Cryptographic Module Security Policy For **Outbacker MXP**

(Non-Proprietary)

FIPS 140-2 Validation

Table of Contents

1 General

1.1 Revision History

Author	Date	Version	Description of Change
J. Sheehy	May 14, 2007	1.0	Initial Draft
J. Sheehy	July 3, 2007	1.1	Updated Firmware Version to 4.19
J. Sheehy	July 12, 2007	1.2	Updated based on feedback from FIPS lab.
L. Hamid	May 26, 2008	1.3	Updated for new hardware
L. Hamid	June 2, 2008	1.4	Incorporate feedback from EWA
L. Hamid	August 25, 2008	1.5	Responded to comments from CMVP

1.2 References

Reference	Title	Author
P1	FIPS PUB 140-2 Security Requirements for Cryptographic Modules	NIST
P2	X9.31 Digital Signatures using Reversible Public Key Cryptography for the Financial Services (DSA)	ANSI

2 Overview

2.1 Purpose

This document contains the Security Policy for Outbacker MXP. It is meant for public consumption and was written to provide a specification of the cryptographic security that will allow individuals and organizations to determine whether a cryptographic module, as implemented, meets a stated security policy. It describes to individuals and organizations the capabilities, protection, and access rights provided by the cryptographic module, thereby allowing an assessment of whether the module will adequately serve the individual or organizational security requirements.

2.2 Scope

This document is based on the requirements and expectations outlined in the FIPS 140-2 specification. This document applies specifically to Outbacker MXP with the following versions:

Hardware:

- Version 1.0 Outbacker MXP 80 GB
- Version 1.0 Outbacker MXP 120 GB
- Version 1.0 Outbacker MXP 160 GB
- Version 1.0 Outbacker MXP 250 GB
- Version 1.0 Outbacker MXP 320 GB

MXI AES: Part # 933000334R Version 1.0

Boot loader: Version 2.1

Firmware: Version 4.23

This document describes the identification and authentication policy, the access control policy, the physical security policy and a security policy for mitigation of other attacks. It also details the roles and services provided by Outbacker MXP and the types of services each role may access.

3 Introduction

Outbacker MXP is a multiple-chip standalone cryptographic module. Specifically, it is a USB mass storage device which implements hardware encryption dependent on user authentication. It provides not only secure encrypted storage, but management of digital identity credentials used for authentication and verification to enterprise and personal services.

As a digital identity and strong authentication device, Outbacker MXP is bound to users with authentication mechanisms that include password, biometric, and both in combination. Outbacker MXP can also provide Portable Security Token Service (PSTS) for WS-Trust Request Security Token messages.

Outbacker MXP offers a host general purpose and industry standard cryptographic services including the following

- Random number generation
- Key generation with internal or external entropy
- Symmetric encryption/decryption (AES)
- Asymmetric signing and verification (RSA)
- Asymmetric encryption and decryption (RSA) – Note: RSA encryption and decryption are non-FIPS approved services.
- Open Authentication HMAC (keyed-hash message authentication code)
- One Time Password (OATH HOTP)
- Secure hash (SHA-1 and SHA-256) and
- Compliance with industry standards such as ANSI X9.31, PKCS #1 (Public-Key Cryptography Standards) and SAML 1.1.

Outbacker MXP provides seamless encryption (AES 256) of hard drive memory storage up to 320GB which is user bound via strong two-factor authentication (biometric identification with verification and password). Outbacker MXP supports the enrollment of 5 users and 6 fingerprints.

The Outbacker MXP makes use of a user-mode communication protocol providing true zero footprint mode – no software installation and no administrator rights required on the host PC.

Figure 1: Photograph of Outbacker MXP

The Outbacker MXP is designed to be a FIPS 140-2 Level 2 cryptographic module for the storage of user credentials and file systems. Unless performing non-FIPS approved functions, the device will remain in the "FIPS Approved" mode of operation. The box marked "Outbacker MXP" in the diagram below represents the device enclosure and all internal components of the Outbacker MXP. As a stand-alone system, the physical boundary of the device is the cryptographic boundary as outline by the red marking.

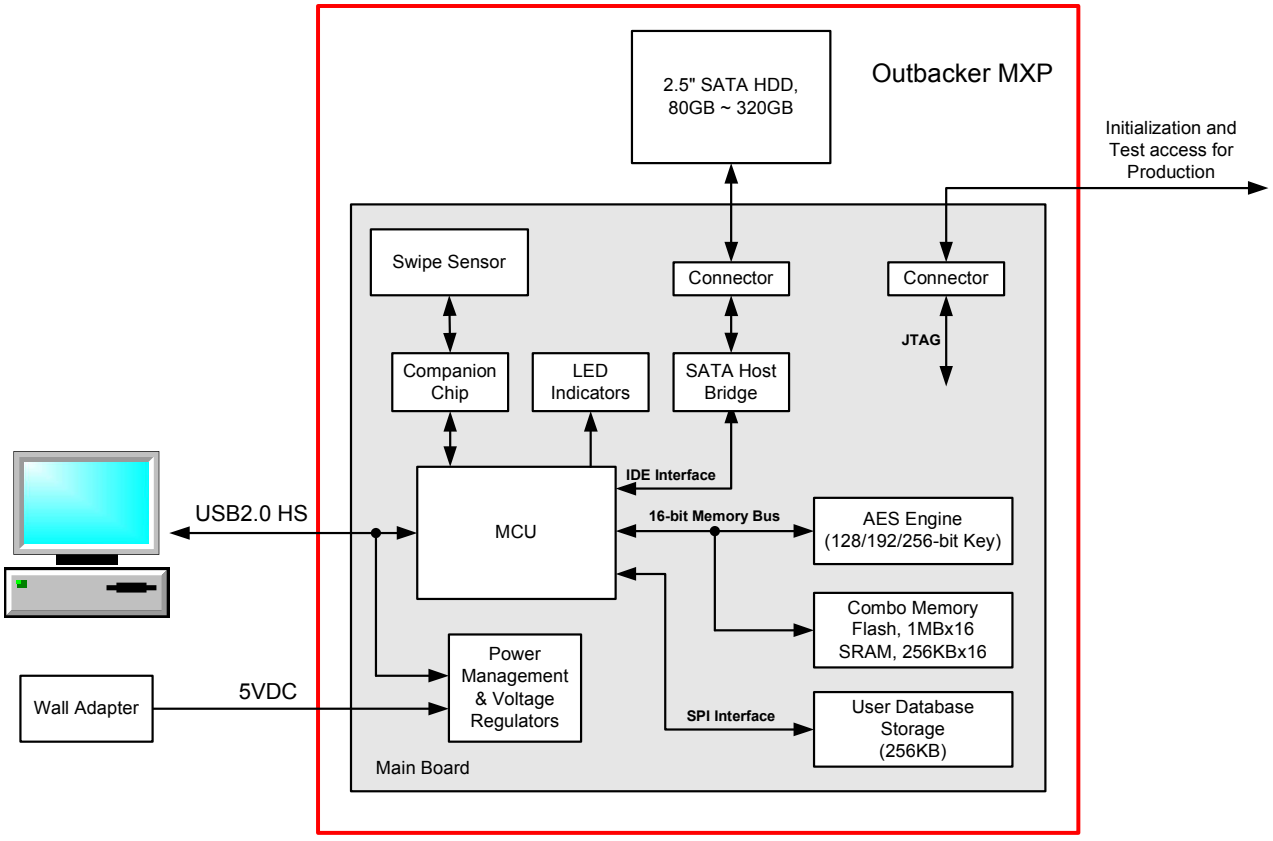

Figure 2: Block Diagram of Outbacker MXP

4 Security Levels

The Outbacker MXP meets an overall security FIPS 140-2 Level 2. The FIPS 140-2 specification defines security requirements that are grouped into Security Requirement Areas. These areas are tested individually for a specific level of achievement. The table below defines the targeted level in each section for the Outbacker MXP.

Table 1 : FIPS 140-2 Security Requirement Levels

FIPS 140-2 Security Requirement Section	Target Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

5 Ports and Interfaces

There are four physical ports on the Outbacker MXP module: a High Speed Universal Serial Bus (USB 2.0) port, a UPEK TouchStrip Fingerprint swipe sensor, status LEDs, and a socket for an external power supply.

A secure port (Secure Channel) is implemented by using an encrypted session between the device and the host. It uses AES encryption with a session key that is generated using random data by both the device and host, exchanged using public keys of the device and the host. This is used to protect data exchanged between host and device. Any command sent to the device can then be protected in the secure port by using the new session identifier.

The secure port key exchange works as follows:

1) Random data is generated by the device (device-random). 32 bytes of data is generated on the device by reading from the device's hardware entropy generator.
2) Random data is generated by the host (host-random). 32 bytes of data is generated using the OpenSSL PRNG, running on the host machine.
3) Device-random is encrypted with the host's RSA public key and sent to the host
4) Host-random is encrypted with the device's RSA public key and sent to the device.
5) The host and the device each decrypt the exchanged random information
6) The host and the device each concatenate host-random and device-random and use the result to seed a PRNG.
7) The secure session key is derived by the host and device using the seeded PRNG.

The following lists the mapping of FIPS 140-2 logical interfaces to physical ports on the Outbacker MXP module.

Table 2: Logical Interface Description

Logical Interface	Physical Ports
Data Input	USB
	UPEK Swipe Sensor
Data Output	USB

Control Input	USB
Status Output	USB
	LEDs
Secure Channel Input (Wrapper of Data and Control) – Input to the device using Secure Channel to protect the communication channel	USB
Secure Channel Output (Wrapper of Data and Status) – Output from the device using Secure Channel to protect the communication channel	USB
Power	USB (Bus powered from host or hub) or (optionally) an external power supply (wall adapter)

6 Cryptographic Key Management

6.1 Critical Security Parameters

The Outbacker MXP module contains the following Critical Security Parameters. These are referred to in the Identification and Authentication Policy and the Access Control Policy. Each parameter gives details about the relative generation, establishment, distribution, entry/output, storage and zeroization mechanisms.

6.1.1 Fingerprint Templates

Outbacker MXP stores enrolled fingerprint templates in non-volatile memory within a dedicated ASIC for fingerprint processing. There is no direct interface to this non-volatile memory. The templates are created in the ASIC during enrollment and never leave that device. Verification and identification operations are performed within that module. All templates associated with a user are deleted upon removal of that user.

6.1.2 Passwords

Passwords are injected upon creation from the external USB interface. A random salt is also injected as plain text through the USB interface and stored in EEPROM. The password is combined with the salt, then hashed using the SHA256 algorithm and stored in EEPROM associated with the user. The password is then deleted from memory. Password authentication and verification is done by comparing the hash of the trial password combined with the salt with the stored hash. The salt and the resulting hash are zeroized when the user is deleted from the device.

6.1.3 Random Numbers

Outbacker MXP contains a random number generator that uses an internal, unpredictable physical source of entropy that is outside of human control. This source of random numbers is also available as an external service for general use, separate from the internal service. Random numbers generated by this physical source are sometimes used as part of a seed value for the FIPS approved pseudo-random number generator (ANSI X9.31 Appendix A.2.4 Using AES). Each time a random number is used for any purpose, it is compared to the previously used value to ensure it is different and then stored until the next use.

6.1.4 AES Device Master Key

Outbacker MXP stores one AES 256-bit Device Secret Key that is created upon initialization of the module. This key is used to encrypt the key storage area and the public storage area. The Device Master Key, which is generated using the FIPS-approved Random Number Generator, is stored in EEPROM, does not leave the device and is not available for external services. When the device is recycled, this key is zeroized and therefore the storage areas become invalid. Because the Master key is only used to encrypt keys for storage, it does not actually need to be zeroized because all keys secured with this key can be overwritten. A new master key is created at the end of the recycle operation.

6.1.5 AES User Master Keys

Outbacker MXP stores one AES Key, known as a User Master Key, for each operator that is defined on the device. This key is used for bulk encryption and decryption of the operator's mass storage partition, private store and any other keys belonging to that operator. AES User Master Keys are either injected onto the device (through the USB interface as plain text assuming that Secure Channel is not being used) from the host system or generated on the device. They can be 128, 192 or 256 bits long. This type of key is generated by the FIPS approved ANSI X9.31 pseudo-random number generator. AES User Master Keys are stored within the module and never leave the module. They are zeroized upon user deletion. Note that even though the key is stored encrypted, it is considered to be stored as plain text according to FIPS 140-2 because the key used to encrypt them is not generated by a FIPS approved method.

6.1.6 AES User Secret Keys

Outbacker MXP stores AES keys, known as User Secret Keys. Each operator may own zero or a few such keys and they can only be used by an authenticated operator. AES User Secret Keys are either injected onto the device (through the USB interface as plain text assuming that Secure Channel is not being used) from the host system or generated on the device by the FIPS approved ANSI X9.31 pseudo-random number generator algorithm. The keys can be 128, 192 or 256 bits long and never leave the module. They are encrypted with the AES User Master Key and stored on the portable hard drive. When a user is deleted, the AES User Master Key is zeroized and therefore the users AES User Secret Keys cannot be decrypted.

6.1.7 PSTS Services

MXI and Microsoft are jointly developing an open standard called Portable Security Token Service (PSTS) that specifies how CardSpace can be managed on portable devices that are capable of issuing SAML tokens. The standard provides ability for a device to be able to support a sub set of WS-Trust standard.

PSTS services of the device are non-FIPS Approved services and thus the following PSTS keys are not to be used in a FIPS-Approved mode of operation.

6.1.7.1 PSTS Credential Master Keys

Credential Master Keys are seed keys (maximum size of 256 bytes) that are used to generate PSTS Private Keys. Each operator of the module may have 1 or more PSTS credential and using them requires authenticated access. There is one Credential Master Key bound to each PSTS credential. Unlike random number seeds Credential Master Keys are injected into the device (through the USB interface as plain text assuming that Secure Channel is not being used) from the host system and are not erased unless the associated credential is erased. They are stored in EEPROM and never leave the module. When the user is deleted, the Credential Master Keys belonging to that user are zeroized.

6.1.7.2 PSTS Private Keys

PSTS Private Keys are 2048 bit RSA keys that are generated internally from Credential Master Keys following the X9.31 [P2] specification. There can be many PSTS Private Keys associated with each credential. Each different PSTS Private Key is bound to a Credential and a PSTS Target Service. PSTS Private Keys are stored on the flash memory, encrypted by the AES User Master Key, and never leave the module. When the user is deleted the AES User Master Key is deleted and therefore the PSTS Private Keys cannot be decrypted.

6.1.8 RSA Private Keys

RSA Private Keys are the private portion of an RSA key pair. RSA key pairs that are used for X9.31 [P2] operations are generated internally following the ANSI X9.31 specification. RSA key pairs that are used for PKCS#1 operations are generated internally using the RSA key generation mechanism of OpenSSL. There are two types of RSA private keys: Device and User keys. The Device and User keys are to be set exclusively for general purpose encryption/decryption or else sign/verify purpose. Private keys can be 1024, 2048, or 3072 bits in length. They can either be generated on the device or injected (through the USB interface as plain text assuming that Secure Channel is not being used) and never leave the module.

Each operator of the module may own 1 or more RSA User Private Keys and using them requires authenticated access. They are encrypted with the AES User Master Key and stored on the flash memory. When the user is deleted the AES User Master Key is deleted and therefore the RSA User Private Keys cannot be decrypted.

RSA Device Private Keys are owned by the device. Device owned private keys require an authenticated user to be used as with any cryptographic operation. When the device is recycled, the RSA Device Private Key is deleted and a new one is generated.

RSA general purpose encryption/decryption is not a FIPS approved service.

6.1.9 Critical Security Parameters Association

Each user has a separate crypto store that is encrypted with his User Master Key. Therefore a user cannot access another user's crypto store. Crypto store separation and encryption are the two mechanisms that link users and their own critical security parameters.

6.2 Non-critical Security Parameters

6.2.1 RSA Public Keys

Public Keys are the public portion of an RSA key pair. RSA key pairs that are used for X9.31 [P2] operations are generated internally following the ANSI X9.31 specification. RSA key pairs that are used for PKCS#1 operations are generated internally using the RSA key generation mechanism of OpenSSL. There are two types of RSA public keys: Device and User keys. The Device and User keys are to be set exclusively for general purpose encryption/decryption or else sign/verify purpose. Public keys can be 1024, 2048, or 3072 bits in length. They can either be generated on the device or injected (through the USB interface as plain text assuming that Secure Channel is not being used) and never leave the module.

Each operator of the module may own 1 or more RSA User Public Keys and using them requires authenticated access. They are encrypted with the AES User Master Key and stored on the flash memory. When the user is deleted the AES User Master Key is deleted and therefore the RSA User Public Keys cannot be decrypted.

When the device is recycled the RSA Device Public Key is deleted and a new one is generated.

RSA general purpose encryption/decryption is not a FIPS approved service.

RSA public and private keys are internally stored as a single entity. When exporting a public key only the public portion of is extracted and output.

7 Identification and Authentication Policy

7.1 Roles

Outbacker MXP performs identity based authentication. Device operators are identified by their user name and authenticated either by password hash comparison, fingerprint template, or both (two-factor). The role of an operator can be either General User, or Administrator. This is defined when the operator is created and may be changed by Administrators under privileged access. A new or recycled device is referred to be in the 'Open' state.

The Administrator role is the Crypto officer role as defined in the FIPS 140-2 specification [P1]. Administrators have access to management, security policy and configuration functions of the device and are responsible for the overall security of the module.

The General User role is a User with limited privileges and access to limited services of the device.

Outbacker MXP can have up to 5 operators. At least one operator must be an Administrator.

FIPS 140-2 authentication requirements are not met when an operator is authenticated to the module with the scan of a finger only. FIPS 140-2 authentication requirements are met when a password or a password combined with the scan of a finger are used for the operator to authenticate to the Outbacker MXP.

Table 3: Roles and Required Identification and Authentication

Identification	Role	Type of Authentication	Authentication Data
User name	Administrator	Password or Two-Factor	password or fingerprint template and password
User name	General User	Password or Two-Factor	password or fingerprint template and password

7.2 Authentication Data

The operators/users of Outbacker MXP can be authenticated by a fingerprint, password or the combination of them both (also known as two-factor authentication). The associated strength of each mode is shown in Table 4. FIPS 140-2 Security Level 3 authentication requirements are not met when an operator is authenticated to the module by a fingerprint only and not with a password or a password and fingerprint.

Upon a failed password attempt, there is a delay of 500 milliseconds. Note that this delay also applies when a password verification operation is done. This delay allows a maximum of 120 tries per minute. Therefore the probability of a random authentication within a one minute period is 1:650000. The number of failed password attempts allowed before blocking the user is configurable from 1 to 255, or unlimited. When a user becomes blocked, he/she cannot authenticate on the device until an Administrator unblocked him/her. In the case where there is only one user on the device with Administrator privileges and this user becomes blocked, then the device must be recycled.

Table 4: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Fingerprint	Configurable False Match Ratio (FMR): 1 : 2 700 1 : 4 500 1 : 23 000 1 : 55 000 1 : 100 000
Password	Minimum 4 characters of the printable ASCII set ~ 1 : 78 000 000 (94^4) Maximum length is 40 characters (UTF8)
Two-Factor (Fingerprint and Password)	Fingerprint x Password Strength

8 Access Control Policy

8.1 Services

The following table enumerates the services on Outbacker MXP. The roles and critical security parameters (CSP) have been defined in the previous sections. Note that in column "Authenticated Role Required" in the table below, *Admin* refers to the *Administrator* role and that *General* refers to *General User* role as defined in table 4.

Note that the column 'Authenticated Role Required' refers to device states. "Open" and "Locked" are not roles as such but indicate that no authenticated users are needed to carry out the operation. However we need to distinguish between "Open" and "Locked" since the set of operations are different between the two states. The device is "Locked" when there is at least one user with an authentication mechanism. The device is "Open" when there are no users or users without authentication mechanisms.

All operations in the table are given explicit permissions to execute in either "Open", "Locked", "Admin" or "General". For example, when the device is in "Open" state, only operations that indicate "Open" can be executed. All operations are verified against the device state to execute.

The "Open" state specifies that the device has not yet been initialized, which means that no users have yet been created with registered methods of authentication.

Table 5: Services Authorized for Roles and Access Rights within Services

Note: "FIPS Approved" means that the service may be used in a FIPS Approved mode of operation.

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
Bypass Service Mass Storage OP to Plain Text LUN	Execute a bulk read or write to the public or read-only mass storage partition			Yes	Open Locked Admin General
Mass Storage OP to Private LUN	Execute a bulk read or write to the user's secure mass storage partition	AES User Master Key	Read	Yes	Admin General

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
OP_BIOCALIBRATE	Calibrates the biometric sensor.			Yes	Open
OP_RESIZEREADONLY	Changes the size of the read-only partition			Yes	Open
OP_CREATEUSER	Creates a new user			Yes	Open Admin
OP_SETKEYS	Injects an AES encryption key for a user	AES User Master Key	Write	Yes - whenever a plaintext key is entered from the host into the Outbacker MXP, the host must not provide any network access during the operation	Open Admin
OP_SETDEVINFO	Changes information about the device			Yes	Open Admin
OP_SETPARTINFO	Sets partition information			Yes	Open Admin
OP_SETPUBSTOR	Writes information to the public store (store data is public – use of CSP is only internal to device)	AES Device Master Key	Read	Yes	Open Admin
OP_DELETEUSER	Removes a user	User password	Set to FF	Yes	Open Admin
		RSA Private Keys	Set to FF		

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
		User AES Secret Key	Set to FF		
		User finger enrollments	Set to FF		
		PSTS Credential Master Keys	Set to FF		
		User PSTS Private Keys	Set to FF		
OP_WRITEUSERINFO	Updates user state information			Yes	Open Admin
OP_MOVESECTOR	Copy sectors from one location to another			Yes	Open Admin
OP_SWITCH_READONLY	Temporarily allows write access to the read-only partition			Yes	Open Admin
OP_GETPRIVSTOR	Retrieves information from the store of an authenticated user	AES User Master Key	Read	Yes	Admin General
OP_SETPRIVSTOR	Writes information to the store of an authenticated user	AES User Master Key	Read	Yes	Admin General
OP_GETUNLOCKEDINFO	Retrieves an application secret payload			Yes	Admin General
OP_SETPWD	Sets a new user password	User password	Write	Yes	Open Admin General (self)

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
OP_ENROLLBIO	Performs an enrollment of a user's finger	User finger enrollment	Write	Yes	Open Admin General (self)
OP_DELBIO	Removes a user's finger enrollment.	User finger enrollment	Removed	Yes	Open Admin General (self)
OP_CHGPWD	Changes an authenticated user's password – note that the user and current password must be provided in the command so there is an implicit authentication even in open state	User password	Write	Yes	Open Admin General (self)
OP_UPDATEFIRMWARE	Upgrades firmware to a new version			Yes	Open Admin
OP_READUSERINFO	Queries information about a user			Yes	Open Locked Admin General
OP_VERIFYPWD	Verifies a password without affecting device state – no users are logged in after operations	User password	Read	Yes	Open Locked Admin General
OP_AUTHPWD	Verifies a password for authenticated access	User password	Read	Yes	Open Locked Admin General
OP_AUTHPWDOTP	Verifies a password encrypted using HOTP for authenticated access	Encrypted User password	Read	Yes	Open Locked Admin General

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
OP_CHGMINPASSLEN	Sets the required minimum length of a password (minimum of 4 characters)			Yes	Open Admin
OP_LOGOUT	Ends the login session for the current authenticated user			Yes	Admin General
OP_SETPROPERTY	Sets behavior properties of the device (CDROM/disk)			Yes	Open Admin
OP_GETPROPERTY	Retrieves behavior properties of the device (CDROM/disk)			Yes	Open Locked Admin General
OP_GETPUB_RW_STOR	Reads information from the RW public store. (store data is public – use of CSP is only internal to device)	AES Device Master Key	Read	Yes	Open Locked Admin General
OP_SETPUB_RW_STOR	Writes information to the RW public store (store data is public – use of CSP is only internal to device)	AES Device Master Key	Read	Yes	Open Locked Admin General
OP_GETPUBSTOR	Reads information from the public store			Yes	Open Locked Admin General
OP_GETBIOINFO	Retrieves status about the current fingerprint operation			Yes	Open Locked Admin General
OP_CANCELBIO	Aborts a finger enrollment operation			Yes	Open Locked Admin General

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
OP_VERIFYBIO	Verifies a finger without affecting device state - no users are logged in after operations.	User finger enrollments	Read	Yes	Open Locked Admin General
OP_AUTHBIO	Verifies a finger for authenticated access.	User finger enrollments	Read	Yes	Open Locked Admin General
OP_GETVERSIONSINFO	Retrieves version info from firmware and hardware components			Yes	Open Locked Admin General
OP_GETMANUFINFO	Retrieves the USB VID/PID, SCSI strings and serial number			Yes	Open Locked Admin General
OP_GETPARTINFO	Retrieves partition information			Yes	Open Locked Admin General
OP_GETDEVINFO	Retrieves information about the device state and configuration			Yes	Open Locked Admin General
OP_GETDISKSIZE	Retrieves the full capacity of the drive			Yes	Open Locked Admin General
OP_GETLOG	Retrieves the debug log			Yes	Open Locked Admin General

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
OP_SELFTEST	Executes the Cryptographic known answer tests. Note: this does not execute the integrity test, to execute the integrity test, the device must be power cycled.			Yes	Open Locked Admin General
OP_STACKREPORT	Reports the stack utilization			Yes	Open Locked Admin General
OP_REPORTCONFIG	Reports the configuration of the hardware			Yes	Open Locked Admin General
OP_SETRECYCLECODE	Allows the management code to be changed			Yes	Open
OP_RECYCLE	Put the device into a new initialized state	All passwords	Set of FF	Yes	Open Locked Admin General
		All RSA Private Keys	Set of FF		
		All AES Keys	Set of FF		
		All finger enrollments	deleted		
		All credential master keys	Set of FF		
OP_CONTINUE	Test completed status of a request			Yes	Open Locked Admin General
OP_GENRANDOM	Generate Random Number	Random Seed	Read Write	Yes	Admin General

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
OP_SEEDRANDOM	Set the seed for the external random number service	Random Seed	Write	Yes	Admin General
OP_GENKEY	Generates an X9.31 key	AES User Secret Key	Write	Yes	Admin General
		Random seed	Read Write		
OP_GENKEYPAIR	Generates an RSA key pair	RSA Private Keys	Write	Yes	Admin General
		Random seed	Read Write		
OP_HASH	Hash data using SHA-1 or SHA-256			Yes	Admin General
OP_HASHINIT	Start a SHA-1 or SHA-256 operation			Yes	Admin General
OP_HASHUPDATE	Continue a SHA-1 or SHA-256 operation			Yes	Admin General
OP_HASHUPDATEKEY	Change key for a SHA-1 or SHA-256 operation			Yes	Admin General
OP_HASHFINAL	Complete a SHA-1 or SHA-256 operation			Yes	Admin General
OP_HASHKEY	Returns the hash of a stored key using SHA-1 or SHA-256	AES User Master Key AES User Secret Key	Read	Yes	Admin General

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
OP_SIGN	Signs data using the user's RSA key	RSA Private Keys	Read	Yes	Admin General
OP_SIGNINIT	Start Sign data using the user's RSA key	RSA Private Keys	Read	Yes	Admin General
OP_SIGNUPDATE	Continue Sign data using the user's RSA key	RSA Private Keys	Read	Yes	Admin General
OP_SIGNFINAL	Complete Sign data using the user's RSA key	RSA Private Keys	Read	Yes	Admin General
OP_VERIFY	Verify data using the user's RSA key		Read	Yes	Admin General
OP_VERIFYINIT	Start Verify data using the user's RSA key		Read	Yes	Admin General
OP_VERIFYUPDATE	Continue Verify data using the user's RSA key		Read	Yes	Admin General
OP_VERIFYFINAL	Complete Verify data using the user's RSA key		Read	Yes	Admin General
OP_ENCRYPT	Encrypts data with a user's AES key	AES User Secret Key	Read	Yes	Admin General

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
OP_DECRYPT	Decrypts data with a user's AES key	AES User Secret Key	Read	Yes	Admin General
OP_INJECTKEY	Injects an AES encryption key for a user	AES User Secret Key	Write	Yes - whenever a plaintext key is entered from the host into the Outbacker MXP, the host must not provide any network access during the operation	Admin General
OP_INJECTKEYPAIR	Injects a RSA encryption key pair for a user	RSA Private Keys	Write	Yes - whenever a plaintext key is entered from the host into the Outbacker MXP, the host must not provide any network access during the operation No if injecting key for RSA encryption/decryption	Admin General
OP_DELETEKEY	Deletes an AES encryption key for a user	AES User Secret Key	Zeroed	Yes	Admin General
OP_GETOTP	Returns Hash based One Time Password (HOTP) according to IETF specifications			Yes	Admin General

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
OP_GETKEYPROP	Retrieve attributes of a specific key			Yes	Admin General
OP _RSAENCRYPT	Encrypt data with User's RSA private key		Read	No	Admin General
OP_RSADECRYPT	Decrypt data with User's RSA private key	RSA Private Keys	Read	No	Admin General
OP_ENUMKEYS	Retrieve listing of available key types			Yes	Open Locked Admin General
OP_READPUBLICKEY	Retrieves a device RSA public key			Yes	Open Locked Admin General
OP_RESETDEVICE	A soft reset is applied to the device. Device's firmware executes from the start. This also causes all the device power-up self tests to be run after the reset.			Yes	Open Locked Admin General
OP_SC_CONNECT	Establish a secure channel connection			Yes	Open Locked Admin General
OP_SC_DISCONNECT	Closes a secure channel connection			Yes	Open Locked Admin General

Service	Description	CSP	Access to CSP	FIPS Approved	Authorized Role/State
OP_SC_WRAPPED	When using secure channel, all commands are 'wrapped' (sent encrypted) via this command.			Yes	Open Locked Admin General
PSTS_VALIDATE	Determines if the device supports PSTS			No	Open Locked Admin General
PSTS_GET_CAPABILITY	Retrieves PSTS properties and policies specific to the device			No	Open Locked Admin General
PSTS_INJECT	Injects an InfoCard credential	PSTS Credential Master Key	Write	No	Admin General
PSTS_REMOVE	Removes an InfoCard credential	PSTS Credential Master Key	Zeroed	No	Admin General
		PSTS Private Keys	Zeroed		
PSTS_RST	Retrieves a SAML token asserting the requested claims	PSTS Credential Master Key	Read	No	Admin General
		PSTS Private Key	Read/Write	No	
PSTS_ENUM_CREDENTIAL	Retrieves a list of credential meta-data (any data specified by application and not requiring protection)			No	Open Locked Admin General
PSTS_UPDATE_CREDENTIAL	Updates information to an InfoCard credential			No	Admin General
PSTS_LOGIN	Verifies a user for authenticated access	User password	Read	No	Open Locked Admin General
		User finger enrollments	Read	No	
PSTS_CANCEL	Cancel any PSTS operations in progress			No	Open Locked Admin General
PSTS_LOGOUT	Ends the login session for the current authenticated user			No	Admin General

8.2 Supported Cryptographic Services

Cryptographic services in Outbacker MXP as detailed in table 5 support both FIPS approved and non-FIPS approved algorithms. The following provides details on both types.

FIPS approved cryptographic algorithms

- AES
  - Encrypt/Decrypt [128, 192, 256 bit keys]
  - Key Generation using X9.31 PRNG
- PRNG
  - X9.31 A.2.4 PRNG using AES
- HASH
  - SHA1
  - SHA256
- X9.31
  - RSA Key Generation [1024,2048,3072 bit keys]
  - RSA Sign/Verify [1024,2048,3072 bit keys] with SHA1 or SHA256
- PKCS #1
  - RSA Key Generation [1024,2048,3072 bit keys]
  - RSA Sign/Verify [1024,2048,3072 bit keys] with SHA1

Non-FIPS approved cryptographic algorithms

- RSA encrypt/decrypt [1024,2048,3072 bit keys]

8.3 Modes of operation

If a command is not FIPS approved, the Outbacker MXP will be in a non-FIPS approved mode of operation for the duration of the service.

8.4 Bypass Services

Outbacker MXP provides bypass services. FIPS 140-2 rules governing bypass services on Outbacker MXP are observed for service usage and service modifications. The following is a list of bypass services supported on Outbacker MXP.

1. **Mass Storage Operation (OP) to Plain Text Logical Unit (LUN)**
    a. Service activation verification: 2 independent actions are required to activate this service
        i. Configuring the public partition
        ii. Check sector offset and boundaries to ensure read and write fall within proper range
    b. Service modification verification: When service parameters are modified, a CRC is first performed on the master table that holds the service parameters to insure its integrity. Modifications can only occur if integrity of the table is correct.

9 Finite State Model

The finite state model of Outbacker MXP is proprietary and can be received upon request with a non-disclosure agreement. Refer to document DD-MSW1023-01.doc in correspondence.

10 Physical Security Policy

This section details the physical security mechanisms that protect the cryptographic module, and the actions operators must take to ensure that physical security is maintained.

10.1 Physical Security Mechanisms

10.1.1 Tamper-Evident Enclosure

Outbacker MXP is secured physically by an opaque tamper-evident metal case. The openings for the USB plug, finger swipe, LEDs, and external power supply are tightly fitted around the connectors. The enclosure does not have any removable covers or ventilation slits. The photo in section 3 shows these details of the Outbacker MXP. The USB mini-B plug is on the end of the device while the finger swipe and the LEDS are located in the middle recessed area. The device receives power and communicates through the USB connection to a USB host. Evidence of tampering is determined by visually inspecting the device. If the device is opened, the bumper pads and at least one of the end caps must be removed. Signs of tamper evidence will include a bent end cap and scratches on the metal case.

10.2 Inspection by Operators

Table 6: Inspection of Physical Security

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-Evident Enclosure	Each insertion	• Visually and tactilely examine enclosure for damage to the metal surface due to prying, cutting, grinding or welding of the material • Visually examine enclosure for bent end caps

11 EMI/EMC

The Outbacker MXP has been tested for and passes the following:

- Certification FCC Part 15 Class B
- CE EN55022 Class B (1998) for conducted and emissions

12 Self-Tests

The Outbacker MXP performs a variety of self tests during startup and on demand while conditional tests are executed on the occurrence of certain events.

12.1 Booting Self-Tests

Initially the bootloader performs a sanity check on both internal and external RAM. This test writes an alternating pattern in memory and then verifies that the pattern has been written properly. In case of any memory errors the Outbacker MXP will enter the Self Test Error State.

Once the RAM test has passed, the bootloader checks if an upgrade is required, and if not it calculates a 16 bit CRC on the firmware image and compares it to the stored value. Upon verification the firmware image starts execution and upon failure enters the Error State described below. Booting self tests are always executed when the device starts up. Performing these tests on-demand requires a complete power cycle.

12.2 Error States

In the case of a fatal error, the Outbacker MXP will start blinking the red and blue light continuously.

12.3 Known Answer Tests

The known answer tests are performed at power-on and on demand. The known answer tests are executed on all approved algorithms:

AES CBC Mode (Key size: 256 bit) Encrypt and Decrypt

HMAC Using SHA-1 (Key size: 256 bit)

HMAC Using SHA-256 (Key size: 512 bit)

RSA ANSI X9.31 Signature Generation (modulus 1024; SHA-1)

RSA ANSI X9.31 Signature Verification (modulus 1024; SHA-1)

RSA PKCS#1 Signature Generation (modulus 1024; SHA-1)

RSA PKCS#1 Signature Verification (modulus 1024; SHA-1)

RNG for ANSI X9.31 (256 bit AES)

If the Known Answer Tests do not pass, the Firmware will enter the Error State described above.

12.4 Conditional Tests

12.4.1 Software/Firmware Load Test

The firmware on the module can be upgraded using an external application, most likely a PC application. The upload process performs RSA digital signature check on the new firmware image before the upgrade is allowed. If the signature is not verified, the upgrade process is aborted and an error is returned to the application.

The public key used to verify a new firmware load is embedded in the currently loaded device firmware.

12.4.2 Pair-wise Consistency Test

The module can generate private and public key pairs as well as perform the verification of digital signatures. The consistency of each new key pair is tested upon generation by signing static data and verifying the signature. If the verify does not pass, the device enters in error state. Pair-wise consistency test are done for the following:

- RSA ANSI X9.31 Key Generation (modulus 1024, 2048, 3072; public key values 3, 17, 65536)
- RSA PKCS #1 Key Generation (modulus 1024, 2048, 3072; public key values 3, 17, 65536).

12.4.3 Continuous Random Number Generator Test

The module can generate random data from a hardware based entropy system. The data generated is stored for comparison to ensure that the next generated number is not the same as the previous. This test is also performed on the ANSI X9.31 pseudo-random number generator. The test consists in comparing each consecutive block of random data against the previous one. If the data is the same, the device enters in error state.

12.4.4 Bypass Test

When the bypass service parameters are modified, a CRC is first performed on its master table that holds service parameters to insure its integrity. Modifications can only occur if integrity of the table is correct. In case of an error, an error code is returned to the user and the operation is aborted.

13 Design Assurance

The design of Outbacker MXP was initiated by a functional specification. A high level language was used (C for the firmware and VHDL for the ASIC) in the creation of the module code to meet the functional specification. Use of low-level language (assembly) was only used in very isolated part of the firmware for performance reasons. The user and administration documents were created from the functional specification to give guidance about the specific tasks and functions of Outbacker MXP.

13.1 Design and Development

Each component of the Outbacker MXP hardware and firmware design is under strict version control. The firmware is maintained with a CVS [Concurrent Version System] server and SmartCVS clients. Every release of firmware and hardware is specifically tagged with a build version number. The hardware version is labeled with the product number on the boards. The firmware version is available through a command in the user interface. During design, the product goes through quality control to confirm that it meets all aspects of the functional specification. Production utilities fully test each device through an automated test suite.

13.2 Delivery and Distribution

There are no security risks during delivery to authorized operators. Devices are shipped from the factory in an open state with no users. The first user that is created is an Administrator and becomes the Crypto Officer. That officer can then perform all services as specified in the Access Control Policy section.

The devices are shipped from the factory using a bonded courier directly to the purchaser.

13.3 Initialization

When a new device is received by an organization or individual, the procedures outlined in the Quick Start Guide and the Administration manual should be followed. It is recommended to change the device management code from the default setting. The device is shipped in the 'open' state with no users enrolled. The first user created becomes an Administrator.

14 Mitigation of Other Attacks Policy

The Outbacker MXP provides additional mechanisms for mitigating attacks not specifically addressed by FIPS 140-2. The following table describes the mechanisms used.

Table 7 : Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
Power Analysis (Simple)	The combination of hardware and software mechanisms makes it very difficult to derive key information. **Hardware mechanism** • Power supply filtering to limit the amount of noise due to calculations of the processor. **Software mechanism** • The device is multithreaded and tasks scheduling is in practice very difficult to guess • User key is only used when the device is unlocked.	If the user participates in the power analysis by unlocking the device for the attacker and the attacker has a significant amount of time to send and receive known data from the encrypted partition, that user's key may be made vulnerable to power analysis.