TITLE: Luna® XPplus Security Policies

ABSTRACT: This document describes the security policies implemented by the Luna® XPplus module and how the design of the Luna XPplus enforces these policies.

DOCUMENT NUMBER: CR-0540

ORIGINATOR: Mark Perry

DEPARTMENT: Systems Engineering

LOCATION OF ISSUE: Ottawa

DATE ORIGINATED: December 11, 2000

CHANGE LEVEL: 12

CHANGE DATE: October 1, 2001

SECURITY LEVEL: None

SUPERSESSION DATA: CR-0540, 11

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Purpose

This document describes the security policies implemented by the Luna® XPplus module and how the design of the XPplus enforces these policies.

1.2. Scope

This document addresses the Luna XPplus token's security policies.

1.3. Intended Audience

The intended audience for this document is the Luna XPplus Engineering and Product Management Team, external agencies for validation or endorsement of the Luna XPplus module; selected industry partners; and potential users of the Luna XPplus module who want to understand the security policies of the product for FIPS-compliant operations.

The reader of this document should be familiar with the PKCS#11 standard defined by RSA Laboratories.

1.4. History of Revision

Revision	Date	Description
1	December 11, 2000	New document for the Luna XPplus module.
2	January 11, 2001	Incorporation of review comments.
3	March 6, 2001	Additional review comments.
4	March 16, 2001	Incorporation of review comments from T. Casar and D. Bailey.
5	March 27, 2001	Change of Security Level to "None" and new proprietary statement.
6	April 11, 2001	Incorporation of comments from B. Woodard regarding FPV_USE_CAV.
7	June 8, 2001	Incorporation of review comments from T. Casar, D. Bailey
8	July 16, 2001	Correction of FPV/TPV tables and descriptions (resolution of Razor Issue #484); modification of text to include information on use of XPplus through Cryptoki.
9	August 1, 2001	Text added to sections 2 and 4 by B. Gagné.
10	August 8, 2001	Description of security seals on enclosure changed by B. Gagné.
11	August 10, 2001	Description of removable screws modified.
12	October 1, 2001	Corrections made to address review comments.

1.5. References

Document Number	Revision	Author	Title
CR-0529	3	Ken Baird	Luna® XPplus Physical Security Design
PKCS#11	V2.10	RSA Laboratories	PKCS#11: Cryptographic Token Interface Standard, December 1999

1.6. Glossary of Acronyms / Abbreviations

Shortforms	*Longform Explanation*
CAV	Cryptographic Algorithm Vector
CCM	Custom Command Module
CSP	Critical Security Parameter
DAC	Discretionary Access Control
FPV	Fixed Policy Vector
KCV	Key Cloning Vector
I&A	Identification and Authentication
SO	Security Officer
SP	Secure Port
TPV	Token Policy Vector
UAV	User Authorization Vector

2. LUNA XPplus OVERVIEW

Luna XPplus is a cryptographic module based on a design equivalent to two Luna CA^3 tokens, and is a subordinate device in a Luna CA^3 system. The Luna XPplus can support all cryptographic algorithms listed in Appendix A of this document.

The Luna XPplus is validated against FIPS 140-1 level 3 security requirements, which includes the use of enhanced physical security mechanisms (described in Section 7).

When a customer chooses Luna CA^3 and requires scalable performance, the user installs a base Luna CA^3 system. Then, with load-balancing software, the user adds more performance to the system by daisy-chaining Luna XPplus devices. In Figure 1, a daisy-chain of a Luna Dock token reader (with two Luna CA^3 tokens) and Luna XPplus devices connects to a server, with a Luna PED device connected via an RJ-45 cable to the Luna Dock reader in the chain. The red token represents a Luna CA^3 token. All cryptographic services are accessed through the Luna CA^3 as in a typical installation.

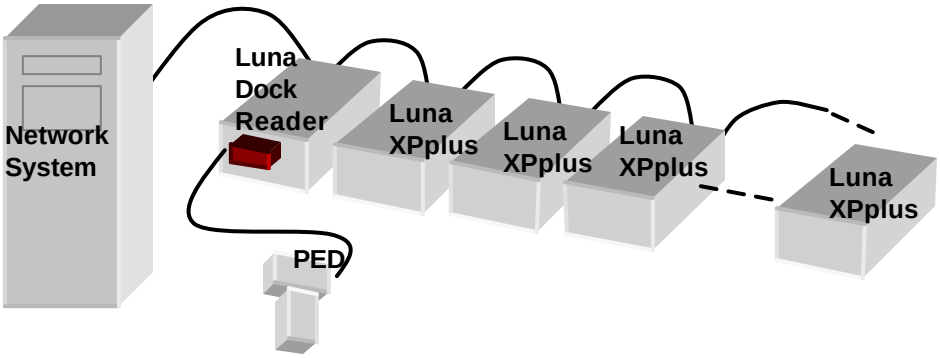

Figure 1: Luna XPplus Installation

Scalability limitations are a factor of host CPU availability (each additional Luna XPplus has a host CPU utilization cost), Luna Dock daisy-chaining restrictions (16 per PCI controller card) and available PCI slots in the server. For example, assuming that there is enough CPU power available, three PCI slots allow a total of 1 Luna Dock reader and 47 Luna XPplus modules for a scalable performance number in the tens of thousands of RSA 1024-bit signings per second.

In this system, the Luna CA^3 token continues to be the main device through which all access control, key generation and symmetric processing is performed. Asymmetric processing, such as signature signing and

signature verification, is offloaded to the Luna XPplus modules. For load balancing to occur, the root pair key on the Luna CA^3 token is cloned to each Luna XPplus. Once a Luna XPplus is removed from the daisy-chain, all sensitive information cloned to the Luna XPplus is zeroized.

The FIPS 140-1 Level 3 validated Luna XPplus configuration is not intended to function as a standalone product; as a prerequisite, a host Luna CA^3 system is required (as described previously). However, the Luna XPplus device can be operated outside of the scope of validation – in a non FIPS-compliant mode. This can be achieved by reinitializing the device, bypassing the FIPS 140-1 Level 3 setup procedures, and initializing the Luna XPplus without indirect login. Once initialized in this manner, the Luna XPplus device will not require use of the Luna CA^3 for login authentication, and keys from the Luna CA^3 will not be automatically cloned to the Luna XPplus. When in this state, the Luna XPplus device will appear and behave like two Luna CA^3 tokens with the following exceptions: the Luna PED is not used for authentication (login); there are no M of N capabilities; and there are no permanent storage capabilities.

As in a Luna CA^3 token, the Luna XPplus modules have the ability to distinguish between two categories of users: super-users and normal users. The super-user category is referred to as the Security Officer (SO) and the normal user category is referred to as the user. The SO functions are available only to the SO; they allow the SO to manage the security policy of the module. Each user has their own authentication code initially assigned under control of the SO, which is used internally to protect the data and cryptographic keys the user owns.

In order to log into an XPplus module, a user must first login to the Luna CA^3 as an SO or a normal user, then indirectly login to the Luna XPplus.

3. SECURITY POLICY TOOLS

The Luna XPplus module provides two levels of security policy enforcement. A vector that is loaded on the module during manufacturing dictates the first level of security. This vector, called the Fixed Policy Vector (FPV), establishes an envelope of security that cannot be modified after manufacturing.

The second level of security is provided by a policy vector that can be modified after manufacturing. This vector is called the Token Policy Vector (TPV), and consists of a series of policy settings that can be established and modified by the module's legitimate SO.

Since the design of the policy vectors is the same for all Chrysalis-ITS modules, some of the settings described below are not applicable to the Luna XPplus.

3.1. Fixed Policy Vector (FPV)

The FPV contains the settings necessary to enforce permanent policy rules that apply across a wide range of XPplus users and organizations. For example, one bit in the FPV defines whether the module can be exported. In an exportable version, the module provides a reduced set of algorithms and imposes limitations on maximum key lengths as required by export regulations.

The FPV cannot be modified by the SO or any of the users. The FPV is loaded during the manufacturing process and remains in place until the module is destroyed or the firmware is erased. The integrity of the FPV is maintained through the same mechanism used to protect the executable code from being modified, using a 32-bit CRC computation.

The format of the FPV is a 32-bit vector that is divided into four fields of eight bits. These fields and their contents are defined in the following sections.

3.1.1. Number of SO Login Fails Allowed

This field defines the number of consecutive failed login attempts that can be made by the SO before the module erases the flash memory to prevent illegal access to its contents.

This security measure prevents an impostor from cracking the SO's password. This bit is not used in the Luna XPplus, as the XPplus uses a different authentication mechanism (see Section 4).

3.1.2. Secret Key Policy

The following table defines the flags that identify the security policies that are followed for secret key objects.

Name	Description
FPV_SECRET_KEY_SENSITIVE	This bit determines whether a secret key object must always be made sensitive or if it can be determined by the high-level application using the token. When this bit is set, all secret keys stored on the token are sensitive. The keys are encrypted when in the flash memory and they can be extracted only outside of the token in encrypted form using the LUNA_WRAP_KEY function. This bit is set for the Luna XPplus.
FPV_SECRET_KEY_NO_CREATE	This bit determines whether a secret key object can be created by an external application using the token, instead of being generated by the token. When this bit is set, an external application cannot create a secret key on the token; it is not possible to enter a secret key in plain text form on the token. This bit is set for the Luna XPplus.

3.1.3. Private Key Policy

The following table defines the flags that identify the security policies that are followed for private key objects.

Name	Description
FPV_PRIVATE_KEY_SENSITIVE	This bit determines whether a private key object must always be made sensitive or if it can be determined by the high-level application using the token through PKCS#11. When this bit is set, all private keys stored on the token must be flagged as sensitive whether or not the high-level application requested this flag when the keys were created. When this bit is set, all private keys are encrypted while stored in flash memory. **Note:** After a private key is sensitive, it cannot be extracted from the token even in encrypted format. This bit is set for the Luna XPplus.
FPV_PRIVATE_KEY_NO_CREATE	This bit determines whether a private key object can be created by an external application using the LUNA_CREATE_OBJECT call, instead of being generated by the token. When this bit is set, an external application cannot create a private key on the token; it is not possible to enter a private key in plain text form on the token. This bit is set for the Luna XPplus.

3.1.4. Token Security Policy

The following table defines the flags that identify the security policies that dictate the behavior of the token in general.

Name	Description
FPV_XPPLUS_TOKEN	This bit indicates that the token is built upon XPplus-style hardware.

Name	Description
	XPplus hardware has: asymmetric math accelerators; extra RAM; non-volatile RAM; tamper detection mechanisms which trigger interrupts and wipe non-volatile RAM. This bit is set for the Luna XPplus.
FPV_XP_TOKEN	This bit determines if the token is used in an XP-style functionality, thus allowing the KCV to be set indirectly (allows XP tokens to get a CA[3]'s domain vector). It allows the token to be initialized as either a FIPS Level 2 or 3 device at InitToken time; all keys must be volatile. This bit is set for the Luna XPplus.
FPV_DOMESTIC_FLAG	This bit determines whether the token can be exported. When this bit is set, the token is configured for the domestic market and cannot be exported. This bit is verified internally every time a cryptographic function implying an encryption or a decryption is performed. If the bit is set, no restrictions exist on key sizes. If the bit is not set, a limitation of 56 bits is applied to any symmetric keys used for encryption or decryption, and a 512-bit limitation on asymmetric keys used for wrapping and unwrapping operations. Signature and verification operations are not restricted in terms of key lengths.
FPV_ENABLE_CLONING	This bit determines whether sensitive objects on the token can be "cloned" to another similarly enabled token. When this bit is set, cloning is enabled. This bit is set for the Luna XPplus.
FPV_USE_CAV	This bit is used by the firmware to determine if the CAV should be checked to validate the desired algorithm. Normally, this bit is zero, which assumes all algorithms are valid. For Luna XPplus, the bit is not set.
FPV_WRAPPING_TOKEN	This bit determines whether RSA private keys can be wrapped. When this bit is set, an RSA private key can be wrapped. RSA private key wrapping is not allowed for Luna XPplus. As such, this bit is not set.
FPV_USE_M_OF_N	This bit defines whether the token can perform M of N activation. When this bit is set, the token can be configured to perform M of N activation. M of N activation is a feature ordinarily enabled on a Luna XPplus. This bit is always set and is used for indirect M of N when using a CA[3] to log indirectly into the XPplus module.
FPV_USE_RAW_RSA	This bit determines whether RAW RSA operations can be performed on the token. When this bit is set, RAW RSA operations are allowed. For Luna XPplus, the bit is set.
FPV_SPECIAL_CLONING	This bit determines whether the token allows the factory-default Chrysalis-ITS key cloning certificate to be modified. When this bit is set, customers can create their own key cloning certificate. For Luna XPplus, the bit is set.
FPV_ENABLE_CCM	This bit determines whether a Custom Command Module (CCM) can be loaded onto the token. When this bit is set, a CCM can be loaded onto the token. This bit is not set for FIPS-compliant tokens (including the XPplus).
FPV_CCM_PRESENT_FWUPDATE	This bit determines whether a CCM must be present before a firmware update operation is allowed to proceed. When this bit is set, a CCM must be loaded on the token to perform a firmware update. Additionally, the CCM must implement the PreModuleUpdate function. This bit does not apply to tokens with FPV_ENABLE_CCM clear.
FPV_FORCE_RSA_BLINDING	This bit determines whether the token must perform blinding, which introduces a random element to the time needed to complete an RSA operation. Blinding defeats timing attacks on an RSA operation. If this bit is set, the token will always use RSA blinding (the TPV_FORCE_RSA_BLINDING bit will have no effect). For Luna XPplus, this bit is not set.
FPV_PIN_MUST_USE_SP	This bit determines if the serial communication port must be used to enter an authentication code. When this bit is set, an authentication code can only be entered through the serial communication port. When this bit is cleared, authentication codes are entered via the host computer. This bit does not apply to the Luna XPplus, and is not set.
FPV_MOFN_MUST_USE_SP	This bit determines if the serial communication port must be used to enter

Name	Description
	the M of N secret. When this bit is set, the M of N secret can only be entered through the serial communication port. When this bit is cleared, the M of N secret is entered via the host computer. This bit does not apply to the Luna XPplus, and is not set.
FPV_KCV_MUST_USE_SP	This bit determines if the serial communication port must be used to enter the key cloning domain identifier. When this bit is set, the key cloning domain identifier can only be entered through the serial communication port. When this bit is cleared, the key cloning domain identifier is entered via the host computer. This bit does not apply to the Luna XPplus, and is not set.

3.2. Token Policy Vector (TPV)

The TPV contains the settings necessary to enforce policy rules locally in an organization. For example, one bit in the TPV defines whether the module can perform a signature operation using a signing key generated by an outside process or if it must use an internally generated key for this function. The TPV can be modified by the module's SO. The TPV contents are used by the internal code to validate the operations performed by the module's USER.

The format of the TPV is a 32-bit vector that is divided into four fields of eight bits. These fields and their contents are defined in the following sections. Since the SO can modify any of these settings, the values provided below are the default values set during manufacturing.

3.2.1. Number of User Login Fails Allowed

This field defines the number of consecutive failed indirect login attempts that can be made by a USER before the USER gets locked out or the USER's data is erased. This security feature prevents illegal access to the USER's data and keys: it prevents an impostor from cracking the USER's password on the token. Whether the user is locked out or the data is erased depends upon the "USER zeroize" bit. If the USER zeroize bit is disabled, too many failed login attempts results in the USER getting locked out. In this case, a USER must make a request to the SO to regain access to the token. The SO also provides a new password for the USER. If the USER zeroize bit is enabled, too many failed login attempts results in the USER being deleted. In this case, the USER's identity and private data (including key material) are erased from the token. The SO must create a new user in order to continue. The new user will have no association with the previous (deleted) user.

3.2.2. Minimum/Maximum PIN Length

These two fields define the minimum and maximum length restrictions for a USER's PIN. These fields do not apply to the Luna XPplus when it is acting as a FIPS 140-1 level 3 device.

3.2.3. Local Policies

The following table defines the flags that identify the security policies that dictate the behavior of the users on the module.

Name	Description

Name	Description
TPV_USER_ZEROIZE	This bit determines whether the token can be zeroized by a normal user or if only the token's SO can zeroize the token. This bit indicates whether the token is centrally controlled. When this bit is set, it indicates that a valid token user can zeroize the token. This bit enables using the token in an environment where the SO is not commonly used. When this bit is set, the SO cannot change a user password, and a user is zeroized after too many unsuccessful login attempts. For Luna XPplus, the bit is initially set.
TPV_USER_FW_UPDATE	This bit determines whether the firmware can be updated by a normal user or if only the token's SO can update the firmware. When this bit is set, a normal user can perform the firmware update. For Luna XPplus, the bit is initially not set.
TPV_M_OF_N_ACTIVATION	This bit determines whether M of N activation is required for a user to gain access to the token. When this bit and the FPV_SECURITY_POLICY_USE_M_OF_N bit in the FPV is set, the token is not activated until the required number of parts to a split secret have been entered. For Luna XPplus, the bit is not set.
TPV_KEY_ATTRIB_LOCK	This bit determines whether the flag attributes of a key can be modified once the key is a valid object on the token. When this bit is set, it indicates that the flag attributes of a key cannot be modified after they have been established. For example, if this bit is set and a DES key is created for encryption and decryption, these attributes cannot be changed to wrap and unwrap once the key exists on the token. For Luna XPplus, the bit is initially set.
TPV_KEY_SINGLE_FUNCTION	This bit determines whether a key can be used to perform multiple types of operations (i.e., use a key for encrypting, signing, and wrapping). When this bit is set, it indicates that keys can be used only to perform single functions. For symmetric keys, a single function is considered to be a pair of related functions such as encryption/decryption, wrapping/unwrapping, or sign/verify. For Luna XPplus, the bit is initially not set.
TPV_SIGNING_KEY_LOCAL	When performing a signing operation, the private key used may have been generated locally or provided by an external source. In most environments, it is preferable to have the signing/verifying key pair generated by the token and never extracted from it. However, in certain cases the signing keys are generated externally and loaded on the token for subsequent signature operations. When this bit is set, it indicates that externally generated keys cannot be used for signing operations performed by the token. For Luna XPplus, the bit is not set.
TPV_FORCE_RSA_BLINDING	This bit determines whether the token must perform blinding on RSA operations. If the FPV_FORCE_RSA_BLINDING bit is on, RSA blinding is performed on the token regardless of this TPV bit. However, if the FPV_FORCE_RSA_BLINDING bit is clear, the TPV_FORCE_RSA_BLINDING bit determines if the token will use RSA blinding. When the bit is set, blinding is performed. For Luna XPplus, this bit is set initially.
TPV_DISABLE_CLONING_BY_USER	This bit determines whether a user or both a user and the token's SO are permitted to clone sensitive objects when the FPV_SECURITY_POLICY_ENABLE_CLONING bit is set. If the FPV_SECURITY_POLICY_ENABLE_CLONING bit is clear, no cloning is permitted and the TPV_DISABLE_CLONING_BY_USER bit has no effect regardless of its value. When TPV_DISABLE_CLONING_BY_USER is clear, both a user and the token's SO are permitted to clone sensitive objects. When the bit is set, only the token's SO is permitted to clone sensitive objects. This bit is initially not set.

Name	Description
TPV_XP_MUST_USE_SP	This bit also determines whether the secure port (SP) must be used or not. This bit is set during initialization and cannot be modified without zeroizing the token (i.e. re-initializing it). When initialized in conjunction with a CA³ token, this bit is set. When initialized in conjunction with a FIPS 140-1 level 2 token this bit is cleared. That is, this bit determines the level of FIPS under which the XPplus operates. When set, the XPplus is a FIPS 140-1 level 3 token; when clear, it is a FIPS 140-1 level 2 token. Once initialized, the XPplus works only with tokens at the same level. That is, you cannot initialize the XPplus as a level 2 device and then use it with CA³ tokens. If the bit is set, all PIN data must be entered either indirectly or through a secure port (FIPS 140-1, level 3). If the bit is cleared, then all PIN data must be entered either indirectly, or in plain text from the host (FIPS 140-1, level 2).

4. IDENTIFICATION AND AUTHENTICATION (I&A)

The Luna XPplus module enforces an identity-based user authentication policy (via an indirect login upon completion of a Luna CA^3 user login). For normal users, the user number and a valid PIN must be provided to the host Luna CA^3 token before access to private data and module services can be granted. For the SO, only a PIN is required.

Note: Normal users also have a text-based name associated with them. The name corresponding to a particular user number can be queried from the host Luna CA^3 token.

When in FIPS 140-1 Level 3 mode, the Luna XPplus uses indirect login through the secure pin port of a Luna CA^3 for login authentication. The following steps describe the procedure that must be followed to configure the Luna XPplus into FIPS 140-1 Level 3 mode:

- select a Luna CA^3 token to be used as the authentication token for the Luna XPplus;
- ensure the authentication token has been initialized and has a ‘User’ on it;
- open a session on the authentication token;
- login to the authentication token as ‘User’;
- indirectly initialize the Luna XPplus with a call to CA_InitIndirectToken;
- open a session on the Luna XPplus;
- login to the Luna XPplus as the SO using the call CA_IndirectLogin;
- create a user on the Luna XPplus using the call CA_InitIndirectPIN.

Note that a single Luna CA^3 token can be the authentication token for several Luna XPplus units. To accomplish this, indirectly initialize a number of Luna XPplus devices without re-initializing the authentication token.

If the authentication token for a Luna XPplus is inadvertently re-initialized, it will no longer function for authentication through indirect login with the Luna XPplus device. To continue using the Luna XPplus, perform the indirect initialization procedure again.

The Luna XPplus module implements policy that limits the number of login attempts. This feature prevents an exhaustive search approach for finding the PIN of the SO or user. When this policy is implemented it results in different effects for users and SOs.

For a user PIN search:

- If *"n"* consecutive user logon attempts fail, the token flags the event in the User's Authorization Vector (UAV). This erases the user's profile and private data from the token. The SO must create a new user, the new user will have no association with the deleted user. (The value of "n" is defined by the SO in the TPV.)

For an SO PIN search:

- If *"n"* consecutive SO logon attempts fail, the token is zeroized and its operational state goes to ZEROIZED. (The value of "n" is defined in the FPV, which is defined when Luna XPplus module is manufactured and cannot be modified without invalidating the CRC value of the software load.)

5. DISCRETIONARY ACCESS CONTROL (DAC)

Every data object on the token can be public or private. Private data objects are labeled with a number that corresponds to the owner and can be accessed only by the legitimate owner. A user cannot create a key or certificate object as a public object. Only data objects can be public or private.

The module does not allow for any granularity of ownership other than that of individual or public (i.e., a data object cannot be owned by two users and restricted from other users). Also, the ownership of an object implies read/write/modify/execute access to the object, which means full access rights to the object.

6. OBJECT REUSE

The module enforces an object reuse policy in that every object is allocated a portion of memory (flash or SRAM). The policy also ensures that no other objects are placed in the same memory location unless all previous memory content is initialized and purged. When cryptographic functions are performed, a cryptographic context is created to hold data required by the function (e.g., a DES key schedule for a DES function or a SHA-1 chaining vector). The cryptographic context only exists in SRAM memory and is not assigned to any functions except those defined by its owner. The memory assigned to a cryptographic context is always purged of its content before being handed over to a function.

7. PHYSICAL SECURITY

7.1. Meeting FIPS 140-1 Requirements

To meet the requirements for physical security for multiple-chip standalone cryptographic modules as set out by FIPS 140-1, security level 3, Chrysalis-ITS provides the following physical security mechanisms, see CR-0529:

- The Luna XPplus circuitry meets production quality standards using standard passivation techniques, and is implemented as a production-grade, multiple-chip embodiment.
- The Luna XPplus is contained within an enclosure with a removable cover that provides protection for the circuitry within the cryptographic boundary from environmental and physical damage (meets level 1).
- When maintenance is to be performed, all plaintext secret and private keys and other unprotected Critical

Security Parameters (CSPs) contained in the cryptographic module are zeroized automatically when the cover is removed (meets level 1).

- The Luna XPplus enclosure is opaque (meets level 2).
- Tamper-evident seals affixed to the bottom of the Luna XPplus enclosure will provide evidence of tampering if an attempt is made to remove the cover. Seals will cover one screw on each side of the bottom of the enclosure to ensure the unit may not be opened without tampering with the seals. In addition, the metal enclosure would be visibly damaged if access were to be attempted without removing all the cover mounting hardware (meets level 2).
- Removable screws that are outside the cryptographic boundary (such as those holding the enclosure to the bottom of the unit) are not protected in any special manner. Removable screws that are located within the cryptographic boundary are protected by closed/blind-threaded fasteners. (meets level 3).
- The Luna XPplus is contained within a strong metal enclosure (meets level 3).
- The Luna XPplus contains tamper response and zeroization circuitry that zeroizes all plaintext secret and private keys and other unprotected CSPs upon the removal of the cover. Furthermore, the circuitry is operational when the plaintext cryptographic keys or other unprotected CSPs are contained within the cryptographic module. The net result of zeroizing these parameters is that the appliance will cease to function (meets level 3).
- The Luna XPplus prevents undetected probing inside the enclosure by means of an interior baffle arrangement. This baffle arrangement either prevents or deflects any probe from accessing the hardware within the cryptographic boundary. This protection is not provided in front of the fan; instead, zeroization circuitry provides protection in this area. When a probe is inserted through the fan, the fan will stop. This stoppage is detected by the zeroization circuitry, which results in the plaintext cryptographic keys being zeroized (meets level 3).

For additional information about the physical security of the Luna XPplus, contact Chrysalis-ITS.

APPENDIX A. Cryptographic Algorithms Support

Encrypt/Decrypt:

- DES-ECB
- DES-CBC
- 3-DES-ECB
- 3-DES-CBC
- RC2-ECB
- RC2-CBC
- RC4
- RC5-ECB
- RC5-CBC
- CAST-ECB
- CAST-CBC
- CAST3-ECB
- CAST3-CBC
- CAST5-ECB
- CAST5-CBC
- RSA X-509

Digest:

- MD2
- MD5
- SHA-1

Sign/Verify:

- RSA -1024
- RSA -2048
- DSA
- DES-MAC
- 3-DES-MAC
- RC2-MAC
- RC5-MAC
- CAST-MAC
- CAST3-MAC
- CAST5-MAC
- SSL3-MD5-MAC
- SSL3-SHA1-MAC
- HMAC-SHA1
- HMAC-MD5

Generate Key:

- DES
- double length DES
- triple length DES
- RC2
- RC4
- RC5
- CAST
- CAST3
- CAST5
- PBE-MD2-DES
- PBE-MD5-DES
- PBE-MD5-CAST
- PBE-MD5-CAST3
- PBE-SHA-1-CAST5
- GENERIC-SECRET
- SSL PRE-MASTER

Generate Key Pair:

- RSA-1024
- RSA-2048
- DSA-1024
- DH-1024

Wrap Symmetric Key Using Symmetric Algorithm:

- DES-ECB
- 3-DES-ECB
- RC2-ECB
- CAST-ECB
- CAST3-ECB
- CAST5-ECB

Wrap Symmetric Key Using Asymmetric Algorithm:

- RSA-1024
- RSA-2048

Wrap Asymmetric Key Using Symmetric Algorithm:

- 3-DES-CBC[1]

Unwrap Symmetric Key With Symmetric Algorithm:

- DES-ECB
- 3-DES-ECB
- RC2-ECB
- CAST-ECB
- CAST3-ECB
- CAST5-ECB

Unwrap Symmetric Key With Asymmetric Algorithm:

- RSA-1024
- RSA-2048

Unwrap Asymmetric Key With Symmetric Algorithm:

- DES-CBC
- 3-DES-CBC
- CAST-CBC
- CAST3-CBC
- CAST5-CBC

Derive Key Value:

- DH-1024
- concatenate Base & Key
- concatenate Base & Data
- concatenate Data & Base
- XOR Base and Data
- Extract Key from Key
- MD2 Derivation
- MD5 Derivation
- SHA-1 Derivation
- SSL3-Master
- SSL3-Key & MAC

[1] Although this is a mechanism that is supported by the base firmware, the FPV settings for CA3 and XPPlus prevent wrapping of asymmetric private keys.

APPENDIX B. Policy Vector Settings

	Standard Luna Domestic	Standard Luna Export
Token Policy Vector Settings		
TPV_USER_ZEROIZE	1	1
TPV_USER_FW_UPDATE	0	0
TPV_M_OF_N_ACTIVATION	0	0
TPV_KEY_ATTRIB_LOCK	1	1
TPV_KEY_SINGLE_FUNCTION	0	0
TPV_SIGNING_KEY_LOCAL	0	0
TPV_MAX_PIN_LEN	48	48
TPV_MIN_PIN_LEN	4	4
TPV_LOGIN_FAILS_ALLOWED	10	10
TPV_DISABLE_CLONING_BY_USER	0	0
Fixed Policy Vector Settings		
FPV_SECURITY_POLICY_DOMESTIC	1	0
FPV_SECURITY_POLICY_ENABLE_CLONING	1	1
FPV_SECURITY_POLICY_USE_CAV	0	0
FPV_SECURITY_POLICY_WRAPPING_TOKEN	0	0
FPV_SECURITY_POLICY_USE_M_OF_N	1	1
FPV_SECURITY_POLICY_USE_RAW_RSA	1	1
FPV_SECURITY_POLICY_SPECIAL_CLONING	1	1
FPV_ENABLE_CCM	0	0
FPV_SEC_KEY_POLICY_SENSITIVE	1	1
FPV_SEC_KEY_POLICY_NO_CREATE	1	1
FPV_PRI_KEY_POLICY_SENSITIVE	1	1
FPV_PRI_KEY_POLICY_NO_CREATE	1	1
FPV_SO_LOGIN_FAILS_ALLOWED	3	3
FPV_PIN_MUST_USE_SP	0	0
FPV_MOFN_MUST_USE_SP	0	0
FPV_KCV_MUST_USE_SP	0	0
FPV_XP_TOKEN	1 if XP Style Token	1 if XP Style Token
FPV_XPPLUS_TOKEN	1 if XPplus Token	1 if XPplus Token

APPENDIX C. Session And Login States Required For Luna Commands

Command To Module	No Session Open	Session Open, No Login	SO Logged On	User Logged On
Token Main Module Commands				
LUNA_ZEROIZE	√			
LUNA_INIT_TOKEN			√	
LUNA_GET	√			
LUNA_GET_USV			√	
LUNA_SET_TPV			√	
LUNA_FW_UPDATE			√	
LUNA_CONFIGURE_SP	√			
Session Manager Commands				
LUNA_OPEN_ACCESS	√			
LUNA_CLEAN_ACCESS	√			
LUNA_CLOSE_ACCESS	√			
LUNA_GET_ALL_ACCESSES	√			
LUNA_OPEN_SESSION	√			
LUNA_CLOSE_SESSION		√		
LUNA_CLOSE_ALL_SESSIONS	√			
LUNA_GET_SESSION_INFO		√		
LUNA_EXTRACT_CONTEXTS		√		
LUNA_INSERT_CONTEXTS		√		
User Module Commands				
LUNA_GET_USER_LIST		√		
LUNA_GET_USER_NAME		√		
LUNA_LOGIN		√		
LUNA_LOGOUT				√
LUNA_SET_PIN				√
LUNA_INIT_PIN			√	
LUNA_CREATE_USER			√	
LUNA_DELETE_USER			√	
Object Management Module				
LUNA_CREATE_OBJECT		√		
LUNA_COPY_OBJECT		√		
LUNA_DESTROY_OBJECT		√		
LUNA_GET_OBJECT_SIZE		√		
LUNA_GET_ATTRIBUTE_VALUE		√		
LUNA_GET_ATTRIBUTE_SIZE		√		
LUNA_MODIFY_OBJECT		√		
LUNA_FIND_OBJECTS		√		
Random Number Generator Module				
LUNA_GET_RANDOM		√		
LUNA_SEED_RANDOM		√		
Key Management Module				
LUNA_GENERATE_KEY				√
LUNA_GENERATE_KEY_W_VALUE				√
LUNA_GENERATE_KEY_PAIR				√
LUNA_WRAP_KEY				√
LUNA_UNWRAP_KEY				√
LUNA_UNWRAP_KEY_W_VALUE				√
LUNA_DERIVE_KEY				√
LUNA_DERIVE_KEY_W_VALUE				√
LUNA_MFG_LOAD				√

Command To Module	No Session Open	Session Open, No Login	SO Logged On	User Logged On
Cryptographic Algorithm Module				
LUNA_ENCRYPT_INIT				√
LUNA_ENCRYPT_INIT_W_VALUE				√
LUNA_ENCRYPT_INIT				√
LUNA_ENCRYPT_INIT_W_VALUE				√
LUNA_ENCRYPT				√
LUNA_ENCRYPT_FIFO				√
LUNA_ENCRYPT_END				√
LUNA_DECRYPT_INIT				√
LUNA_DECRYPT_INIT_W_VALUE				√
LUNA_DECRYPT				√
LUNA_DECRYPT_FIFO				√
LUNA_DECRYPT_END				√
LUNA_DECRYPT_RAW_RSA				√
LUNA_DIGEST_INIT		√		
LUNA_DIGEST		√		
LUNA_DIGEST_FIFO		√		
LUNA_DIGEST_KEY				√
LUNA_DIGEST_KEY_VALUE				√
LUNA_DIGEST_END		√		
LUNA_SIGN_INIT				√
LUNA_SIGN_INIT_W_VALUE				√
LUNA_SIGN				√
LUNA_SIGN_FIFO				√
LUNA_SIGN_END				√
LUNA_SIGN_SINGLEPART				√
LUNA_SIGN_UPDATE_KEY				√
LUNA_SIGN_FINAL_DERIVE_KEY				√
LUNA_VERIFY_INIT				√
LUNA_VERIFY_INIT_W_VALUE				√
LUNA_VERIFY				√
LUNA_VERIFY_FIFO				√
LUNA_VERIFY_END				√
LUNA_VERIFY_SINGLEPART				√
LUNA_GET_MECH_LIST	√			
LUNA_GET_MECH_INFO	√			
LUNA_SELF_TEST	√			
LUNA_SET_UP_MASKING_KEY	√			
LUNA_CLONE_AS_SOURCE				√
LUNA_CLONE_AS_TARGET_INIT				√
LUNA_CLONE_AS_TARGET				√
LUNA_GEN_TKN_KEYS			√	
LUNA_LOAD_CERT			√	
LUNA_GEN_KCV				√
LUNA_LOAD_CUSTOMER_VERIFICATION_KEY			√	
LUNA_M_OF_N_GENERATE			√	
LUNA_M_OF_N_ACTIVATE				√
LUNA_M_OF_N_MODIFY			√	
Special Packet Processing Commands				
LUNA_IPSEC_INIT_NO_USER	√			
LUNA_IPSEC_PROCESS_PACKET	√			
LUNA_IPSEC_END	√			
LUNA_GEN_CRC32	√			

Command To Module	No Session Open	Session Open, No Login	SO Logged On	User Logged On
LUNA_SCP_TEST	√			