PrimeKey Labs GmbH
Secure Execution Environment (SEE) Loader

FIPS 140-2 Non-Proprietary Security Policy

Hardware versions: 1.0.0 and 1.0.1

Firmware version: V1.0.2-FIPS

Date: 07/30/2021

Prepared By:

2400 Research Blvd, Suite 395
Rockville, MD 20850
tel: +1 (703) 375-9820
info@acumensecurity.net
www.acumensecurity.net

About this Document

This non-proprietary Cryptographic Module Security Policy for the Secure Execution Environment (SEE) Loader from PrimeKey Labs GmbH (also referred to herein as PrimeKey) provides an overview of the product and a high-level description of how it meets the overall Level 3 security requirements of FIPS 140-2.

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment Canada (CSE) Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. The NVLAP accredits independent testing labs to perform FIPS 140 testing; the CMVP validates modules meeting FIPS 140 validation. Validated is the term given to a module that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at:
http://csrc.nist.gov/groups/STM/cmvp/index.html

SEE Loader may also be referred to as the “module” in this document.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. PrimeKey shall have no liability for any error or damages of any kind resulting from the use of this document.

Notices

This document may be freely reproduced and distributed in its entirety without modification.

Table of Contents

Public Material – May be reproduced only in its original entirety (without revision).

List of Tables

List of Figures

Public Material – May be reproduced only in its original entirety (without revision).

1. Introduction

1.1 Scope

This document describes the cryptographic module security policy for the Primekey Labs GmbH Secure Execution Environment (SEE) Loader cryptographic module with firmware V1.0.2-FIPS (also referred to as the “module” hereafter). It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-2 standard.

1.2 Overview

The SEE Loader module is a multi-chip embedded module that is used for providing functionality for the secure loading of applications and ensuring the integrity of any loaded application required by the module’s operation. All such applications to be loaded by the module shall be signed by PrimeKey.

The secure loading includes verifying the signature of an application. This is achieved by the Boot Loader executing the following steps:

- Utilizing the Application Provider (AP) Public Key;
- Verifying the Application Provider (AP) Public Key using the Production Authority (PA) Public Key;
- Computing the Application hash; and
- Verifying the hash signature using the Application Provider (AP) Public Key.

This mechanism ensures that only applications signed by the Application Provider can be loaded in the SEE Loader module.

The validation is only for the SEE Loader firmware version V1.0.2-FIPS and hardware versions 1.0.0 and 1.0.1. It does not include the loaded SEE primary or SEE secondary firmware or applications. The cryptographic functions in the loaded firmware and applications have not been tested or validated as part of the SEE Loader module validation. Once control passes from the Loader to the application (an application has been started), the module is no longer validated. Any future validation scenario whereby an application is included as part of the cryptographic boundary will be validated separately from this validation.

Public Material – May be reproduced only in its original entirety (without revision).

1.3 Glossary

Term	Description
AP	Application Provider
ATX	Advanced Technology eXtended
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standard
GPIO	General Purpose Input/Output
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
PA	Production Authority
PiLO	PrimeKey Integrated Lights Out
RAM	Random Access Memory
RSA	Rivest, Shamir, and Adleman
SATA	Serial Advanced Technology Attachment
SEE	Secure Execution Environment
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard

Table 1 - Glossary of Terms

Public Material – May be reproduced only in its original entirety (without revision).

2. Security Level

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
Electromagnetic Interference / Electromagnetic Compatibility	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall Level	3

Table 2 – FIPS 140-2 Target Level

Public Material – May be reproduced only in its original entirety (without revision).

3. Cryptographic Module Specification

3.1 Cryptographic Boundary

The SEE Loader module is a multi-chip embedded hardware cryptographic module residing within a PrimeKey SEE appliance (note: the appliance is not included in the scope of the SEE Loader validation). The cryptographic boundary of the module is defined to encompass all components inside of the metal shielding/walls and hard epoxy resin potting material shown in Figures 2, 3, 4 and 5. The Figure below shows the positioning of the SEE Loader module in its host PrimeKey SEE appliance.

Figure 1 - PrimeKey SEE Appliance

As shown in the Figures below, the module is entirely encapsulated in potting material and the sides and bottom are also protected by a metal walls which obscures visibility to all the electronic components.

Figure 2. Front of the Secure Execution Environment (SEE) Loader

Public Material – May be reproduced only in its original entirety (without revision).

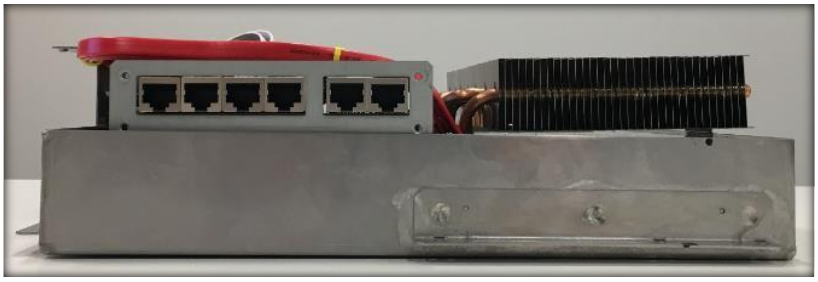

Figure 3. Back of Secure Execution Environment (SEE) Loader

Figure 4. Left Side of the Secure Execution Environment (SEE) Loader

Figure 5. Right Side of the Secure Execution Environment (SEE) Loader

Public Material – May be reproduced only in its original entirety (without revision).

Figure 6. Top View of the Secure Execution Environment (SEE) Loader

Figure 7. Bottom View of the Secure Execution Environment (SEE) Loader

Public Material – May be reproduced only in its original entirety (without revision).

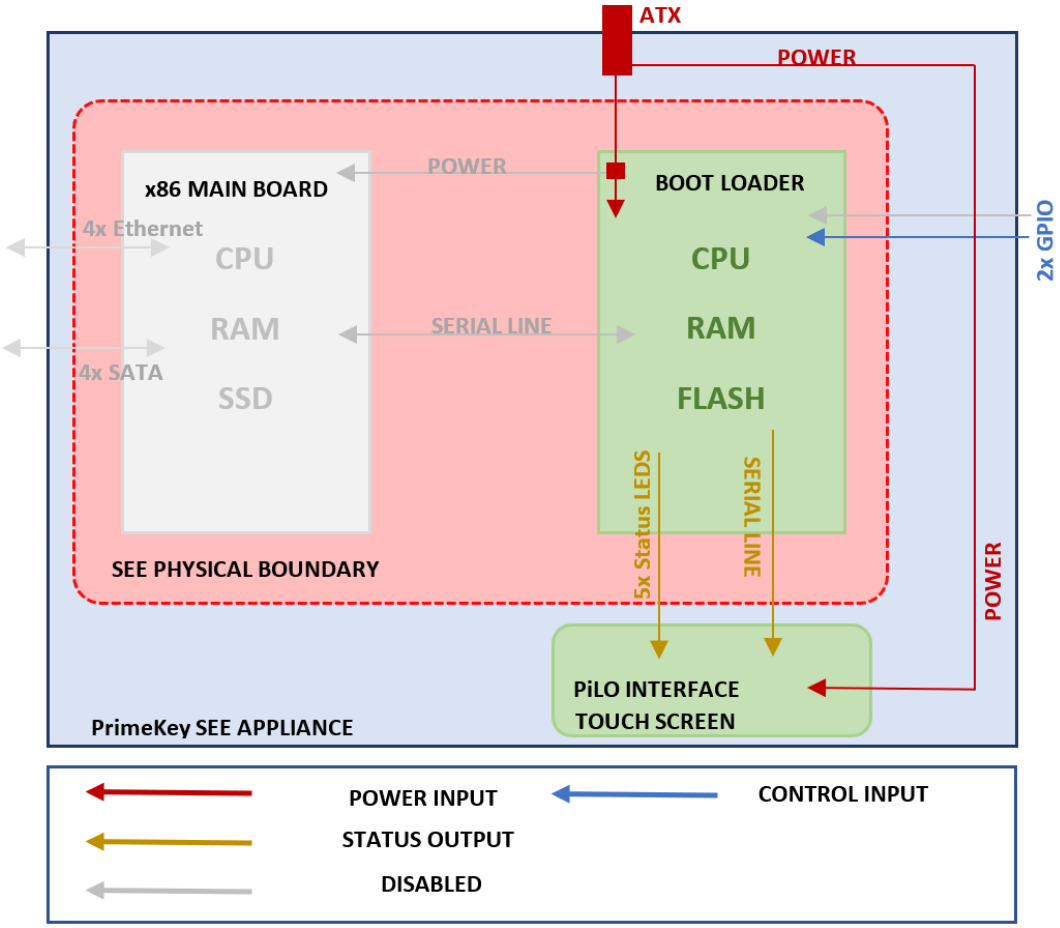

Figure 8 – Block Diagram for SEE Loader Cryptographic Boundary

The area shown to be in red in Figure 8 is encapsulated in hard epoxy resin and surrounded by three hard metal shields which cover the sides and bottom of the module.

4. Cryptographic Module Ports and Interfaces

The following table shows how the physical ports map to the logical interfaces of the module in Figure 2:

Physical Port	FIPS 140-2 Logical Interface Mapping
GPIO Pin (Used for FIPS GPIO Zeroize Input)	Control Input
PiLO Serial Line	Status Output
ATX Power connector	Power In
5x LED Status lines	Status Output
4x SATA Connectors	Not used by the module
4 Ethernet Ports	Not used by the module
GPIO Pin	Not used by the module

Table 3 - Physical Port and Logical Interface Mapping

Public Material – May be reproduced only in its original entirety (without revision).

4.1.1 GPIO Pin

The module uses a GPIO pin for the FIPS GPIO Zeroize Input function. Once this function is initialized the module proceeds to remove all data within the secured storage area of the Flash partitions.

4.1.2 Serial Line

The Serial Line is used for status output. Status output from the “Boot Loader” is sent via the serial line to the PiLO touch screen on the host PrimeKey SEE appliance.

4.1.3 PiLO Power

The PiLO Power output provides power to the PiLO board and touchscreen on host appliance. This power is available directly from the ATX Power Interface.

4.1.4 ATX Power

The ATX Power input is used to supply power to the module.

4.1.5 LED Status lines

The five (5) LED status lines from the module connect to three (3) LEDs located on the front panel of the host appliance as shown in Figure 8 below:

Figure 9 - Status LEDs on the PrimeKey Appliance

- FIPS Status – This LED will turn Red when power is applied. Then will transition to Yellow when loading its firmware and to Blue once its power-up self-tests have completed successfully. Upon successful verification of the application images the LED will turn Green.
- SEE Operational – This LED will turn solid Green once the SEE primary firmware is loaded.
- Zeroized – This LED will turn solid Green after zeroization has been invoked and the module has rebooted.

Public Material – May be reproduced only in its original entirety (without revision).

5. Roles, Services and Authentication

5.1 Roles and Authentication

The SEE Loader module supports an authentication mechanism relying on RSA signature verification. This authentication mechanism applies for secure loading and secure starting of an application. Two components are involved in this authentication mechanism, the Production Authority (PA) Key and the signature of an Application.

Role	Type of Authentication	Authentication Data
Application Provider (User)	Identity Based	3072-bit RSA Public Key
Production Authority (Crypto Officer)	Identity Based	3072-bit RSA Public Key

Table 4 - Roles and Authentication Data

An Application Provider (User) is authenticated with an RSA 3072-bit Production Authority (PA) Public Key before the Primary and Secondary SEE firmware images are validated and the provided application is started. If the signatures can be validated, the application can be started by the module.

New applications may be generated and signed by the Application Provider using the AP Private Key that is held securely by Application Provider.

Authentication of the Crypto Officer is provided by secure manufacturing procedures at the factory.

The strength associated with the authentication methods can be found in Table 5 below.

Type of Authentication	Authentication Strength
Production Authority (PA) Public Key	The module uses 3072-bit RSA keys for authentication, which has an associated false acceptance or random-access rate which is well less than one in 1,000,000. Per NIST SP 800-57 Pt. 1 Rev. 4, a 3072-bit RSA key is regarded to have 128-bits of equivalent security strength. The probability of a successful random attempt is 1/2^128, which is less than 1/1,000,000. Assuming the module can only perform one (1) digital signature verification per second, the probability of a success with multiple consecutive attempts in a one-minute period is 60/2^128, which is less than 1/100,000.
Application Provider (AP) Public Key	The module uses 3072-bit RSA keys for authentication, which has an associated false acceptance or random-access rate which is well less than one in 1,000,000. Per NIST SP 800-57 Pt. 1 Rev. 4, a 3072-bit RSA key is regarded to have 128-bits of equivalent security strength.

Public Material – May be reproduced only in its original entirety (without revision).

	The probability of a successful random attempt is 1/2^128, which is less than 1/1,000,000. Assuming the module can only perform one (1) digital signature verification per second, the probability of a success with multiple consecutive attempts in a one-minute period is 60/2^128, which is less than 1/100,000.

Table 5 - Strength of Authentication

The Crypto Officer role involves the loading of a 3072-bit Production Authority (PA) key into the module at the factory. The PA Public Key is used by the module to verify the signature chain on any application that it loads. An authorized Crypto Officer performs the loading of the PA Public Key at the factory. Once the module is fielded, the signed Application and Application Provider (AP) Public Key are verified as part of the "Application and AP Public Key Load" service.

This is the only cryptographic application offered by the module's software.

5.2 Services

The SEE Loader module provides secure loading and storage of signed applications. In addition, the module offers the following services.

Service	User	Crypto Officer	Unauthenticated
Show Status		X	
Application and AP Public Key Load		X	
Application Start	X		
On-Demand Self-test	X	X	
FIPS GPIO Zeroize			X

Table 6 - Approved Services and Role allocation

The Application and AP Public Key Load Service controls the loading of the application and the Application Provider (AP) Public Key. When an application is loaded, the Boot Loader verifies the chain of signatures. If an error occurs during loading, the application is not loaded, and the module reports the error to the User on the serial port and the status lines to the LED on the host appliance.

When the Application Start Service is invoked the module transfers the control to the application after it has been successfully loaded.

6. Physical Security

The module is a multiple-chip embedded cryptographic module made with production grade components and standard passivation.

The module's cryptographic boundary is defined to be the outer perimeter of the hard epoxy enclosure containing the module's hardware and firmware components. The module is opaque and completely

Public Material – May be reproduced only in its original entirety (without revision).

conceals the internal components of the cryptographic module. The epoxy enclosure of the module prevents physical access to any of the internal components without having to destroy the module.

7. Operational Environment

The FIPS 140-2 Section 6 Operational Environment requirements are not applicable because the cryptographic module supports a non-modifiable operational environment.

Public Material – May be reproduced only in its original entirety (without revision).

8. Cryptographic Algorithms and Key Management

8.1 Cryptographic Algorithms

The module implements the following Approved algorithms in the module's firmware:

CAVP Cert #	Algorithm	Standard	Mode/Method	Use
2990	RSA	FIPS 186-4	Mod: 3072 Signature Verification, Public Key Validation	Digital Signature Services
4464	SHS	FIPS 180-4	Byte Oriented SHA-256	Digital Signature Verification

Table 7 - Approved Algorithms

8.2 Cryptographic Key Management

All keys and the Primary and Secondary SEE firmware images are stored in flash memory. The flash memory is protected by the physical security mechanisms described in Section 6. However, disclosure of the PA Public Key shall not be considered as a security risk. The public key cannot be used for signing an application.

The signature of the Application is a security related data. However, it shall not be considered as a Critical Security Parameters (CSPs) as disclosing it is not a security risk.

There are no Critical Security Parameters (CSPs) associated to the module but the SEE Loader Cryptographic Module offers a secure storage area for CSPs of the loaded Application. None of the Keys listed in Table 8 are loaded in the field.

Keys	Description	Algorithm and Key Size	Generation	Role	Storage
Production Authority (PA) Public Key	Authenticates the Crypto Officer (AP Public signature verification)	RSA 3072	Outside of Module	Crypto Officer	Flash, write protected
Application Provider (AP) Public Key	Authenticates the Application Provider (AP) (verification of the signature of the Application)	RSA 3072	Outside of Module	User	Flash, signed by PA private key

Table 8 - Approved Keys and CSPs Table

The module implements the following access control policy on keys and CSPs shown in the following table. The access policy is noted by R=Read, W=Write and X=Execute.

Module Service	CSP Access	Rights (R/W/X)
Show Status	N/A	N/A
Application and AP Public Key Load	RSA Public Key (PA)	X
Application Start	RSA Public Key (AP)	X

Public Material – May be reproduced only in its original entirety (without revision).

On-Demand Self-test	N/A	N/A
FIPS GPIO Zeroize	RSA Public Key (AP)	R, W

Table 9 - Approved Service to Key/CSP Mapping

8.3 Zeroization

Zeroization can be performed by holding down the zeroization button which activates the GPIO pin connected to the processor of the module. This process zeroizes AP key and the primary and secondary SEE operational images. Once the zeroize function has been completed, the device will no longer be operable. The device is to be returned to the manufacturer who can re-initialize the device.

9. Self-tests

FIPS 140-2 requires the module to perform self-tests to ensure the module integrity and the correctness of the cryptographic functionality at start up. Some functions require conditional tests during normal operation of the module.

When the self-tests pass successfully the GPIO pins output status to turn the LED blue on the host appliance.

If any of the tests fails, the module enters an error state where no functions can be executed. The module may be rebooted to attempt to clear the error. If the error persists, then the module should be returned to manufacturer for repair.

9.1 Power-On Self-Tests

Power-on self-tests are run upon the initialization of the module and do not require operator intervention to run. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module.

The module implements the following power-on self-tests:

Type	Test
Integrity Test	• SHA-256 EDC over the executable firmware image
Known Answer Test	• RSA 3072-bit PKCS1.5 signature verification KAT • RSA 3072-bit PSS signature verification KAT • SHA-256 KAT

Table 10 - Power-up Self-tests

9.2 Conditional Self-Tests

Conditional self-tests are test that run during operation of the module. The module performs the following conditional self-test:

Type	Test Description
Application Load Test	RSA Signature Verification operation performed prior to loading an application.

Table 11 - Conditional Self-tests

Both the “Application Start” and “Application and AP Public Key Load” services include conditional tests performed sequentially:

Public Material – May be reproduced only in its original entirety (without revision).

- The Boot Loader verifies the Application Provider's Public Key signature using the Production Authority (PA) Public Key stored in the module.
- The Boot Loader verifies the primary and secondary SEE firmware images using the Application Provider (AP) Public Key stored in the module.
- The Boot Loader then verifies the application's signature using the Application Provider's (AP) Public Key.

To verify signatures, the Boot Loader computes a hash using SHA-256 according to FIPS 180-4. The hash function is used by the RSA signature verification algorithm according to either RSASSA-PKCS1- v1_5 or RSASSA-PSS.

If one of these tests fail, the module will transition to an error state and will be inoperable until the module is rebooted.

If all the tests pass, the application verification is successful.

10. Guidance and Secure Operation

There is no FIPS 140-2 specific guidance required to place the module into its Approved mode of operation. The FIPS 140-2 functional requirements are always invoked.

As stated above, the SEE primary and secondary firmware images and Applications developed by Application Providers and intended to execute with SEE Loader module are not included as part of this validation.

Public Material – May be reproduced only in its original entirety (without revision).