ProtectHost Orange Hardware Security Module

(Hardware Revision A, Firmware Version 1.34.00,
Software Version 1.01.11)

and

ProtectHost Orange Hardware Security Module with ORGA FM

(Hardware Revision A, Firmware Version 1.34.00,
Software Version 1.01.11, ORGA FM Version 1.2)

FIPS 140-2 Validation Security Policy

Level 3 Validation

August 2003

Version: 1.4.8

Table of Contents

1 INTRODUCTION 3

1.1 PURPOSE 3
1.2 REFERENCES 3
1.3 TERMINOLOGY 3
1.4 DOCUMENT ORGANIZATION 3

2 THE *PROTECTHOST ORANGE* MODULE 5

2.1 CRYPTOGRAPHIC MODULE 6
2.2 MODULE INTERFACES 7
2.2.1 Physical Ports, Connectors, and Interfaces 8
2.2.2 PKCS#11 Interface 10
2.2.3 FIPS 140-2 Logical Interface Mapping 10
2.3 TRUSTED CHANNELS 10
2.4 ROLES AND SERVICES 10
2.4.1 Administrative Token SO 11
2.4.2 Administrative Token User 12
2.4.3 Token SOs 12
2.4.4 Token Users 12
2.4.5 Roles and Services Table 13
2.5 PHYSICAL SECURITY 14
2.6 CRYPTOGRAPHIC KEY MANAGEMENT 15
2.6.1 Key Generation 15
2.6.2 Key derivation with ORGA FM 15
2.6.3 Key Access/Storage 16
2.6.4 Key Protection/Zeroization 16
2.7 CRYPTOGRAPHIC ALGORITHMS 16
2.8 SELF-TEST 17
2.8.1 Power-Up Self-Tests 17
2.8.2 Conditional Self-Tests 17

3 SECURE OPERATION OF THE PHO MODULE 19

4 ACRONYM LIST 20

1 INTRODUCTION

1.1 Purpose

This is a non-proprietary cryptographic module security policy for the Eracom Technologies Australia, Pty. Ltd. (Eracom Technologies*)* ProtectHost Orange Hardware Security Module (Hardware Revision A, Firmware Version 1.34.00, Software Version 1.01.11) and ProtectHost Orange Hardware Security Module with ORGA FM (HardwareRevision A, Firmware Version 1.34.00, Software Version 1.01.11, ORGA FM Version 1.2). This security policy describes how the ProtectHost Orange Hardware Security Module and ProtectHost Orange Hardware Security Module with ORGA FM meet the security requirements of FIPS 140-2, and how to securely operate the ProtectHost Orange Hardware Security Module and ProtectHost Orange Hardware Security Module with ORGA FMn a FIPS compliant manner. This policy covers the operation of the ProtectHost Orange Hardware Security in a FIPS approved manner without any Functionality Modules (FM) loaded and with the ORGA FM loaded. This policy was prepared as part of the level 3 FIPS 140-2 validation of the PHO Module.

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 website at http://csrc.nist.gov/cryptval/.

1.2 References

This document deals only with the operations and capabilities of the ProtectHost Orange Hardware Security Module and ProtectHost Orange Hardware Security Module with ORGA FMn the technical terms of a FIPS 140-2 cryptographic module security policy. For more information on the PHO, as well as other Eracom Technologies products, visit http://www.eracom-tech.com/.

1.3 Terminology

In this document, the ProtectHost Orange Hardware Security Module and ProtectHost Orange Hardware Security Module with ORGA FM will sometimes be referred to as the ProtectHost Orange, the PHO, the PHO Module, or the module.

1.4 Document Organization

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

- Executive summary
- Finite state machine
- Vendor evidence document
- Other supporting documentation as additional references

This document explains the ProtectHost Orange's FIPS 140-2 relevant features and functionality. The first section of this document provides an overview and introduction to the Security Policy. Section 2 describes the PHO Module, and how it meets FIPS 140-2 requirements. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

This Security Policy and other Validation Submission Documentation was produced by Corsec Security, Inc. under contract to Eracom Technologies. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Eracom Technologies-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Eracom Technologies.

2 The *ProtectHost Orange* Module

The ProtectHost Orange is a hardware security device intended specifically for host processing in public key infrastructure environments. Its dedicated cryptographic processor and key management features allow an organization to off-load much of their host-based Certificate Authority's (CA) processing to a secure, back-end peripheral device. The PHO's capabilities include support for X.509 and PKCS#10 digital certificates and public-private key pairs, secure key storage, and certificate issuance, storage, and authentication.

Figure 1 shows the PHO in an electronic commerce environment providing cryptographic support to a Certification Authority. It can also be seen that the functionality of the PHO is sufficiently comprehensive to support PKI operations at the Merchant Server and the Payment Gateway or anywhere else PKI functionality is required.

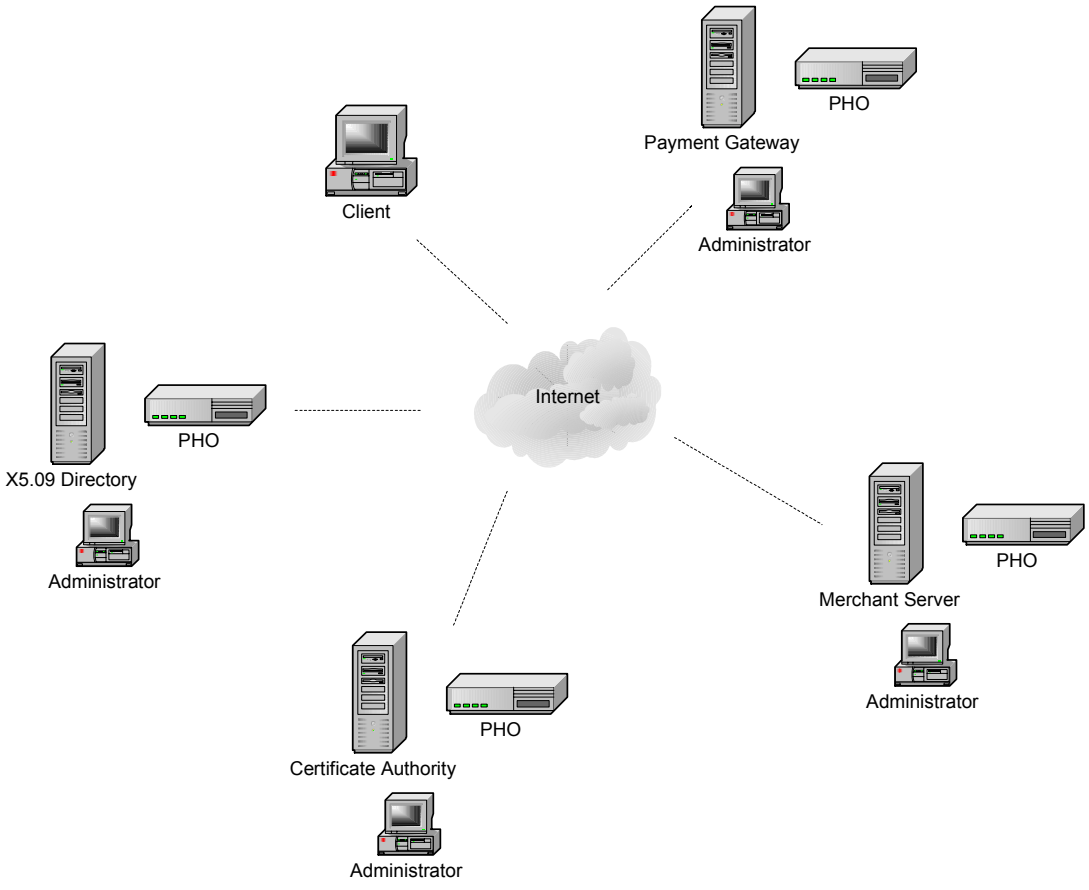

Figure 1 - Example PHO Usage

The PHO provides cryptographic services for encryption, decryption, secure key exchange, and digital signature generation and verification through its PKCS#11 application programming interface (API). Its ample memory and processing power provides great stability, scalability, and flexibility without sacrificing performance. The PHO addresses the need for a high level of physical security through a multi-layer architecture that incorporates tamper-resistant hardware as well as various intrusion detection and response mechanisms including key zeroization

and visible and audible alarms. In addition, the PHO can extend the PKCS#11functionality to include additional methods for key and PIN derivation with the inclusion of the ORGA FM as described in Section 2.6.2 and Section 3.

By isolating cryptographic processing and key management into a secure unit, the PHO will benefit any organization by increasing its defense against unauthorized and potentially malicious access. No longer does key management have to rely on insecure host-based certificate authorities, or software-based key management solutions.

2.1 Cryptographic Module

The metal casing that fully encloses the PHO Module establishes the cryptographic boundary for the device. All the functionality discussed in this document is provided by components within the casing.

Figure 2 shows the PHO's basic components.

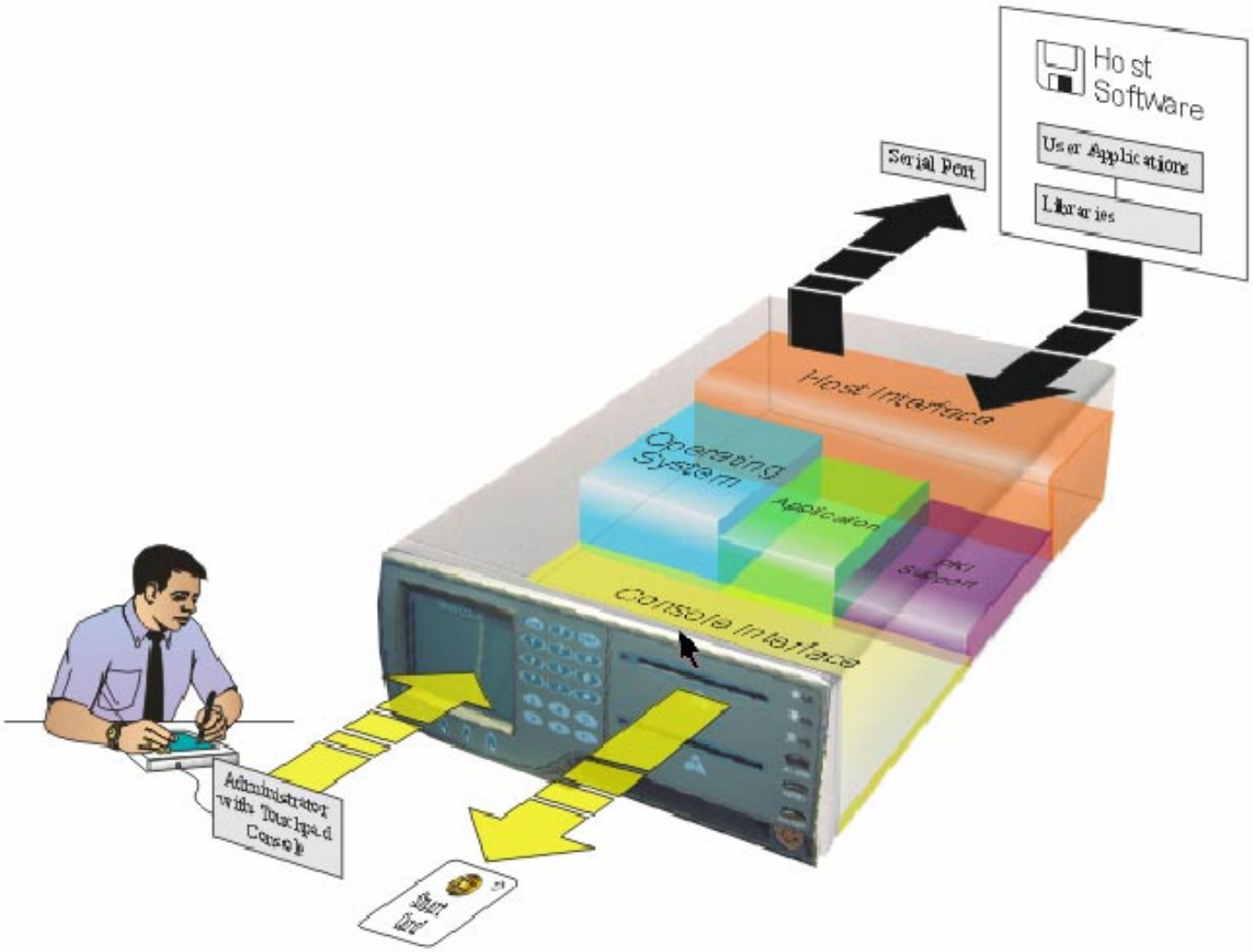

Figure 2 - Major Componets

The PHO has two major components:

- Module firmware
- Hardware

The module firmware implements the secure processing for the PHO. As depicted in Figure 2, the module firmware consists of four areas:

- The host interface is responsible for accepting request packets from one of the module's two Ethernet ports (it performs no cryptographic processing)
- The operating system[1] provides resource management and task scheduling
- The PHO application area provides high level processing required to implement the PHO host and console functions
- The PKI support area provides overall system management function including status operations and self-tests of the cryptographic components. All of the cipher and hashing mechanisms are found here.

The hardware portion of the PHO is comprised of the module's rear external interface, front panel console interface, and physical security components (for more on the module's physical interfaces see Section 2.2.1). Figure 3 shows the module's encasement and cryptographic boundary.

Figure 3 - Module Encasement

2.2 Module Interfaces

The PHO provides a number of physical interfaces that enable it to interface with devices outside the cryptographic boundary. Per FIPS 140-2, the module has been designed to support four logical interfaces:

- Data input
- Data output
- Control input
- Status output

[1] Note: The term "operating system" is used for the sake of consistency with Figure 2. The PHO's operational environment is a limited operational environment with no general purpose operating system upon which the operation environment resides.

The sections 2.2.1 – 2.2.3 describe the module's physical and logical interfaces and the relationship between them.

2.2.1 Physical Ports, Connectors, and Interfaces

The physical interfaces for the PHO are located on the rear and front panels. These interfaces include a power plug, integrated keypad and LCD, smartcard readers, and Ethernet, COM, and USB ports. The module also has a VGA interface and LED for indicating operational status.

Figures Figure 4 and Figure 5 show the module's physical front and rear panels.

Figure 4 - Front Panel

Figure 5 - Rear Panel

Figures Figure 6 and Figure 7 graphically illustrate the module's physical ports.

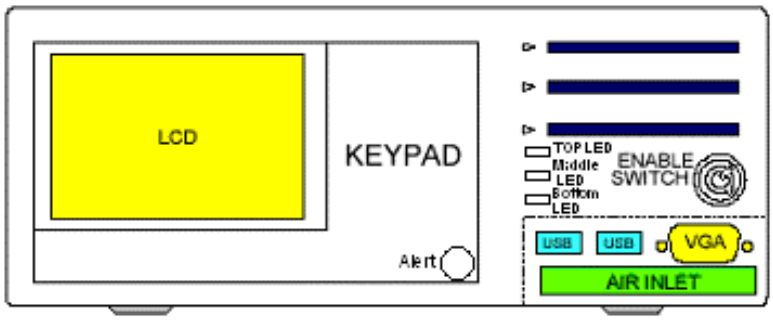

Figure 6 - Front Panel Interfaces

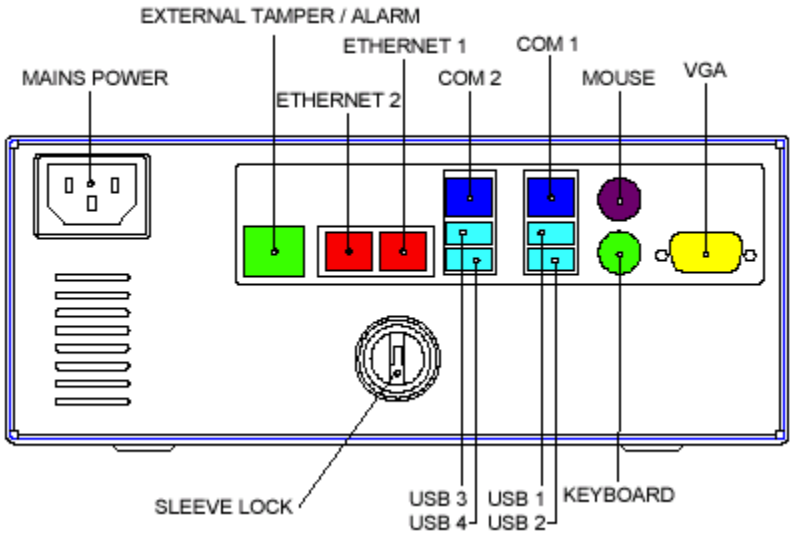

Figure 7 - Rear Panel Interfaces

Complete lists of all physical interfaces are summarized in Tables Table 1 and * Note: The Enable Switch is not a true port, connection, or interface but was included for completeness.
** Note: The Sleeve Lock is not a true port, connection, or interface but was included for completeness.
Table 2.

Connector	Description
USB 5 and 6	Two Universal Serial Bus (USB) connectors for the connection of peripherals (e.g. keyboard, mouse).
VGA	Output for a standard VGA compatible monitor, used for viewing the console interface. This is a duplicate connection to that found on the rear panel.
Integrated keypad and LCD	Provides a basic subset of PHO configuration and administration options. It is used as the initial point of entry when authenticating to the device after applying power and making changes to the internal settings.
Enable switch*	A key operated switch used to turn the PHO on or off.
Three integrated smartcard readers	Used to interface with a smartcard.
Three smartcard LEDs	LEDs that indicate if a smartcard is inserted in a particular smartcard reader
Top LED	Indicates if the PHO is powered-on
Middle LED	Indicates if the battery is low
Bottom LED	Indicates if the PHO is on-line and can be accessed by a remote client
Tamper light	The visible tamper alarm

Table 1 – Front Panel Interface Description

Connector	Description
Mains power	Connects to a 240/250 Volt mains power supply.
External tamper alarm	Allows another connection to a visible or audible alarm. This output provides a closed circuit when alarmed. This interface is disabled.
Ethernet 1 and 2	Two standard 10/100 BaseT network connections used for connecting the module to an Ethernet network.
COM 1 and 2	Two standard serial communication ports for connecting peripherals such as smart card readers. These interfaces are disabled.

USB 1, 2, 3, and 4	Four Universal Serial Bus (USB) connectors for the connection of peripherals (e.g. keyboard, mouse).
Mouse	Input for a standard PS/2 compatible mouse which is used to control the module via its console interface. This interface is disabled.
Keyboard	Input for a standard PS/2 compatible keyboard which is used to control the module via its console interface. This interface is disabled.
VGA	Output for a standard VGA compatible monitor, used for viewing the console interface. This is a duplicate connection to that found on the front panel
Link lights (green)	A link light indicates if an Ethernet link is active established
Connection lights (amber)	A connection light indicates if a Ethernet cable has been connected to the module
Sleeve lock**	A lock that secures the outside cover of the PHO to the internal chassis.

* Note: The Enable Switch is not a true port, connection, or interface but was included for completeness.
** Note: The Sleeve Lock is not a true port, connection, or interface but was included for completeness.

Table 2 - Rear Panel Interface Description

2.2.2 PKCS#11 Interface

In addition to the PHO specific functionality, the PHO utilizes RSA's PKCS#11 interface for cryptographic operations. For information on PKCS#11 see RSA's *PKCS #11: Cryptographic Token Interface Standard*.

2.2.3 FIPS 140-2 Logical Interface Mapping

The module supports the four FIPS 140-2 defined logical interfaces. The PHO's logical/physical interface mapping is summarized in the table below.

Physical Interface	Logical Interface(s)
Ethernet	Data input, data output, control input, and status output
USB	Control input, data input, and data output
VGA	Status output
Integrated keypad	Control input
Integrated smartcard readers	Data input, data output
LCD	Status output
LED	Status output

Table 3 - Logical/Physical Interface Mapping

2.3 Trusted Channels

The PHO Module implements a Trusted Channel which enables operators to securely communicate data sent over the Ethernet interface. Every time a session is initiated with the module over a communication interface a TDES session protection key is negotiated using Diffie-Hellman. This key is used to encrypt all traffic, including keys and authentication information, into and out of the PHO.

2.4 Roles and Services

The PHO supports identity-based authentication of its operators and supports multiple simultaneous operators each with their own individual set of services. Additionally, individual operators can request multiple sessions simultaneously. The module separates operators based

on their sessions, thus maintaining the separation of the authorized roles and services performed by each operator. Operators are authenticated to the module by selecting a token and presenting a Personal Identification Numbers (PINs). PINs can use any byte value of length 4-32 bytes, which exceed FIPS 140-2 strengths of mechanism requirements. Considering a PIN of the minimum size (4 bytes), the number of combinations available is 4,294,967,296.

The PHO allows access to unauthenticated services available from the front panel (or the VGA console if the VGA console has been enabled). Unauthenticated services include review of system naming information, system status information, and basic commands such as shutdown, LCD contrast, and IP configuration. The ***ProtectHost Orange*** Administration Manual describes all LCD and VGA console access. These unauthenticated services are available to all roles listed below.

Roles are based on the PKCS#11 concept of Tokens (for more information see RSA Laboratory's *PKCS #11: Cryptographic Token Interface Standard*). The PHO supports two types of Tokens: a single Administrative Token and multiple regular Tokens. Each token supports two operators: a Security Officer (SO) and a User. An operator may, therefore, assume one of four roles listed below:

- Administrative Token SO
- Administrative Token User
- Token SOs
- Token Users

The operator explicitly selects a role when logging in by selecting a PKCS#11 Token and choosing either User or SO Role.

2.4.1 Administrative Token SO

The primary function of the Administrative Token SO (ATSO) is to set up an Administrator account. Note that there is only one ATSO for the entire module (as module has only a single Administrative Token). This ATSO is able to set the initial crypto officer PIN value but is not able to change the administration PIN after it is initialized. There is a factory default login ID and password, which allows access to the ATSO role. The ATSO can perform the following actions:

- Create and destroy public objects on their own token.
- Specify a key EXPORT attribute on a specific key
- Specify TRUSTED on a specific public certificate
- Exercise status querying services.
- May change his/her own PIN

Keys must be configured as exportable in order to be output from the module. Keys that are exportable are output wrapped, and the keys used as key wrappers must themselves be configured for key wrapping.

2.4.2 Administrative Token User

The Administrative Token User (ATU) is responsible for the overall security management of the PHO Module. Again, note that the there is only one ATU for the module, and the following actions are available to the ATU:

- Set or Change Real Time Clock (RTC) value
- Read the Hardware Event Log
- Purge a full Hardware Event Log
- Specify the Security Policy for the PHO.
- Create new Tokens
- Initialize smart cards
- Destroy Individual Tokens.
- Erase all adapter Secure Memory including all PINS and User Keys
- Perform Firmware Upgrade Operation
- Create, destroy, import, export, generate, and derive public or private objects on their Admin token.
- Exercise cryptographic services with private, public, and secret keys on the Admin Token
- Exercise status querying services
- Change his/her own PIN

2.4.3 Token SOs

The Token SO is responsible for granting and revoking Token User ownership for her specific token. The module provides one Token SO role for each token within the module. If a token does not have a User PIN, the Token SO should initialize it by assigning it a label and User PIN. She 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.

- Set the Token User PIN on a Token with no Token User PIN.
- Reset (re-initialize) the Token (destroys all sensitive and non sensitive data) and sets new Label and Token SO PIN
- Create, destroy, public objects on their own token.
- Specify a key EXPORT attribute on a specific key
- Specify TRUSTED attribute on a specific public certificate
- Exercise status querying services.
- Change his/her own PIN

2.4.4 Token Users

The Token User of each token may manage and use private and public keys on their own tokens.

- Exercise cryptographic services with private, public, and secret keys on the Admin Token
- Create, destroy, import, export, generate, and derive private or public objects on their own token.
- Exercise status querying services.
- Change his/her own PIN

2.4.5 Roles and Services Table

The PHO provides bounded services to an operator based on the role to which the operator authenticated. * denotes functionality provided by the ORGA FM module
Table 4 lists the services available to each role.

Services	Administrative Token SO	Administrative Token User	Token SO	Token User	CSP Access
Specify Key Export Attribute on a Public Key	X		X		
Specify Trusted Attribute on a Public Certificate	X		X		
Set Initial Administrator PIN Following a Tamper	X				PIN (read/write)
Get Token Info	X	X	X	X	
Change Own Password	X	X	X	X	PIN (read/write)
Change RTC		X			
Read Hardware Event Log	X	X			
Purge Full Hardware Event Log		X			
Set Transport Mode		X			
Specify Adapter Security Policy		X			
Create Tokens		X			
Initialize Token Labels and SO PIN		X			PIN (read/write)
Initialize Smart Cards/Labels/SO PIN's		X			PIN (read/write)
Specify Smart Card Min PIN Length		X			
Destroy Tokens		X			
Erase Adapter Secure Memory/PIN's/Keys		X			All CSPs (write)
Perform Firmware Upgrade		X			
Public Key Cryptographic Services On an Admin Token	X	X			
Create Public Admin Token Objects	X	X			
Destroy Public Admin Token Objects	X	X			
Generate Public Admin Token Objects	X	X			
Derive Public Admin Token Objects	X	X			
Private Key Cryptographic Services On Admin Token		X			Secret/private keys (read/write)
Create Private Admin Token Objects		X			Secret/private keys (write)
Destroy Private Admin Token Objects		X			Secret/private keys (write)
Generate Private Admin Token Objects		X			Secret/private keys (write)

Derive Private Admin Token Objects		X			Secret/private keys (write)
Initialize Normal Token User PIN			X		PIN (read/write)
Reset (re-Initialize) Normal Token			X		
Public Key Cryptographic Services on a Normal Token			X	X	Secret/private keys (write)
Create Public Objects on a Normal Token			X	X	
Destroy Public Objects on a Normal Token			X	X	
Generate Public Objects on a Normal Token			X	X	
Derive Public Objects on a Normal Token			X	X	
Private Key Cryptographic Services on a Normal Token				X	Secret/private keys (read)
Create Private Objects on a Normal Token				X	Secret/private keys (write)
Destroy Private Objects on a Normal Token				X	Secret/private keys (write)
Generate Private Objects on a Normal Token				X	Secret/private keys (write)
Derive Private Objects on a Normal Token				X	Secret/private keys (write)
Create Public Objects on a Smart Card Token			X	X	
Destroy Public Objects on a Smart Card Token			X	X	
Create Private Objects on a Smart Card Token				X	
Destroy Private Objects on a Smart Card Token				X	
*Derive a PIN by ORGA FM		X		X	
*Derive a secret for use by the ORGA FM PIN derivation		X		X	Secret/private keys (write)

* denotes functionality provided by the ORGA FM module

Table 4 - Roles and Services Table

2.5 Physical Security

The PHO is equipped with multiple layers of physical security mechanisms. The entire module is surrounded by a strong outside cover (sleeve) that is locked to the internal chassis. Attempting to penetrate the cover will damage the module. Removing the cover (even while using the correct physical key) will cause all critical security parameters, including all key material, to be zeroized.

The inner workings of the PHO are protected with three additional layers of security. First a metal case is securely fastened around the CPU's and memory. Secondly, the internal cover is equipped with a zeroization mechanism that is triggered when the cover is removed. Lastly, a

light sensor is mounted within the internal cover. If the light sensor detects a specified brightness of light a trigger is activated and all key material is zeroized.

The module's battery compartment is also equipped with a pick-resistant lock and two zeroization/tamper switches. The first switch is activated whenever the battery compartment lock is unlocked. The second switch is activated whenever the battery compartment is removed from the module.

The module's physical security mechanisms are summarized in the table below.

Mechanisms	Description
Outside cover	A strong, opaque, metal cover.
Pick-resistant lock with zeroization/tamper switch	A lock the securely fastens the outside cover to the internal chassis. If unlocked, a tamper is triggered and all CSPs are zeroized.
Outside cover zeroization mechanism	A mechanism that zeroizes all CSPs when the outside cover is removed.
Internal cover	A strong, opaque, metal cover.
Internal cover zeroization mechanism	A mechanism that zeroizes all CSPs when the internal cover is removed.
Light sensor zerioization mechanism	A mechanism located within the internal cover that zeroizes all CSPs when it detects a specified brightness of light.
Pick-resistant lock with zeroization/tamper switch on battery compartment	A lock the securely fastens the battery compartment to the internal chassis. If unlocked, a tamper is triggered and all CSPs are zeroized.

Table 5 - Physical Security Mechanisms

2.6 Cryptographic Key Management

The PHO 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 PHO Module supports generation of DSA, RSA, ECDSA, and DH public and private keys. Furthermore, the module implements a FIPS 186-2 Change Notice 1 PRNG (Appendix 3.1 with SHA-1 for the underlying G function as detailed in Appendix 3.3) for generating keys used in FIPS approved algorithms.

2.6.2 Key derivation with ORGA FM

The ORGA FM introduces two additional methods for PIN derivation that are not provided through the standard PKCS#11 interface: `CKM_ORGA_KEY_DERIVE` and `CKM_ORGA_PIN_DERIVE`. These methods are incorporated by extensions to the existing PKCS#11 C_DeriveKey function. The `CKM_ORGA_KEY_DERIVE` function uses a method incorporating TDES and two blocks of random data to derive a 16 byte TDES key for use in the derivation of a PIN. The `CKM_ORGA_PIN_DERIVE` function uses a similar method to derive an 8 byte PIN.

2.6.3 Key Access/Storage

All keys except module specific keys are stored as plaintext token objects in secure memory (battery-backed RAM), and the module prevents physical access to this RAM 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. Any key input to the module is done so over a TDES encrypted, trusted channel, and the module only allows wrapped (encrypted) keys to be output. Wrapped keys can be encrypted with RSA public keys, or DES, TDES, or AES keys.

Specifically, the keys stored by the module are:

- Embedded in the module's firmware
  - 2048-bit RSA public key used to verify the authenticity of loaded firmware
  - The default Administrative Token SO's PIN
- Stored within the secure memory (battery-backed RAM)
  - The Diffie-Hellman public parameters used to establish a trusted (encrypted) channel between an operator and the module (generated anew each power-up).
  - The operating PINs (Administrative Token SO, Administrative Token User, Token SOs, and Token Users PINs–all stored in secure memory).
  - All token keys (AES, DES, DH, DSA, ECDSA, RSA, and TDES—stored as token objects in secure memory)

2.6.4 Key Protection/Zeroization

All keys CSPs that are not ephemeral or exported from the module are stored in memory within the module's strong metal cover. All keys are protected by the physical security and key zeriozation mechanisms discussed in section 2.5, and keys can be zeroized via these methods, or individually deleted through the module's services.

2.7 Cryptographic Algorithms

The PHO Module supports a wide variety of cryptographic algorithms. FIPS 140-2 requires that only FIPS Approved algorithms be used whenever there is an applicable FIPS standard. Thus, Table 6 is divided into two sections: FIPS Approved and non-FIPS Approved. When the module is placed into FIPS mode (see Section 3) only the algorithms listed under the FIPS Approved section of Table 6 will be available.

FIPS Approved	Non-FIPS Approved
AES (ECB, CBC)	CAST 128 (ECB, CBC)
DES (ECB, CBC, OFB64)	CAST MAC
DES MAC	IDEA (ECB, CBC)
DSA	IDEA MAC
ECDSA	DH
RSA PKCS#1 and ANSI X9.31	MD2
SHA-1	MD5
SHA-1 HMAC	MD5 HMAC
TDES (ECB, CBC, OFB64)	RC2 (ECB, CBC)
TDES MAC	RC2 MAC
	RC4
	RC4 MAC
	RIPEMD-128

	RIPEMD-160
	RMD128 HMAC
	RMD160 HMAC

Table 6 - Cryptographic Algorithms

2.8 Self-Test

The PHO Module performs a number of power-up and conditional self-test to ensure proper operation.

2.8.1 Power-Up Self-Tests

When the PHO is initially powered-on, it executes a battery of power-up self-tests. If any of the power-up self-tests fail, the module will enter an error state and prohibit an operator from exercising the module's cryptographic functionality. Table 7 provides a complete list of all power-up self-tests implemented within the PHO.

Test	Function	FIPS 140-2 Required
SDRAM	Tests the module's volatile working memory by performing a connectivity test	No
SRAM	Tests the module's static RAM by performing a connectivity test	No
Secure Memory File System Integrity	Initializes and checks the module's secure memory file system	No
SA0	Verifies a checksum over the module's ROM	No
RTC Connectivity	Verifies that the CPU can connect to the UART device	No
Symmetric Cipher KATs	Performs known answer tests for CAST, AES, IDEA, DES, TDES, RC2, and RC4.	Yes for AES, DES, and TDES
MAC and HMAC KATs	Performs known answer tests for CAST MAC, IDEA MAC, DES and TDES MAC, and RC2 and RC4 MAC. Also performs known answer test for SHA-1, MD5, and RMD HMACs.	Yes for DES/TDES MAC and SHA-1 HMAC
Asymmetric Cipher KATs	Performs a known answer test for RSA operations.	No
Sign/Verify	Tests signature verification tests for RSA and DSA.	Yes
Message Digest KATs	Verifies known message/hash pairs for MD2, MD5, RMD, and SHA-1.	SHA-1
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 digest to a known good result.	Yes
Statistical RNG	Performs a Statistical Chi Square test of 2500 bytes of random data	(Legacy)

Table 7 - Power-Up Self-Tests

2.8.2 Conditional Self-Tests

The PHO performs the conditional self-tests outlined in Table 8.

Test	Function	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.	Yes for DSA, RSA, ECDSA
Continuous RNG	Performs the FIPS 140-2 required continuous RNG check each time the module's RNGs are used to produce	Yes

	random data.	
Software Load	Checks that software is digitally signed before it can be loaded. Note: The PHO must be reconfigured for successful load of new software, requiring reconfiguration to assure FIPS mode. All keys and CSPS will be zeroized in this process.	Yes

Table 8 – Conditional Self-Tests

3 Secure Operation of the PHO Module

The PHO allows its administrators the choice of employing a wide range of security technologies.

During the initialization of the module for FIPS 140-2 operation, the default PIN for the Administrative Token SO must be changed. This step must be completed before the following configurations steps are performed.

To operate the module in a FIPS 140-2 compliant manner, however, the PHO must be configured to use only the FIPS approved cryptographic algorithms listed in Table 6. In order to set the module into a FIPS mode of operation, the operator must set the following security mode attribute flags.

- CKF_NO_CLEAR_PINS (0x00000002)
- CKF_AUTH_PROTECTION (0x00000004)
- CKF_NO_PUBLIC_CRYPTO (0x00000008)
- CKF_TAMPER_BEFORE_UPGRADE (0x00000010)
- CKF_MODE_LOCKED (0x10000000)
- CKF_FIPS_ALGORITHMS (0x00000040)

Once these flags are set, the PHO will reject all requests for non-FIPS algorithms or configurations. An operator may easily set all of these security mode attribute flags by running the `CTCONF -fF` command from the remote management facility.

If, at any time, an operator would like to check the module's mode of operation, the operator can check the security mode attribute to ensure that it has a value of 0x1000005E, which is the combination of the flags listed above. A simple way to perform this query is to run the `CTCONF -v` command from the remote management facility.

The PHO can be loaded with individual Functionality Modules (FMs) that have been FIPS 140-2 validated and be operated in FIPS mode. This security policy covers validation of the PHO with no FM loaded, and with the ORGA FM loaded. If an operator of the PHO loads enables FIPS mode, the module cannot load additional FMs without resetting and reinitializing the module, which includes the erasure of all information, keys and CSPs stored in the PHO (i.e., returns the module to the factory state). Loading other FMs into the PHO causes the PHO to run in an un-validated mode. In order to maintain FIPS 140-2 validation, all FMs must be separately tested and validated for use with PHO.

Finally, as mentioned in section 2.6.2, because use of derived keys for data encryption and decryption does not meet the FIPS 140-2 requirements, the operator of the module must be aware of the restrictions of such keys and must not use derived keys for data encryption and decryption to ensure FIPS compliance.

Please refer to the separate operational manuals with Crypto Officer and User Guidance for more information on operation of the PHO module.

4 Acronym List

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
ATSO	Administrative Token Security Operator
ATU	Administrative Token User
CA	Certificate Authority
CPU	Central Processing Unit
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
IDEA	International Data Encryption Algorithm
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Message Authentication Code
MD2	Message Digest (algorithm) 2
MD5	Message Digest (algorithm) 5
MD5 HMAC	Message Digest 5 Hashed Message Authentication Code
NIST	National Institute of Standards and Technology
NO	Normal Operator
PHO	ProtectHost Orange
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RC2	Rivest's Cipher 2
RC4	Rivest's CIpher 4
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir and Adleman
RTC	Real Time Clock
SDRAM	Synchronous Dynamic Random Access Memory
SHA1	Secure Hash Algorithm 1
SHA1 HMAC	Secure Hash Algorithm Hashed Message Authentication Code
SO	Security Operator
SRAM	Static Random Access Memory
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus
USO	User Security Operator
VGA	Video Graphics Array