# gemalto

# LEVEL 3 NON-PROPRIETARY SECURITY POLICY FOR

# ProtectServer Internal Express 2 (PSI-E2)

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF APPENDICES

# 1. INTRODUCTION

## 1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the ProtectServer Internal Express 2 (PSI-E2). This security policy describes how the PSI-E2 meets the security requirements of FIPS 140-2 and how to operate the PSI-E2 in a secure FIPS 140-2 mode. This policy was prepared as a part of the Level 3 FIPS 140-2 validation of the PSI-E2.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 - *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST web site at http://csrc.nist.gov/groups/STM/cmvp/index.html.

## 1.2 References

This document deals only with operations and capabilities of the PSI-E2 in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the PSI-E2 and other Gemalto products from the following sources:

- The Gemalto internet site contains information on the full line of security products at https://safenet.gemalto.com/data-encryption/hardware-security-modules-hsms/protectserver-security-module/

- For answers to technical or sales related questions please refer to the contacts listed on the Gemalto internet site at https://safenet.gemalto.com/contact-us/

| Gemalto Contact Information: | |
| --- | --- |
| **Gemalto (Corporate Headquarters)** | 4690 Millennium Drive<br>Belcamp, MD 21017<br><br>**Telephone:** 410-931-7500<br>**TTY Users:** 800-735-2258<br>**Fax:** 410-931-7524 |
| **Gemalto (Ottawa)** | 20 Colonnade Road<br>Suite 200<br>Ottawa, Ontario<br>K2E 7M6<br><br>**Telephone:** +1 613 723 5077<br>**Fax:** +1 613 723 5079 |
| **Gemalto Sales:** | |
| **U.S.** | (800) 533-3958 |
| **International** | +1 (410) 931-7500 |
| **Gemalto Technical Support:** | |
| **U.S.** | (800) 545-6608 |
| **International** | +1 (410) 931-7520 |

| Gemalto Customer Service: | |
|---|---|
| **U.S.** | (866) 251-4269 |
| **EMEA** | +44 (0) 1276 60 80 00 |
| **APAC** | 852 3157 7111 |

## 1.3 Terminology

In this document the Gemalto ProtectServer Internal Express 2 card is referred to as the PSI-E2, the adapter, or the module.

## 1.4 Document Organization

This document provides an overview of the PSI-E2 and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the PSI-E2.  Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

## 2. THE PSI-E2 CARD

### 2.1 Cryptographic Module Specification

The Gemalto PSI-E2 is a cryptographic module is a multi-chip embedded hardware cryptographic module in the form of a PCI-Express card that provides a wide range of cryptographic functions using firmware and dedicated hardware processors.  This document refers specifically to PSI-E2 hardware version VBD-05, Version Code 0200 with Firmware Version 5.03.01 and 5.03.02.
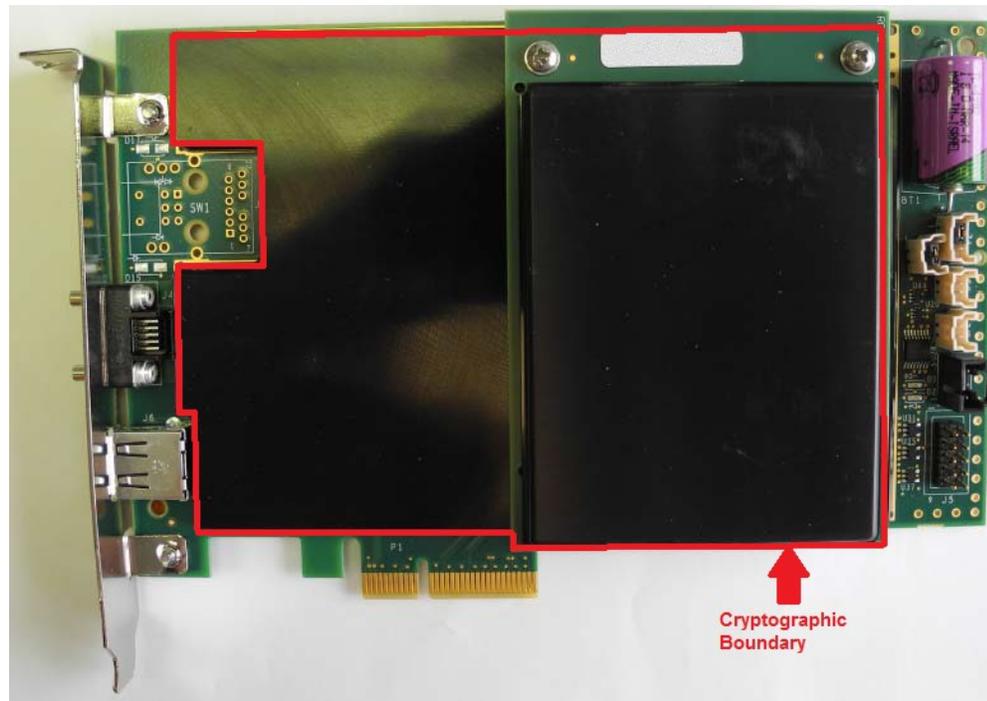


Figure 2-1  ProtectServer Internal Express 2 Card

The module, running Gemalto's Cprov firmware, implements the Cryptoki cryptographic API as defined by RSA Data Security. While certain Cryptoki features are not supported, the module does provide a comprehensive compliance to the PKCS#11 standard as well as vendor-specific extensions.

The cryptographic boundary for this module includes the metal cover enclosure that is outlined in red above, under which a hard epoxy coating is protecting the PCB. This boundary encapsulates the Data Ciphering Processor (DCP), embedded processor, SDRAM memory chips, and the Real Time Clock (RTC). The battery, battery isolation link, and external alarm input link are excluded from the FIPS 140-2 security requirements.

The module provides key management (e.g., generation, storage, deletion, and backup), an extensive suite of cryptographic mechanisms, and process management including separation between operators. The PSI-E2 also features non-volatile tamper protected memory for key storage, a hardware random number generator, and an RTC.

The FIPS 140-2 cryptographic boundary is defined by the perimeter of the protection covers.

The PSI-E2 meets all level 3 requirements for FIPS 140-2 as summarized in Table 2-1.

| 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 Machine | 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 |

Table 2-1  FIPS 140-2 Security Levels

## 2.2    Cryptographic Module Ports and Interfaces

The PSI-E2 has the following physical interfaces:

- A standard PCI Express bus interfacing to the motherboard of the host machine;
- One USB serial connector;
- One Luna Remote PED connector (not used);
- One external battery isolation connector; and
- One External tamper input.

The PSI-E2 provides a tightly secured cryptographic element. All requests for services sent to the adapter over the PCI bus or the serial ports are captured by the adapter's processor, which controls the level of access to the on-board cryptographic services and the keys. The adapter's processor also responds to PKCS #11 commands, ensuring that during FIPS operation only authenticated users receive cryptographic services.

The module's physical interfaces are separated into the logical interfaces, defined by FIPS 140-2,

and described in Table 2-2:

| FIPS 140-2 Logical Interfaces | Adapter Physical Interfaces |
|---|---|
| Data Input Interface | PCI Bus, USB Serial port |
| Data Output Interface | PCI Bus, USB Serial port |
| Control Input Interface | PCI Bus, External tamper input |
| Status Output Interface | PCI Bus |
| Power Interface | PCI Bus, External battery isolation connector |

Table 2-2  FIPS 140-2 Logical Interfaces

## 2.3    Roles, Services, and Authentication

The PSI-E2 supports identity-based authentication of its operator. Operators are identified by a token name and PIN. The different roles and required authentication are shown in Table 2-3.

| Operator | Role | Type of authentication | Authentication Data |
|---|---|---|---|
| Administrator SO | Crypto Officer | Identity Based | Operator Unique PIN |
| Administrator | User | Identity Based | Operator Unique PIN |
| Token SO | Crypto Officer | Identity Based | Operator Unique PIN |
| Token User | User | Identity Based | Operator Unique PIN |
| Audit User | User | Identity Based | Operator Unique PIN |

Table 2-3  Roles and Required Identification and Authentication

The PSI-E2 supports three types of Tokens: one Administration Token, multiple Cprov Tokens and one or more Smart Card Tokens. All Tokens have two operators: a Security Officer (SO) and a User.  For the Administration Token, the Administrator SO is the FIPS 140-2 Crypto Officer and the Administrator is the User. For all other Tokens, the Token SO is the FIPS 140-2 Crypto Officer and the Token User is the User.

The operator explicitly selects a role when logging in by selecting a PKCS#11 Token and nominating either User or SO Role.  The adapter provides restricted services to an operator based on the role to which the operator authenticated. There is only one operator assigned to each role. The Administrator SO and Token SO perform FIPS 140-2 Crypto Officer roles while the Administrator and Token User performs a FIPS 140-2 User role.

The PSI-E2 enforces a minimum PIN length of 4 characters and a maximum PIN length of 32 characters.  The module allows the PIN character to be any value but the software typically used with the module restricts the dictionary to the ANSI C character set.  This character set provides for 92 visible characters which, with a 4 character PIN, provides a probability of less than one in 1,000,000 that a random PIN attempt (e.g., guess) will succeed (actual probability is approximately 1/71,600,000). The module is protected from brute force PIN attacks by imposing an increasing delay for every failed PIN attempt after the first three failed attempts. The initial delay is 5 seconds and increases by an additional 5 seconds for each subsequent failed attempt, e.g., 3 fails causes a 5 second delay; 4 fails causes a 10 second delay; 5 fails causes a 15 second delay; etc.

### 2.3.1  Services for Authorized Roles

Table 2-4 lists the services related to each authorized role within the adapter:

| Role | Services |
|---|---|
| Administrator SO | Initialize Administrator Token User PIN |
| Administrator | Manage Adapter and Administrator Token |
| Token SO | Manage Token |
| Token User | Use Token and manage token keys |
| Unauthenticated operator | Unauthenticated services |
| Audit User | Manage Audit Key and logs |

Table 2-4  Types of Available Services

All services listed in Sections 2.3.1 through 2.3.6 can be accessed in FIPS and non-FIPS mode.  The services listed in Sections 2.3.1 through 2.3.6 use the security functions listed in Table 2-7, Table 2-8, Table 2-9, and Table 2-10.  When the module is operating in FIPS-approved mode as described in Section 3, the Non-FIPS Approved key derivation mechanisms in Table 2-10 are disabled and cannot be used for these services.  The non-Approved functions in Table 2-10 can only be accessed through the services when the module is in non-FIPS Approved mode.

### 2.3.2  Administrator Security Officer

The primary role of the Administrator Security Officer (ASO) is to introduce the Administrator to the system. The ASO is able to set the initial Administrator PIN value but is not able to change the administration PIN after it is initialized. The ASO can perform the following services:

- Set the initial Administrator PIN value (may not change it later);

- Set the CKA_TRUSTED attribute on a Public object in the Administrator Token;

- Set the CKA_EXPORT attribute on a Public object in the Administrator Token;

- Manage Host Interface Master Keys;

- Exercise cryptographic services with Public objects

- Create, destroy, import, export, generate, and derive[1] Public objects;

- May change his/her own PIN;

- Read the Hardware Event Log;

- May modify Monotonic Counter object[2] and

---

[1] Key Derive operations are listed in Table 2-9.

[2] Monotonic counter objects represent hardware counters which exists on the device. The counters are incremented sequentially each time it is read. There is only one monotonic counter per token.

- Power-up self-test on demand.

### 2.3.3 Administrator

The Administrator is responsible for the overall security management of the adapter. Token Security Officers and Slots are controlled by the Administrator. The following services are available to the Administrator:

- Set or Change RTC value[3];

- Read the Hardware Event Log;

- Purge a full Hardware Event Log;

- Configure the Transport Mode feature[4];

- Specify the Security Policy of the adapter;

- Create new Cprov Slots/Tokens and specify their Labels, SO PINs, and minimum PIN Length;

- Initialize smart cards and specify their Labels and SO PINs;

- Destroy individual Cprov Slots/Tokens;

- Zeroize all adapter Secure Memory including all PINs and User Keys;

- Perform Firmware Upgrade Operation;

- Manage Host Interface Master Keys;

- Exercise cryptographic services with Public objects on Administrator Token;

- Exercise cryptographic services with Private objects on Administrator Token;

- Create, destroy, import, export, generate, and derive Public objects on Administrator Token;

- Create, destroy, import, export, generate, and derive Private objects on Administrator Token;

- May change his/her own PIN; and

- Power-up self-test on demand.

### 2.3.4 Token SO

The Token SO is responsible for granting and revoking ownership of the token. If the Token does not have a User PIN, the Token SO should initialize it by assigning the Label and User PIN.  The token SO may also revoke the Token User's privileges (and possibly reassign the token to another operator) but only by destroying all the key material of the original operator first.  The following services are available to the Token SO:

- Set the initial User PIN value (may not change it later)

- Reset (re-initialize) the Token (destroys all keys and User PIN on the Token) and set a new Label

- Set the CKA_TRUSTED attribute on a Public object in his or her Token

- Set the CKA_EXPORT attribute on a Public object in his or her Token

---

[3] The clock on the module can be synched to the host where it is installed.
[4] Transport Mode allows removal of HSM from the PCI slot. The removal can be single time or continuous for storage. This feature depends upon the battery backup.

- Exercise cryptographic services with Public objects in his or her Token;

- Create, destroy, import, export, generate, and derive Public objects in his or her Token

- May change his/her own PIN;

- May modify Monotonic Counter object; and

- Power-up self-test on demand.

### 2.3.5  Token User

Token users may manage and use private and public keys on their own tokens.  The following services are available to the Token User:

- Exercise cryptographic services with Public objects in his or her Token;

- Exercise cryptographic services with Private objects in his or her Token;

- Create, destroy, import, export, generate, derive Public objects in his or her Token;

- Create, destroy, import, export, generate, and derive Private objects in his or her Token;

- May change his/her own PIN; and

- Power-up self-test on demand.

### 2.3.6  Unauthenticated Operators

Certain services are available to operators who have not (yet) authenticated to the adapter:

- Exercise status querying services;

- Authenticate to a Token; and

- Force session terminate, restart adapter by setting a register which is memory mapped to the PCI bus. The host application can force a restart by writing a certain value to the register through the PSI-E2 device driver.  The transparent PCI chip will then generate a bus cycle restart which in turn will restart the adapter.

All of the services available to the Unauthenticated Operators are also available to all authenticated operators.

### 2.3.7  Audit User

The AuditUser role is present on the Admin Token and can be initialized by the AdminSO role. The responsibility of this role is limited to:

- Create/Destroy AUDIT_KEY; and
- Verify the generated audit logs.

### 2.4     Physical Security

The adapter provides tamper evidence and tamper response mechanisms.  A metal casing covers the epoxy-covered PCB board.  The epoxy provides a strong tamper evident enclosure. The Administrator should perform routine visual inspection of the module for evidence of tamper such as scratches.

The module is actively protected through a combination of an external tamper jumper switch and a voltage monitor. The PSI-E2 protection can also be activated by removal of the adapter from the host machine or via an external alarm input capability. In the event of a tamper the PSI-E2 enters a Tamper state in which all processing is halted and the Non-Volatile secure memory is zeroized.

Hardness testing of the epoxy was performed from a low of -50° to +60° Celsius. No assurance is provided for Level 3 hardness conformance at any other temperature.

### 2.5     Operational Environment

This section does not apply. The PSI-E2 does not provide a modifiable operational environment.

### 2.6     Cryptographic Key Management

The PSI-E2 is a general-purpose cryptographic management device and thus securely administers both cryptographic keys and other critical security parameters (CSPs) such as passwords.

#### 2.6.1  Key Generation

The PSI-E2 Module supports the generation of DSA, RSA, ECDSA (also known as ECC), and DH public and private keys. The module also supports the generation of three-key Triple-DES keys as well as AES 128-bit, 192-bit, and 256-bit keys.  The module implements a FIPS approved AES-CTR DRBG specified in NIST SP 800-90A. ECDH is supported for key derivation functions.

#### 2.6.2  Key Access / Storage

All keys except module specific keys are stored in one of three media.

Flash memory is used to store encrypted keys, plaintext keys are stored either in Volatile RAM or in tamper responding secure memory (battery-backed RAM). The module prevents physical access all these media through the physical security mechanisms discussed in section 2.4. Logical access to keys and other CSPs is restricted to authenticated operators with valid permissions. The communication to the module including key generation and key creation is performed over a Three Key Triple DES encrypted trusted channel and the module only allows keys to be output if they are wrapped using a FIPS Approved algorithm.

Table 2-5 outlines all the keys stored by the module.

| CSP | CSP Type | Generation | Input/Output | Storage | Destruction Mechanism | Use |
|---|---|---|---|---|---|---|
| Firmware upgrade Public Key | 2048 bit RSA | FIPS 186-4 RNG | Not input/output | Plaintext in Flash | None | To verify the signature attached to a new firmware image. Generation done at manufacture. |
| Default Administrator Token SO PIN | PIN | N/A | Not input/output | Plaintext in Flash | Replaced as part of the initialization process | For initial authentication to the module. Replaced after the module is initialized. |
| DH Key Agreement Keys | 2048, 3072 and 4096 - bit Modulus Size | Private Component Generated Via FIPS approved RNG; Public Value Computed via Diffie-Hellman | Public key exported as part of key agreement | Working memory | Power cycle, tamper, or C_DestroyObject() API | To establish an encrypted channel between an operator and the module. |
| Message Encryption Shared Secret  Key | 3-key Triple-DES | Established via DH | Not input/output | Working memory | Power cycle, tamper, or C_DestroyObject() API | Protects data between an operator and the module. Triple-DES is used to protect the secure channel established using DH. |
| Message Authentication Key | HMAC-SHA-1 | Established via DH | Not Input/Output | Working memory | Power cycle, tamper, or C_DestroyObject() API | Provide data authentication of encrypted data between an operator and the module. |
| Operating PINs | PIN | N/A | Input encrypted[5] | Obfuscated with MMK | Tamper or Zeroize command (ctconf –x) or C_DestroyObject() API | All users' PINs – Administrator Token SO, Administrator Token User, Token SOs, and Token users used to authenticate to the module. |
| Module Master Key | 3-key Triple-DES | FIPS Approved RNG | Not input/output | Tamper responsive memory in NVRAM of RTC | Tamper or Zeroize command (ctconf –x) | Obfuscates other keys and zerorizes contents of secure memory on object deletion. |

---

[5] PINs encrypted using Triple-DES

| CSP | CSP Type | Generation | Input/Output | Storage | Destruction Mechanism | Use |
|---|---|---|---|---|---|---|
| ECDH Key Agreement Keys | ECDH (P224-P521) | Private Component Generated Via FIPS approved RNG; Public Value Computed via Diffie-Hellman | Public key exported as part of key agreement | Working memory | Power cycle, tamper, or C_DestroyObject() API | User-created keys for use by user applications |
| D-H Key Agreement Keys | 2048-4096 bit Modulus Size | Private Component Generated Via FIPS approved RNG; Public Value Computed via Diffie-Hellman | Public key exported as part of key agreement | Working memory | Power cycle, Tamper, Zeroize command (ctconf –x) or C_DestroyObject() API | User-created keys for use by user applications for key agreement |
| Secret Key | 3-Key Triple-DES, AES 128, 192 and 256 bit | Established via ECDH, DH, transported using RSA or Secret Key or generated by FIPS approved RNG | Encrypted[6] or split knowledge | Working memory or Secure Memory obfuscated with MMK | Power cycle, Tamper, Zeroize command (ctconf –x) or C_DestroyObject() API | User-created keys for use by user applications for Encryption, Decryption, or Signature Verification/Generation and key wrapping/unwrapping |
| RSA Public/Private Keys | 2048, 3072 bit RSA | FIPS 186-4 | Public key exported | Working memory or Secure Memory obfuscated with MMK | Power cycle, Tamper, Zeroize command (ctconf –x) or C_DestroyObject() API | User-created keys for use by user applications for Signature Generation/Verification |
| DSA Public/Private Keys | 2048 – 4096 bit DSA | FIPS 186-4 | Public key exported | Working memory or Secure Memory obfuscated with MMK | Power cycle, Tamper, Zeroize command (ctconf –x) or C_DestroyObject() API | User-created keys for use by user applications for encryption, Decryption, and Signature Generation/Verification |
| ECDSA Public/Private Keys | 224 – 512 bit ECDSA | FIPS 186-4 | Public key exported | Working memory or Secure Memory obfuscated with MMK | Power cycle, Tamper, Zeroize command (ctconf –x) or C_DestroyObject() API | User-created keys for use by user applications for encryption, Decryption, Key wrapping/Unwrapping and Signature Generation/Verification |

---

[6] Token Keys encrypted using AES or Triple-DES Application Keys

| CSP | CSP Type | Generation | Input/Output | Storage | Destruction Mechanism | Use |
|---|---|---|---|---|---|---|
| DRBG Seed | 384 bits | H/W RNG | Not input/output | Not permanently stored | Power cycle or tamper | Used as part of the RNG process. |
| DRBG V | 128 bits | Hardware Random Source | Not input or output | Not permanently stored | Power cycle or tamper | Part of the secret state of the approved DRBG. The value is generated using the methods described in NIST SP 800-90A. |
| DRBG Key | AES-256 | Hardware Random Source | Not Input or Output | Not permanently stored | Power cycle or tamper | 32 bytes AES key stored in the RAM. Used in an implementation of the NIST SP 800-90A CTR (AES) DRBG. |
| DRBG Entropy Input | 384 bits | Hardware Random Source | Not Input or Output | Not permanently stored | Power cycle or tamper | The 384-bit entropy value used to initialize the approved DRBG. |

Table 2-5  List of Keys Stored in Module

Table 2-6 outlines the access that "Authorized Services" (see Table 2-4) have to the keys listed in Table 2-5. Here 'R' stands for "Read", 'W' stands for "Write", X stands for "Execute" and "Z" stands for "Zeroize".

| | FW Upgrade Cert | Default Administrator Token SO PIN | DH / ECDH Ephemeral Keys | Key Agreement Keys | Message Authentication Key | Operating PINs | Token Keys (Public) | Token Keys (Private) | DRBG | Module Master Key |
|---|---|---|---|---|---|---|---|---|---|---|
| Initialization | - | - | - | X | - | WX | - | - | - | W |
| Administrator SO | WX | WX | - | WXZ | - | WXZ | RWXZ | RWXZ | - | RWXZ |
| Administrator | - | - | WZ | X | WZ | WXZ | - | - | - | RWXZ |
| Token SO | - | - | RXZ | X | RXZ | X | - | - | - | - |
| Token User | - | - | RXZ | X | RXZ | X | XZ | XZ | XW | - |
| Unauthenticated Operators | - | - | - | - | - | X | - | - | - | - |

Table 2-6  Access to Keys for Authorized Services

Please note that the FW Upgrade Cert is never zeroized because it is a public key. The Default Administrator Token SO PIN is never zeroized because it's a pre-initialization value. The DRBG Seed is zeroized when a tamper event is detected or overwritten when the module is restarted. All other CSPs/Keys identified in Table 2-5 are zeroized by a call to C_DestroyObject() API by the respective role or through a tamper event.

### 2.6.3 Security Functions

The PSI-E2 supports a wide variety of security functions. FIPS 140-2 requires that only FIPS Approved algorithms be used whenever there is an applicable FIPS standard.

Table 2-7 lists the PSI-E2 FIPS Approved security functions. In the FIPS mode of operation these Approved security functions are available.

| FIPS Approved Security Function | Firmware | SafeXcel-3120 | SafeXcel-1746 |
|---|---|---|---|
| **AES**<br>*ECB, CBC, OFB, KW, KWP, CMAC, GCM (The module generates IVs internally using the Approved DRBG which are at least 96-bits in length)*<br>*(Key Size = 128, 192, 256)* | *5571* | *n/a* | *n/a* |
| **AES**<br>*ECB, CBC*<br>*(Key Size = 128, 192, 256)* | *n/a* | *4849* | *4960* |
| *KTS (AES Cert. #5571; key establishment methodology provides between 128 and 256 bits of encryption strength)* | *5571* | *n/a* | *n/a* |
| **DSA**<br>*Parameter Generation [2048,3072],*<br>*Key Generation [2048,3072],*<br>*Signature Generation [2048,3072],*<br>*Signature Verification [1024,2048,3072]* | *1434* | *n/a* | *n/a* |
| **ECDSA**– *Only NIST Recommended Curves*<br>*Key Generation, Signature Generation, Signature Verification*<br>*Curves: P-224, P-256, P-384, P-521* | *1503* | *n/a* | *n/a* |
| **RSA**<br>*Key Generation [2048], Signature Generation [2048,3072],Signature Verification [1024,2048,3072]* | *2998* | *n/a* | *n/a* |
| **KAS (FFC)**<br>*dhEphem, dhOneFlow* | *192* | *n/a* | *n/a* |
| *SHA-1, SHA-224, SHA-256, SHA-384, SHA-512* | *4476* | *n/a* | *n/a* |
| *SHA3* | *57* | *n/a* | *n/a* |
| *HMAC: SHA1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512* | *3713* | *n/a* | *n/a* |
| **Triple-DES**<br>*ECB, CBC, KW, OFB* | *2807* | *n/a* | *n/a* |
| **Triple-DES**<br>*ECB, CBC* | *n/a* | *n/a* | *2573* |

| KTS (Triple-DES Cert. #2807 ; key establishment methodology provides 112 bits of encryption strength) | 2807 | n/a | n/a |
|---|---|---|---|
| **DRBG** <br> NIST SP 800-90A DRBG (CTR) AES-256 | n/a | 1704 | n/a |
| **CKG** | Vendor Affirmed (Resulting Symmetric keys and seeds used for asymmetric key generation are an unmodified output from the Approved DRBG.) | | |

Table 2-7  FIPS Approved Security Functions

Table 2-8 lists the PSI-E2 Non-Approved but FIPS allowed security functions. In the FIPS mode of operation

| **Non-Approved FIPS but Allowed Security Functions** |
|---|
| AES (Cert. #5571, key unwrapping; key establishment methodology provides  between 128 and 256 bits of encryption strength) |
| Triple-DES (Cert. #2807, key unwrapping; key establishment methodology provides 112 bits of encryption strength) |
| Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength) |
| RSA (key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength) |
| EC Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength) |
| NDRNG[7] |

Table 2-8  Non-Approved FIPS Allowed Security Functions

Table 2-9 lists the PSI-E2 key derivation mechanisms that are non-Approved but Allowed in FIPS mode.

| **MECHANISMS FOR SPLIT KNOWLEDGE ENTRY/OUTPUT OF KEY** <br> **(Allowed in FIPS Mode)** |
|---|
| CKM_SECRET_SHARE_WITH_ATTRIBUTES |

Table 2-9  Non-Approved FIPS Allowed Key Derivation Mechanisms

Table 2-10 lists the PSI-E2 key derivation mechanisms that are non-Approved and not Allowed in FIPS mode. These key derivation mechanisms are actively disabled by the module when operating in FIPS mode.

---

[7] This is being built-in 3120 SafeExcel module. The estimated amount of entropy provided by the NDRNG is 4 bits per each byte of data

| NON-ALLOWED DERIVATION METHODS (Disabled in FIPS Mode) |
| :--- |
| CKM_DES3_DERIVE_CBC |
| CKM_DES3_DERIVE_ECB |
| CKM _SHAxxx_KEY_DERIVATION |
| CKM_SSL3_KEY_AND_MAC_DERIVE |
| CKM_SSL3_MASTER_KEY |
| CKM_EXTRACT_KEY_FROM_KEY |
| CKM_CONCATENATE_BASE_AND_KEY |
| CKM_XOR_BASE_AND_DATA |
| CKM_XOR_BASE_AND_KEY |

Table 2-10  Non-Approved Key Derivation Mechanisms

## 2.7    Self-Tests

The PSI-E2 Module performs a number of power-up and conditional self-tests to ensure proper operation.

### 2.7.1  Power-Up Self-Tests

When the module is initially powered-on, each cryptographic library in the module executes its own battery of power-up self-tests.  If any of the power-up self-tests fail in any of the cryptographic library implementations, the module will enter an error state and prohibit an operator from exercising the module's cryptographic functionality. Table 2-11 lists the power-up self-tests:

| Test | Function | Where Performed | FIPS 140-2 Required |
| :--- | :--- | :--- | :--- |
| Secure Memory File System Integrity | Initializes and checks the module's secure memory file system | Firmware | No |
| DRBG KAT | Performs a known answer test for the AES CTR DRBG. | SafeXcel-3120 | Yes |
| Symmetric Cipher KATs | Performs known answer tests for AES, Triple-DES, CAST, IDEA, RC2, DES, and RC4 operations (encrypt/decrypt) | Firmware, SafeXcel-3120, SafeXcel-1746 (AES)<br><br>Firmware, SafeXcel-1746 (Triple-DES) | AES and Triple-DES |

| Test | Function | Where Performed | FIPS 140-2 Required |
|------|----------|-----------------|---------------------|
| MAC and HMAC KATs | Performs known answer tests for CAST MAC, IDEA MAC, RC2 MAC, DES MAC and Triple-DES MAC. Performs known answer tests for MD5 HMAC, HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, RMD128 HMAC and RMD160 HMAC. | Firmware | HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 |
| Asymmetric Cipher KATs | Performs known answer tests for RSA operations (sign and verify, encrypt/decrypt). | Firmware | Yes |
| Asymmetric Key Derive KATs | Performs known answer tests for ECDH Derive | Firmware | No |
| Asymmetric Pairwise Consistency Test | Performs a pairwise consistency test on a DH key pair | Firmware | No |
| DH X9.42 Parameter Verification KAT | Performs a known answer test on DH X9.42 Parameter Verification algorithm | Firmware | Yes |
| DH X9.42 Pairwise Consistency Test | Performs a pairwise consistency test on a random DH X9.42 key pair | Firmware | Yes |
| DH X9.42 ASN1 KDF KAT: CS_DA_SHA1 | Known answer Test of ASN1 KDF | Firmware | Yes |
| DH X9.42 Concatenate KDF KAT: CS_DA_SHA1 | Known answer Test of Concatenate KDF | Firmware | Yes |
| Sign/Verify | Known Answer signature/verification tests for RSA, DSA and ECDSA. | Firmware | Yes |
| Message Digest KATs | Verifies known message/hash pairs for MD2, MD5, RMD128, RMD 160, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 and SHA-3 | Firmware | SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 SHA-3 |
| Software/Firmware Integrity | Ensures that the software/firmware on the module has not been modified / damaged by calculating a SHA-1 hash over all software/firmware components and comparing the result to a known good result. | Firmware | Yes |

Table 2-11  Power-up Self-Tests

**2.7.2 Conditional Self-Tests**

The module performs conditional self-tests as outlined in Table 2-12.

| Test | Function | Where Performed | FIPS 140-2 Required |
|---|---|---|---|
| Pairwise Consistency | Runs a pairwise consistency check each time the module generates a DSA, RSA, ECDSA, or DH public/private key pair. | Firmware | DSA, RSA, ECDSA |
| Continuous HW RNG | Performs the FIPS 140-2 required continuous RNG check each time the module's Hardware RNG is used to produce random data. | SafeXcel-3120 | Yes |
| Continuous RNG | Performs the FIPS 140-2 required continuous RNG check each time the module's RNG is used to produce random data. | Firmware | Yes |
| Firmware Load | Checks that the firmware to be loaded is verified with a digital signature. If the signature cannot be verified, the module will report an error and the firmware will not be loaded. The verification algorithm used is RSASSA-PKCS-v1_5 using SHA512 and 2048 bit key. **Note:** Following a successful verification, all keys and CSPs will first be zeroized and then the firmware will be updated A firmware upgrade in FIPS mode will reset the HSM to factory default state, forcing the user to re-initialize the module, enable the FIPS mode and re-load the cryptographic keys. | Firmware | Yes |

Table 2-12  Conditional Self-Tests

**2.8      Mitigation of Other Attacks**

The PSI-E2 does not employ any technology specifically intended to mitigate against other attacks.

# 3.  FIPS APPROVED MODE OF OPERATION

**3.1      Description**

The PSI-E2 allows its administrators the choice of employing a wide range of security technologies.  To comply with FIPS mode of operation the PSI-E2 must be configured in a secure manner.  This includes:

- Operation with FIPS Approved algorithms as listed in Table 2-7, Non-Approved but FIPS allowed algorithms as listed in Table 2-8 and Table 2-9;

- Not permitting the export of clear keys;

- In accordance to SP 800-67Rev2, the firmware implements a counter to ensure the same Triple-DES keys used for encryption are not utilized more than $2^{28}$ operations.

- Locking the security mode to prevent circumvention of the mode setting;

- Not permitting PINs to be used in clear;

- Not permitting changes to the PSI-E2 firmware without first clearing all protected keys and CSPs; and

- Providing authentication and session management security.

This Security Policy describes a particular PSI-E2 firmware and hardware. The PSI-E2 firmware can be replaced (with a firmware upgrade operation) or extended (by loading Functionality Modules [FMs]). Operators can load their own trusted code into the module. However, by doing so, the module is no longer FIPS validated unless the FM has been separately FIPS validated.

The PSI-E2 checks that new firmware is digitally signed before it can be loaded. Following a successful verification all keys and CSPs will be zeroized. After the zeroization, the PSI-E2 will automatically transition to a non-FIPS mode and will require reconfiguration to return to FIPS mode.

### 3.2    Invoking Approved Mode of Operation

An operator may easily place the PSI-E2 in "FIPS mode" by simply running the administrative `CTCONF -fF` command from the remote management facility. Once this command is executed the PSI-E2 will reject all requests for non-FIPS algorithms or configurations. Please note that the operator has to be logged in as an Administrator to invoke the FIPS mode of operation.

### 3.3    Mode of Operation Indicator

Running the display status command from a remote management facility will return a status displaying the current PSI-E2 operating mode.

```
Security Mode: FIPS 140-2 Mode: <list of flags indicating attributes set for FIPS>
```

When the module is not running in FIPS mode, this status displays as:

```
Security Mode:
```

### 3.4    Invoking Mode of Operation Indicator

An operator may easily view the current PSI-E2 mode of operation by simply running the administrative `CTCONF -v` command from the remote management facility. Once this command is executed the PSI-E2 will respond with full details of the adapter configuration. The configuration details include details of the firmware loaded and a listing of the adapter security mode flags one of which indicates that the module is in the FIPS mode of operation.

## 4.  DESIGN ASSURANCE

### 4.1    Distribution and Delivery of Module

The module is shipped in an anti-static shipping envelope that is sealed with a Gemalto security sticker and placed inside a Gemalto shipping box. The user should inspect the product shipping boxes to make sure they have not been tampered with or damaged upon receiving the modules, which could indicate a security compromise.

# APPENDIX A.   CRONYMS AND ABBREVIATIONS

| Acronym | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| AK | Application Key |
| ANSI | American National Standards Institute |
| API | Application Programming Interface |
| ARIA | Korean Government Standard Encryption Algorithm |
| ATSO | Administrator Token Security Operator |
| ATU | Administrator Token User |
| CA | Certificate Authority |
| CPU | Central Processing Unit |
| CSP | Critical Security Parameter |
| DES | Data Encryption Standard |
| DH | Diffie-Hellman |
| DHEK | Diffie-Hellman Ephemeral Key |
| DRBG | Deterministic Random Bit Generator |
| DSA | Digital Signature Algorithm |
| ECDH | Elliptic Curve Diffie-Hellman |
| ECDHEK | Elliptic Curve Diffie-Hellman Ephemeral Key |
| FIPS | Federal Information Processing Standard |
| HRNG | Hardware Random Number Generator |
| IDEA | International Data Encryption Algorithm |
| KAT | Known Answer Test |
| LCD | Liquid Crystal Display |
| LED | Light Emitting Diode |
| MAK | Message Authentication Key |
| MD2 | Message Digest Algorithm 2 |
| MD5 | Message Digest Algorithm 5 |
| MD5 HMAC | MD5 Hashed Message Authentication Code |
| MMK | Module Master Key |
| NIST | National Institute of Standards and Technology |
| NO | Normal Operator |
| PSI-E2 | ProtectServer Internal-Express 2 |

| Acronym | Definition |
|---|---|
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| RAM | Random Access Memory |
| RC2 | Rivest's Code 2 |
| RC4 | Rivest's Code 4 |
| RNG | Random Number Generator |
| RoHS | Restriction on Hazardous Substances |
| ROM | Read Only Memory |
| RSA | Rivest, Shamir and Adleman |
| RWXZ | Read, Write, Execute, Zeroize |
| SDRAM | Synchronous Dynamic Random Access Memory |
| SHA | Secure Hash Algorithm |
| SO | Security Operator |
| SRAM | Static Random Access Memory |
| Triple-DES | Triple Data Encryption Standard |
| USB | Universal Serial Bus |
| USO | User Security Operator |
| VGA | Video Graphics Array |