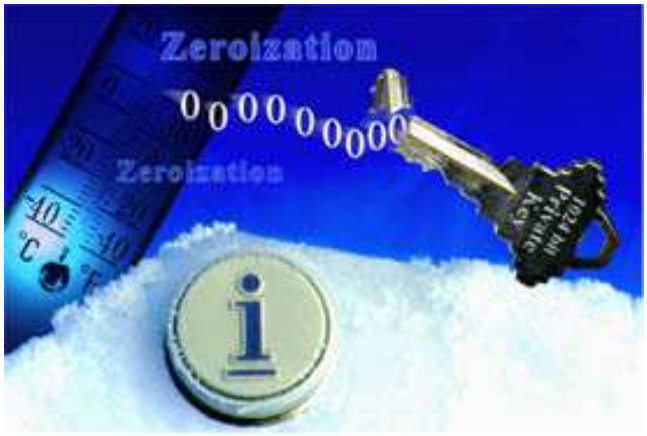
Pitney Bowes iButton Postal Security Device (PSD)

Hardware Version: DS1955B PB4 – 4.00



FIPS 140-2 Non-Proprietary Security Policy

Level 3 Validation
Version 4.00

November 17, 2005

Table of Contents

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Pitney Bowes iButton Postal Security Device (PSD) hardware version DS1955B PB4 – 4.00. This security policy describes how the DS1955B PB4 PSD iButton meets the security requirements of FIPS 140-2 as a multiple-chip standalone module. This policy was prepared as part of the Level 3 (with Environmental Failure Testing) FIPS 140-2 validation of the module.

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

The DS1955B PB4 PSD Postal Security Device is referred to throughout this document as the PSD, PSD iButton, and the module.

References

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

- The Pitney Bowes website http://www.pb.com/cgi-bin/pb.dll/jsp/Home.do contains information on the full line of products from Pitney Bowes.

- The NIST Validated Modules website (http://csrc.ncsl.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

DS1955B PB4 PSD POSTAL SECURITY DEVICE IBUTTON

Overview

An iButton® is a small hand held device that can be used to carry information. It is durable enough to be able to withstand everyday wear and tear much like the keys on a key chain. They can be dropped, stepped on, and even sent through the washer and dryer without compromising the information inside of the module.

A Postal Security Device (PSD) is an iButton that provides the same physical security of the standard iButton, and can also perform cryptographic functions. It also contains a tamper response system that will respond if the PSD is intentionally tampered with and zeroize all of the critical information contained on the module.

The DS1955B PB4 PSD is designed to work within the Pitney Bowes Postage Meter System, where it can create and print indicia while keeping track of how much postage the iButton has used and how much it has remaining. The DS1955B PB4 has been hardened to contain only the functionality necessary to perform the postal services, with only one PSD applet locked on to the module.

The DS1955B#PB4 PSD is manufactured for compliance to the Restriction of Hazardous Substances (ROHS) Act. A # sign is laser branded within the part number to indicate ROHS Compliance.

Module Interfaces

The cryptographic boundary of the DS1955B PB4 PSD iButton is defined by the stainless steel metal MicroCAN®. There is one physical interface on the PSD iButton that is accessed through the steel lid contact. There are five different logical interfaces on the PSD iButton. The logical interfaces are: Data Input, Data Output, Control Input, Status Output, and Power.

The logical interfaces are kept logically separate by the 1-Wire® protocol which controls the physical and logical interfaces. The 1-Wire interface is implemented to control how information enters and exits the module. This interface only allows one communication (input/output) at any one given time, which separates the logically interfaces very efficiently.

The physical interface is separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Module Physical Interface	FIPS 140-2 Logical Interface
Steel Lid Contact	Data Input Interface
Steel Lid Contact	Data Output Interface
Steel Lid Contact	Control Input Interface
Steel Lid Contact	Status Output Interface
Steel Lid Contact	Power Interface

Table 1 – FIPS 140-2 Logical Interfaces

Input and Output

All of the input and output to and from the module is done through the use of Application Protocol Data Units (APDU). The APDU is broken down into these sections:

- Class (CLA)
- Instruction (INS)
- Parameter 1 (P1)
- Parameter 2 (P2)
- Length of Data Command (Lc)
- Command Data (Data [Lc])

The first five define what type of command is being issued. The command data portion holds information that is needed to execute the command. Each service that is provided by the module requires a different APDU to execute the service.

Roles and Services

The module supports identity-based authentication. There are three roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer Role, a Provider Role and a User Role.

Crypto Officer Role

The Crypto Officer role has the ability initialize the module at the factory before having it shipped to the consumer (end-user). Initialization at the factory consists of installing the PSD applet into the ROM of the PSD, running the Power On Self Tests and loading the keys into their specific location in memory in order to prepare the iButton for use by the user. In addition, the Crypto-Officer has access to status functions that return the current status of several of the components of the module. These status functions do not require authentication and are also included in the User Role Services. Descriptions of the services available to the Crypto Officer role are provided in the table below.

The Crypto-Officer functionality includes:

- Initialization of the module (which includes Running Self Tests on the module.) Initialization for the PSD occurs for the actual country(s) of usage: Initialize – USA, FR, or IT; or German Initialize – Deutsche Post (DP) and CA specific (non-FIPS mode). This affects German specific services for the Provider and User roles. These services are; ProcessGermanPVDMessage, ProcessGermanPVRMessage, PrecreateGermanIndicium, CreateGermanIndicium, GetGermanPSDParameters, GetGermanParamData, and CreateGermanFinalizingFrank

- Loading keys onto the module

- Generating internal keys (part of the Manufacture Service in the table below)

- Distributing the module

- Master Erase - Key Zeroization

A complete description of the functions available to the Crypto-Officer role (except module distribution service) can be found in the following table (table 2). The distribution of the module is performed by the crypto-officer by shipping the part to the provider or user role. In table 2, the input and output only depict the data part of the APDU. The first five sections defining which command is being issued is implied. In addition to the APDU, every operation also returns a status output indicating the status of the operation. If the operation completed successfully, the status output

reflects this. If the operation is not completed successfully, the output reflects this as well.

Role	Service	Description	Input	Output
Crypto-Officer	Get Speed	Returns the approximate speed of the processor and co-processor in 1000's of Hz.	None	Approximate speeds of the co-processor and the CPU
Crypto-Officer	Load Provide Key	Loads the Provider Public Key onto the module	Provider Public Key	None
Crypto-Officer	Initialize	Writes the Module's serial number to memory, resets the ascending and descending registers to 0	Initialize Input Data	None
Crypto-Officer	German Initialize(while operating in non-FIPS mode)	Writes the Module's serial number to memory, resets the ascending and descending registers to 0	German Initialize Input Data	None
Crypto-Officer	Manufacture	Loads the secret key that is shared between Pitney Bowes and Maxim/Dallas onto the module	Encrypted Secret Key	None
Crypto-Officer	Run Algorithm	Gives access to the Cryptographic Algorithms for FIPS Validation	Dependant upon the algorithm being executed	Dependant upon the algorithm being executed
Crypto-Officer	Transport Unlock	Executes the Self Tests and authenticates the Crypto-Officer to the Module	Encrypted Random Variable	None
Crypto-Officer	Master Erase	Erases all information from the module, and transitions to the Transport PSD State.	Master Erase Data	None

Table 2 – Crypto-Officer Services, Descriptions, Inputs, and Outputs

Provider Role

The Provider role can perform status checks, load postal configuration data, and generate key pairs. Service descriptions and inputs/outputs are listed in the table below.

The Provider functionality includes:

- Loading Postal Configuration Data
- Authorizing the module to the host
- Generating Keys

- Master Erase – Key Zeroization

A complete description of the Provider role services can be found in the following table. In this table, the input and output only depict the data part of the APDU. The first five sections defining which command is being issued is implied. In addition to the APDU, every operation also returns a status output indicating the status of the operation. If the operation completed successfully, the status output reflects this. If the operation is not completed successfully, the status output reflects this as well.

Role	Service	Description	Input	Output
Provider	Load Secret Key	Replace the current secret exchange key, provide a Keypad Refill Key, or keys specific to the French or German market (non-FIPS mode)	Secret Key Data Structure	None
Provider	Generate Keys	Generates a DSA Key pair	Generate PSD Key Data	PSD Public Key Data Structure
Provider	Load Postal Configuration	Loads important module specific postal information to the module	Postal Configuration Data	None
Provider	Authorize	Authorizes the module to the host	PSD Certificate Data	None
Provider	Process PVD Message	Accepts a Postage Value Download Message from the host and increments the Descending register accordingly	Response Message	PB Data Center Status
Provider	Process PVR Message	Accepts the Postage Value Refund message from the host and adjusts the registers accordingly	Response Message	PB Data Center Status
Provider	Process Audit Response	Resets the Watchdog Timer by giving the PSD a valid response from the Provider	Audit Response Message	None
Provider	Verify Hash Signature	Verifies a hash signature	Verify Hash Signature Structure	None
Provider	Master Erase	Erases all information from the module, and transitions to the Transport PSD State.	Master Erase Data	None
Provider	Disable PSD	Places the PSD in a mode in which it cannot perform any Postal functions.	None	None
Provider	Enable PSD	Reverts the PSD to a mode in which it can carry out its Postal functions.	None	None

Table 3 - Provider Services, Descriptions, Inputs, and Outputs

User Role

The User role can perform status checks, basic postal functions, and self tests. Service descriptions and inputs/outputs are listed in the table below.

The User functionality includes:

- Logging into/out of the module
- Creating Indicium
- Printing Indicium
- Adding/Removing Postage

A complete description of the User role services can be found in the following table. In this table, the input and output only depict the data part of the APDU. The first five sections defining which command is being issued is implied. In addition to the APDU, every operation also returns a status output indicating the status of the operation. If the operation completed successfully, the status output reflects this. If the operation is not completed successfully, the status output reflects this as well.

Role	Service	Description	Input	Output
User	Commit Transaction	Updates the Ascending and Descending registers and outputs the signed indicium	None	Signed Indicium Data
User	Create Indicium	Creates an Indicium using the input date	Postage Value, Date of Mailing, and Rate Category	Signed Indicium Data
User	Pre Compute R	Pre computes the R portion of the DSA signature so that the create indicium function can be executed faster	None	A signed device audit message
User	Pre Create Indicium	Pre-creates the indicium based on the input values, and adjusts the precreated register values	Postage Value, Date of Mailing, and Rate Category	None
User	Generate PVD Request	Makes a request to the host to download a Postage Value	Value of Postage Requested	Postage Value Download Request Message
User	Generate PVR Request	Generates a Postage Value Refund Request Message to send to the host	None	Postage Value Refund Request Message

Role	Service	Description	Input	Output
User	Keypad Refill	Adds postage to the Descending register	Refill amount, and ASCII Combination Data	None
User	Keypad Withdrawal	Removes Postage from the Descending register	ASCII Combination Data	None
User	User Login	Authenticates the User to the module	Hash of Login Challenge and User Password	None
User	User Logout	Logs the user out, and returns the module to the Full Postal State	None	None

Table 4 – User Services, Descriptions, Inputs, and Outputs

Un-Authenticated Services

The PSD iButton provides several un-authenticated services. These services consist of basic status inquiries that do not require authentication and are available from any state of operation. The Run Self Tests service is also available from any state in the module, and does not require authentication. These services are detailed in the following table.

Role	Service	Description	Input	Output
All Roles	Get State	Returns the state that the Module is currently in.	None	The current state
All Roles	Create Device Audit Msg	Sends the value of the Ascending and Descending registers to the provider	None	Device Audit Message
All Roles	Run Self Tests	Runs the Self Tests	None	None
All Roles	Get Module Status	Returns the values of the Ascending and Descending registers	None	The values of the Ascending and Descending registers
All Roles	Get Challenge	Returns the most recent Login Challenge	None	The Value in the Login Challenge Variable
All Roles	Get PSD Parameters	Returns the most recent Login Challenge	None	The Value in the Login Challenge Variable
All Roles	Set GMT Offset	Sets the Local time offset from the GMT Time.	GMT offset in seconds	None
All Roles	Get Firmware Version	Returns the Firmware Version String	None	Firmware Version String
All Roles	Get Free RAM	Returns the number of free bytes of RAM	None	Number of bytes of free ram
All Roles	Get RTC	Returns the value of the Real Time Clock	None	The number of seconds since the battery was attached

Role	Service	Description	Input	Output
All Roles	Get POR Count	Returns the number of Power On Resets since the battery was attached	None	Number of Power On Resets since the battery was attached
All Roles	Get Random	Returns the number of random bytes requested	A request for N bytes of random data	N bytes of random data
All Roles	Get Log Data	Returns the contents of a specified log	Parameter to indicate which log to return	Contents of the appropriate log
All Roles	Get PSD Key Data	Returns the PSD Public Key if the PSD has been authorized	None	The PSD Public Key

Table 5 – Un-authenticated Services, Descriptions, Inputs, and Outputs

Authentication Mechanisms

Authenticating to the module is done through either challenge response or by asymmetric signature. The Crypto-Officer, User, and Provider authenticate through identity-based authentication, by demonstrating knowledge of their key or PIN (a 128-bit TDES key, 64-bit password/PIN, and DSA key set for the CO, User, and Provider respectively). The types of authentication are listed in the table below.

Authentication Type	Strength	Roles
Transport Key Authentication	The most recent random login challenge is encrypted using the Transport Key, which is a 2-key 3DES Key. The PSD Transport Key is 128 bits. There are 2^128 possible combinations for the transport key, which makes the strength of the key 1/(2^128).	Crypto-Officer Role
User Password Authentication	The User Password is 20 bytes long, and it is hashed with a random challenge that is 8 bytes long. These are both hashed with SHA-1 to create a 20-byte login command used to authenticate the user. Because the password is 64 bits, the strength of this authentication is a 1/(2^64).	User Role
PSD Certificate Data Authentication	The PSD Certificate Data is digitally signed with the provider key. The module verifies the signature with the provider key that was loaded into memory during Initialization and either authorizes the module or does not authorize the module. The strength of this key is based on a 1024 bit DSA key set. DSA is an asymmetric key that is based on the discreet logarithm problem, which is a difficult mathematical function.	Provider Role

Table 6 – Estimated Strength of Authentication Mechanisms

Physical Security

The DS1955B PB4 PSD iButton is a multi-chip standalone cryptographic module. The cryptographic boundary for the module is the steel enclosure that makes up the iButton. The PSD iButton is contained inside a steel case that is strong, without any doors or hinges to open to access the

module. It does not have any ventilation holes that allow an unauthorized user to gain access to the module. The iButton has a tamper evident mechanism that zeroizes all information if an attempt to tamper the module has occurred.

The United States Postal Service requires that devices involved with the Information Based Indicia Program (IBIP) must meet the physical requirements for FIPS 140-2 Level 3. In addition to the level 3 requirements, all modules must be tested for EFP/EFT, which is a level 4 requirement for FIPS.

The DS1955B PB4 conforms to the USPS standard by undergoing EFT Tests in addition to meeting the requirements for a FIPS 140-2 Level 3 Validation. The module has been tested in the temperature range between -100C and 200C and in the voltage range of -14 Volts to +14 Volts. These tests have been conducted by the testing laboratory.

The Module has been tested and meets Federal Communications Commission (FCC) requirements for home use with regards to Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) for home use as defined in subpart A of FCC part 15.

The PSD iButton also meets European Community (EC) Directives Conformity. The CE Mark EMC/EMI/ESD testing requirements are specified by Application of Council Directive 89/336/EEC Standard to which Conformity is Declared:

- EN 55022
- EN 55024
- EN 61000

Cryptographic Key Management

The implementations of the FIPS-approved algorithms have the following FIPS algorithm certifications:

- SHA-1 (certificate #167)
- PRNG (Certificate #86)
- 3DES in CBC Mode (certificate #185)
- 3DES MAC (certificate #185 vendor affirmed)

- DSA (certificate #90)

In non-FIPS mode (i.e. for German Indicia Type) the module uses RSA encryption/decryption to transport the mSecret value as part of the Deutsche Post Specification.

In non-FIPS mode (i.e. for Canada Indicia Type) the module uses HMAC-SHA-1 to construct a security code as part of the Canada Post Specification.

The module supports the following critical security parameters:

Key	Key Type	Generation	Storage	Use
K_{pb}	2 key Triple-DES (128-bit)	External by manufacturing	External – by Pitney Bowes and Dallas Semiconductor	Derive Transport Key
PSD Transport Key	2 key Triple-DES (128-bit)	Internal – set at Dallas prior to shipment using the Transport Key Derivation Algorithm in the Manufacture function at state 0	Plaintext in non-volatile memory	Decrypt input data in Transport Unlock function at state 1, and encrypt PSD Secret Exchange Key in Load Secret Key function
PSD Secret Exchange Key	2 key Triple-DES (128-bit)	External by User or Crypto-Officer	Plaintext in non-volatile memory	Encrypt/decrypt data between the PSD and the infrastructure
Keypad Refill Key	2 key Triple-DES (128- bit)	External by User or Crypto-Officer	Plaintext in non-volatile memory	Compute CBC-MAC for keypad type refill
PSD Private Key	DSA key set (160-bit)	Internal – uses the RNG as specified in FIPS 186-2 Appendix 3, and uses DES as the mixing function G	Plaintext in non-volatile memory	Digital Signature
PSD Public Key	DSA key set (1024-bit)	Internal – computed from PSD Private Key	Plaintext in non-volatile memory	Compare public key in Certificate signed by Provider, for operators to verify PSD's signature
Provider Public Key	DSA key set (1024-bit)	External by Provider	Plaintext in non-volatile memory	Verify signed messages by Provider
French K-Fab-MA Key	2 key Triple-DES (128-bit)	External – computed from a shared secret key and the PSD serial number	Plaintext in non-volatile memory	Only for PSDs configured for the French market – used to encrypt French K-MA Key
French K-MA Key	2 key Triple-DES (128-bit)	External – loaded upon installation at the customer site	Plaintext in non-volatile memory	Only for PSDs configured for the French market – used to compute a CBC-MAC
User Password	Password (64-bit)	External – Created by User	Plaintext in non-volatile memory	Use by the User login process

Table 7 – Critical Security Parameters

Key Entry and Output

Keys that are created externally from the module are never transmitted to the module in plaintext. Keys are encrypted with the (2 key [128-bit] TDES) PSD Secret Exchange Key and sent through the physical interface and are then decrypted and stored in plaintext in Non-volatile RAM. After a key has been stored on the module, it is never output for any reason.

Key Generation

There are two types of keys that are generated within the module. These keys are the PSD Transport Key, and the PSD DSA key set. The PSD Transport Key is derived using the shared secret key K_{pb} which is shared between Pitney Bowes and Maxim/Dallas Semiconductor. This key is generated before the PSD has been shipped to the user, and only the Crypto-Officer has access to the PSD Transport key.

The PSD DSA key set is generated during the Generate Keys function, which can be executed in both the Crypto-Officer Role and the User Role. To ensure that the key pair functions properly, a pairwise consistency check is performed on any DSA key set that the module creates before the pair is used.

Key Access

This is a chart that shows which CSP's are available to the different roles and what services they are associated with.

Role	**Key**	**Services Associated**	**Type of Access**
Crypto-Officer	K_{pb}	Manufacture	Read Only
Crypto-Officer	PSD Transport Key	Transport Unlock Load Secret Key	Read Only
Crypto-Officer	PSD Secret Exchange Key	Transport Unlock Load Secret Key Master Erase	Read/Write
Provider	PSD Secret Exchange Key	Master Erase	Write Only
Crypto-Officer	Keypad Refill Key	Load Secret Key	Write Only
User	Keypad Refill Key	Key Pad Refill	Read Only
Crypto-Officer	PSD Private Key	Load Secret Key Generate Keys	Read/Write
Provider	PSD Private Key	Generate Keys	Read/Write
Crypto-Officer	PSD Public Key	Generate Keys	Read/Write
Provider	PSD Public Key	Generate Keys Authorize Verify Hash Signature	Read/Write
Crypto-Officer	Provider Public Key	Initialize Load Secret Key	Write Only
Provider	Provider Public Key	Verify Hash Signature Master Erase	Read Only
Crypto-Officer	French K-Fab-MA Key	Load Secret Key	Read Only
Crypto-Officer	French K-MA Key	Load Secret Key	Read Only
User	User Password	Initialize User Login	Read Only
Crypto-Officer	German mSecret (while operating in non-FIPS mode)	Load Secret Key	Read/Write

Crypto-Officer	Deutsche Post RSA Private Key (while operating in non-FIPS mode)	Load Secret Key	Read/Write
Crypto-Officer	Deutsche Post RSA Public Key (while operating in non-FIPS mode)	Load Secret Key	Read/Write

Table 8 – Critical Security Parameter Access Table

Key Zeroization

Key zeroization can occur in two different ways. The first is through a master erase function call that can be called from any state after the module has been initialized. The master erase function removes all of the keys and critical security parameters from the module, and all of them must be entered again for the module to return to normal operation. The module must be returned to the Crypto-Officer to be reinitialized.

The second method of zeroization is from a tamper event. If the module is tampered with, the tamper response system engages and zeroizes all of the information on the module. Once the module has been tampered, it cannot return to normal operation.

Self-Tests

The module performs the following Power On Self Tests:

- CRC32 Firmware Image Tests – This test performs a cyclic redundancy check on the firmware image, and if it does not pass, the test fails.
- SHA-1 Known Answer Tests – This test performs a known answer test on the SHA-1 algorithm implemented by the module.
- DES/3DES Known Answer Tests – This test performs a known answer test on the DES and 3DES algorithms implemented by the module.
- PRNG Known Answer Tests – This test performs a known answer test on the PRNG algorithm that is implemented by the module.
- DSA Pairwise Consistency Tests – This test creates a DSA key pair, and tests the signing and verification processes with a known message.

If one of the Power On Self Tests fail, then the module transitions to the Error state. Once in the error state, successfully passing the self-tests is

the only way the module can transition back to the normal mode of operation.

The module performs the following Conditional Tests:

- RNG Tests – When a new set of random bytes is created, it is compared to the previous set created. If the two sets match, then the test fails.

- DSA Pairwise Consistency Tests

If the conditional tests fail, an error is sent to the status output, and the tests are run again until they are completed successfully.

Design Assurance

Dallas Semiconductor implements ISO-9000 for design insurance.

Mitigation of Other Attacks

The DS1955B PB4 PSD iButton is designed to mitigate against side channel attacks.

The 1-Wire® interface transmits power and I/O, this complicates both monitor triggering and collection of data. Signal to noise on the single point of entry through the cryptographic boundary, obscures listening, and making reception of critical data signals more difficult. The main processor is running while the coprocessor operates to introduce additional noise during strong source powered operation. This increased operating current may also improve the Signal/Noise ratio. The ROM based PSD application precludes unauthorized operation or plain text attacks.

The following patents can provide additional information for mitigating side channel attacks. The patents are available from the United States Patent Office.

Patent Number	Name	Patent Date
4,890,263	Ram with Capability for Rapid Clearing of Data From Memory by Simultaneously Selecting All Row Lines	12/26/89
5,327,564	Timed Access System for Protecting Data in a Central Processing Unit	07/05/94
5,812,004	Current Compensated Clock for a Microcircuit	09/22/98
6,064,740	Method and Apparatus for Masking Modulo Exponentiation Calculations in an Integrated Circuit	05/16/00
6,219,789	Microprocessor with Co-processing Capabilities for Secure Transactions and Quick Clearing Capabilities	04/17/01
6,330,668	Integrated Circuit Having Hardware Circuitry to Prevent Electrical or Thermal Stressing of the Silicon Circuitry	12/11/01

Table 9 – Module Mitigation of Other Attacks Patents

FIPS 140-2 OPERATION OF THE PSD IBUTTON

The DS1955B PB4 PSD Postal Security Device has three roles, the Crypto-Officer Role, Provider Role and the User Role. The PSD is powered on only once when the battery is attached during the manufacturing process. The PSD iButton is a FIPS compliant device and is always in a FIPS approved mode of operation.

Crypto-Officer Guidance

The Crypto-Officer is responsible for the Initialization of the module at the beginning of its life, as well as any re-initializations that may be needed during the life of the module. The Crypto-Officer is also responsible for distributing the module in a secure manner to prevent compromise before the Provider/User obtains the module. The end of the modules life occurs when the lithium battery dies.

Initialization

The module is manufactured and initialized at the same facility, so the process of the Crypto-Officer obtaining the module from the manufacturing facility is insignificant.

When the Crypto-Officer first receives the module, it is powered on and the Power On Self Tests are executed. After the tests have been successfully completed, then the Crypto-Officer authenticates to the module using information that is encrypted with the PSD Transport Key. After the Crypto-Officer has been authenticated, then the module is ready to be initialized.

The Crypto-Officer Initializes the PSD by loading keys onto the module to prepare it to be used by users. The Ascending and Descending registers are initialized and the module is prepared to be distributed to the provider/user.

Distribution

After the PSD has been initialized and is ready to be distributed to providers/users, it is packaged in a secure package. The package shall contain tamper evident labels that indicate if the module has been tampered with before the provider/user receives it.

Provider/User Guidance

When the provider/user receives the module, they shall ensure that the tamper evident labels are intact, and that there is no evidence that the device has been tampered. If there is any indication that tampering might have occurred, the provider/user shall return the module to the Crypto-Officer.

Initialization

After the provider/user determines that the module is safe to use, the provider must initialize the module. This involves loading the postal configuration data, and authorizing the module to the host. The postal configuration data includes the zip code, the maximum and minimum postage, and the vital information about the module that separates the module from others of the same type (e.g. serial number, etc.).

Zeroization

When the module has reached the end of its functional life cycle the provider shall perform a Master Erase on the module. The Master Erase zeroizes all information on the module so no unauthorized access can occur. After the Master Erase, the provider shall return the module back to the Crypto-Officer.

If, for any reason, the module no longer functions properly, the provider/user shall return the module back to the Crypto-Officer.

SECURE OPERATION

The DS1955B PB4 PSD iButton meets Level 3 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

Initial Setup

Once the module has been assembled and the firmware applet has been locked onto the modules ROM, depending on the indicia format for which the module has been initialized, the iButton will either be in the FIPS140-2 compliant mode or the non-FIPS compliant mode. The module remains in this mode during the entire life of the module.

If the module has been initialized for U.S.A., Italy or France indicia format, it is considered to be in FIPS 140-2 compliant mode. On the other hand, if

the module has been initialized for German post indicia format, it is considered to be in non-FIPS mode of operation.

To determine the mode of operation, the user of the module can call the GetPSDParameters function. Field 16 of the return data structure PSD Parameter List Data indicates the indicia type for which the module has been initialized. If the indicia type is U.S.A., Italy or France, the module is in FIPS 140-2 compliant mode. If the indicia type is German post, the module is considered to be in non-FIPS mode.

The iButton provides strong physical protection of the module, and has a tamper response system that will zeroize all information on the module if it is compromised by physical tampering. The module does not contain any openings, covers, doors, or ventilation holes, and does not require tamper evident labels for FIPS mode.

ACRONYMS

ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DES/3DES	Data Encryption Standard/Triple Data Encryption Standard
DPA	Differential Power Analysis
DSA	Digital Signature Algorithm
EDC	Error Detection Code
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
GMT	Greenwich Mean Time
IBIP	Information Based Indicia Program
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
POST	Power On Self Test
PRNG	Pseudo Random Number Generator
PSD	Postal Security Device
PVD	Postage Value Download
PVR	Postage Value Refund
RAM	Random Access Memory
RNG	Random Number Generator
ROHS	Restriction of Hazardous Substances
ROM	Read Only Memory
RSA	Rivest, Shamir, And Adleman
SHA	Secure Hash Algorithm