPS PUB 197. Advanced Encryption Standard. Nov 2001
[12] FIPS PUB 198. The Keyed-Hash Message Authentication Code (HMAC). March 2002.
[13] ISO9798-2 Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms. July 1999.
[14] ISO9797-1. Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher, 1999
[15] ISO7816-3. Integrated Circuit Cards - Part 3: Cards with contacts: Electrical interface and transmission protocols. Dec 2004.
[16] ISO7816-4. Integrated Circuit Cards - Part 4: Organization, security and commands for interchange. Sept 2004.
[17] RFC 2459. Internet X509 Public Key Infrastructure Certificate and CRL profile Jan 1999
[18] RFC 4226. HOTP: An HMAC-Based One-Time Password Algorithm. Dec 2005
[19] ANSI X9.19
[20] ANSI X9.31. Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA). 1998.
[21] ANSI X9.62. Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©. 1998.
[22] Philips® - THE I^{2}C-BUS SPECIFICATION VERSION 2.1 - January 2000
[23] Universal Serial Bus Specification Revision 2.0. April 2000
[24] DWG - Specification for USB Integrated Circuit(s) Card Devices Revision 1.0. April 2005
[25] DWG - Specification for Integrated Circuit(s) Cards Interface Devices Revision 1.1 April 2005
[26] GlobalPlatform. Card specification v2.2. March 2006.
[27] GlobalPlatform. Secure Channel Protocol 03 - Card Specification v2.2 Amendment D - February 2009
[28] Handbook of Applied Cryptography. ISBN: 0-8493-8523-7. Oct. 1996.
[29] INSIDE Secure. 6528B Secure your embedded devices - February 2011.
[30] Microsoft® - Smart Card Minidriver Specification for Windows® Base Cryptographic Service Provider (Base CSP) and Smart Card Key Storage Provider (KSP) Version 5.07 - Sept 2007
[31] NIST SP 800-89 - Recommendation for Obtaining Assurances for Digital Signature Applications - November 2006
[32] NIST SP 800-108 - Recommendation for Key Derivation Using Pseudorandom Functions, November 2008
[33] NIST SP 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication - May 2005
[34] NIST SP 800-63 - Electronic Authentication Guideline - April 2006
[35] NIST SP 800-90 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators - March 2007

Definitions and abbreviations

AES	Advanced Encryption Standard algorithm as defined in FIPS PUB 197 [11]
Authentication	An identification or entity authentication technique assures one party (the verifier), through acquisition of corroborative evidence, of both the identity of a second party involved, and that the second (the claimant) was active at the time the evidence was created or acquired. (From Handbook of Applied Cryptography [28])
Authenticity	The property that data originated from its purported source.
ASSP	Application Specific Standard Product
Brute force attack	Hacking technique that consist in trying every character combination to guess a password.
CBC	Cipher Block Chaining method applied to block ciphers
CFB	Cipher Feedback Register chaining method applied to block ciphers
CMAC	Cipher-based Message Authentication Code
CPU	Central Processing Unit
Cryptographic key	A bit string used as a secret parameter by a cryptographic algorithm. To prevent a key from being guessed, keys need to be generated truly randomly and contain sufficient entropy.
DES	Data Encryption Standard algorithm as defined in FIPS PUB 46-3 [6]
Device	Any CPU with master or slave capability
DRBG	Deterministic Random Bit Generator as defined in SP 800-90 [35]
Dictionary attack	Hacking technique that consist in trying commonly used passwords to guess a password.
DSA	Digital Signature Algorithm as defined in FIPS PUB 186-3 [7]
ECB	Electronic Code Book chaining method applied to block ciphers
ECDSA	Elliptic Curves DSA as defined in FIPS PUB 186-3 [7]
FIPS	Federal Information Processing Standards
FIPS-Approved	An algorithm or technique that is specified or adopted in FIPS.
HMAC	Hash-based Message Authentication Code as defined in FIPS PUB 198 [12]
Host	Entity that communicates (directly or not) with the device.
HOTP	HMAC-based One Time Password algorithm as defined in RFC 4226 [18]
Integrity	The property that received data has not been altered
ISO7816	Smart Card interface
MAC	Message Authentication Code - A bit string of fixed length, computed by a MAC generation algorithm, that is used to establish the authenticity and, hence, the integrity of a message.
Master	The device that initiates and terminates a transmission. The Master also generates the clock for synchronous interface.
NIST	National Institute of Standards and Technology
OFB	Output Feedback Register chaining method applied to block ciphers

OS	Operating Systems
PKI	Public Key Infrastructure
Receiver	The device reading data from the bus
RSA	Rivest Shamir Adleman algorithm
Seed	(pseudo-)random number
SCP	Secure Channel Protocol as defined by GlobalPlatform v2.2 [27]
SHA	Secure Hash Algorithm as defined in FIPS PUB 180-3 [8]
Slave	The device addressed by a master
SPI	Serial Protocol Interface
Strong Authentication	Exchange of messages during which a claimant proves its identity to a verifier by demonstrating its knowledge of a secret but without revealing it
Transmitter	The device placing data on the bus
TWI / I^2C	Two Wire Interface and Inter Integrated Circuit Bus respectively
USB	Universal Serial Bus as defined in USB 2.0 standard [23]

Headquarters

INSIDE Secure
41, Parc Club du Golf
13586 Aix-en-Provence Cedex 3
France
Tel: +33 (0)4-42-39-63-00
Fax: +33 (0)4-42-39-63-19

Product Contact

Web Site
www.insidesecure.com

Technical Support
e-security@insidefr.com

Sales Contact
sales_web@insidefr.com