FIPS 140-2
Security Policy

Data Pac Mailing Systems Corp.
iButton Postal Security Device

Hardware Version: MAXQ1959B-F50#

Firmware Version: 1.3

Document Date: 09/18/2012
Document Version: 1.7

Notice
© 2012 Data-Pac Mailing Systems Corporation. All rights reserved. This document may be reproduced in its entirety.Other product and company names mentioned herein may be the trademarks of their respective owners.

Table of Contents

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

1. Introduction

1.1 Overview

This is a Cryptographic Module Security Policy for Data-Pac Mailing Systems Corp. iButton Postal Security Device (PSD). The purpose of this policy is for FIPS 140-2 validation of the iButton PSD as outlined by the requirements for cryptographic modules in FIPS PUB 140-2.

The iButton PSD's purpose in relation to postal services is to provide a secure tamper proof device capable of storing customer postal credit until a request to dispense the credit in the form of valid postal indicia and then account for the request.

The iButton PSD provides data protection by keeping the Critical Security Parameters (CSPs) secret and by providing data integrity protection for Postal Relevant Data Items (PRDIs).

1.2 Scope

This security policy for Data-Pac Mailing Systems iButton PSD (Hardware Version: MAXQ1959B-F50#) outlines how the device meets the requirements of FIPS 140-2 as a multiple-chip stand-alone module. This policy has been prepared in support of overall security level 3 FIPS 140-2 validation of the module with level 3 physical security and environmental failure protection (a level 4 requirement).

1.3 References

Table 1: References

Document	Description
FIPS PUB 140-2	Security Requirements for Cryptographic Modules (05-25-2001)
FIPS PUB 180-2	Secure Hash Standard (08-01-2002)
FIPS PUB 186-2	Digital Signature Standard (DSS) (01-27-2000)

1.4 Glossary

Table 2: Glossary

Term	Description
Provider	Data-Pac Mailing Systems CMRS
iButton PSD	Data-Pac Mailing Systems Postage Security Device
Host	Data-Pac Mailing Systems Postage Metering System
Module	Data-Pac Mailing Systems iButton PSD

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

Device	Data-Pac Mailing Systems iButton PSD
CSPs	Critical Security Parameters
PRDIs	Postal Relevant Data Items

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

2. iButton PSD (HW Version MAXQ1959B-F50#)

2.1 Overview

The MAXQ1959B-F50# iButton® shown below in Figure 1 along with the USB adapter in Figure 2 is a small ROHS compliant device designed to store and protect information. The USB adapter is outside of the cryptographic boundary (as it implements no security features or cryptography), but it provides the most convenient method to interface the module with a general purpose personal computer.

When loaded with Data-Pac's proprietary PSD firmware, the MAXQ1959B-F50# becomes Data-Pac's iButton PSD implemented as a multi-chip stand-alone cryptographic module as defined by [FIPS 140-2]. The iButton PSD includes a secure micro-controller, battery backed RAM, and a tamper detection and response system. The iButton PSD is typically used in hosting systems manufactured by Data-Pac Mailing Systems Corp. The iButton PSD performs all of the postage meter cryptographic and postal security functions and protects the CSPs and PRDIs from unauthorized access.

Figure 1: Image of iButton PSD

Figure 2: Image of USB Adapter

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

2.2 Crpytographic Boundary

The cryptographic boundary of the iButton PSD using the MAXQ1959B-F50# hardware is defined by the stainless steel F5 MicroCan®. The F5 MicroCan® provides a rugged and durable outer shell that will withstand the elements of daily use including moisture without jeopardizing the data contained within the device. The iButton PSD provides a tamper response system that will zeroize the CSPs and the proprietary PSD application code while keeping the PRDIs available for retrieval.

2.3 Security Level

The iButton PSD is a multi-chip stand-alone cryptographic module as defined in FIPS PUB 140-2. The iButton PSD meets the overall requirements for level 3 security as defined in FIPS PUB 140-2. Table 3 lists the security level requirement for the different sections, as defined in FIPS PUB 140-2.

Table 3: FIPS 140-2 Security Levels

Section	Security Requirement	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services and Authentication	3
4	Finite State Model	3
5	Physical Security	3+EFT
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	(EMI/EMC)	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

2.4 Roles and Services

The iButton PSD supports three distinct roles. These roles are the Cryptographic Officer or Crypto Officer, the User, and Auxiliary. (Note the admin state requires the operator to login as the Crypto-Officer role and the active state requires the operator to login as the User role. The operator cannot change roles without proper log-off and login procedures)

2.4.1 Cryptographic Officer and User Roles

The Cryptographic Officer or (Admin role for communication with the provider) is authenticated using an identity based authentication method. This includes a random 20-byte number as the Admin login challenge response from the provider. The host passes the Connect Request response to the provider and the provider combines the challenge and the secret admin ID into a message which is then hashed with SHA-1 to produce a message digest. The provider then sends this message digest with the ADMIN login command (via the host) to the PSD. The PSD performs the same operations as the provider to determine the expected response, and compares it with the response provided on the ADMIN login command. If they match, the provider is logged into ADMIN, else an error is returned.

The User or (Active role for printing postage) is authenticated using an identity based authentication method. When the host logs in as the user, the host sends the get active challenge command to the PSD to get the ACTIVE challenge. The PSD responds with a random 20-byte number. The host combines the challenge, secret user ID, and origin ZIP into a message which is then hashed with SHA-1 to produce a message digest. The host then sends this message digest to the PHD with the ACTIVE login command. The PHD performs the same operations as the host to determine the expected response, and compares it with the response provided on the ACTIVE login command. If they match, the user is logged into ACTIVE, else an error is returned.

On processing either login command, the PSD zeroes the challenge to prevent it from being reused in any way. Also, if the PSD receives a login command while the challenge is zeroed, the login always fails, so a hacker can't keep guessing at the response.

The Cryptographic Officer and User Role shall provide those services necessary to activate, authorize and validate the iButton PSD. Furthermore the Crypto Officer role provides all services that enter or modify critical security parameters. The Data-Pac Mailing Systems Provider assumes the Cryptographic Officer role and the Data-Pac Mailing Systems Host assumes the User role.

2.4.2 Auxiliary Role

The Auxiliary Role is an unauthenticated role. The services associated with the Auxiliary Role are services performed when the host is not authenticated; furthermore, the services of the Auxiliary Role do not affect the security of the module (as the “Request Connection to Provider” command is a mandatory precursor to the “Login Administrator” command, the “Set iButton PSD Clock” is used to correct clock skew, and the Login commands themselves).

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

2.5 Services

Table 4 lists the services performed by the iButton PSD and the role required to perform each service.

Table 4: Services and Roles

Service	State	Role	Result
Login User	Inactive	Auxiliary	iButton PSD enters the Active State for services to be performed by the user
Login Administrator	Inactive	Auxiliary	iButton PSD enters the Administration State for services to be performed by the Crypto Officer.
Get Active Challenge	Inactive	Auxiliary	iButton PSD authenticates get active challenge and responds with the User Login message.
Request Connection to Provider	Inactive	Auxiliary	Provider authenticates Connection Request and responds with the Administrator Login message.
Set iButton PSD Clock	Inactive	Auxiliary	Synchronizes the iButton PSD clock with the Host clock.
Status Admin	Administration	Crypto Officer	iButton PSD will send a signed status message to the Provider.
Reset Request	Administration	Crypto Officer	Provider authenticates Reset Request and responds with the Add Funds message provided sufficient funds exist in the user's account, and requested amount is within valid range.
Add Funds	Administration	Crypto Officer	iButton PSD verifies the status information on the Add Funds message then adds funds to the descending register, and then responds with a signed status message indicating the new descending register value to the Provider. If the status information does not match the current PSD status, the funds are not added.
Refund Request	Administration	Crypto Officer	Provider authenticates Refund Request and responds with the Refund message.

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

Refund	Administration	Crypto Officer	iButton PSD verifies the status information on the Refund message then removes all funds from the descending register by setting the descending register to zero, and then responds with a signed status message indicating the new descending register value to the Provider. If the status information does not match the current PSD status, the funds are not removed.
Zero Keys	Administration	Crypto Officer	Zeroizes all CSPs. This includes the DSA private key, DSA public key, Admin ID, and User ID.
New iButton DSA Key Pair	Administration	Crypto Officer	The device generates a new DSA key pair and overwrites the old ones. The new DSA public key is output to the CMRS.
Change Origin Zip	Administration	Crypto Officer	Changes the zip code to be printed in the indicia.
Exit Admin	Administration	Crypto Officer	iButton PSD will exit the Administration State and return to the Inactive State.
Status User	Active	User	iButton PSD will send a status message to the Host.
Subtract Stamp	Active	User	Request for postage to be printed, registers will be adjusted accordingly.
Subtract Label	Active	User	Request for postage to be printed, registers will be adjusted accordingly.
Exit Active	Active	User	iButton PSD will exit the Active State and return to the Inactive State.

2.6 Algorithms

The iButton PSD cryptographic module implements the following FIPS approved algorithms:

- DSA Certificate #544
- SHA-1 Certificate #1526
- RNG Certificate #927

2.6.1 Hashing Algorithm

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

SHA-1 is used to hash data for the generation and verification of digital signatures.

2.6.2 DSA

DSA is used to authenticate messages received from the Data-Pac CMRS, to sign messages sent to the CMRS from the iButton PSD, and to create the signatures of indicia.

2.6.3 RNG

RNG is used when generating key pairs and digital signatures.

2.7 Self-Tests

The iButton PSD performs a series of self-tests upon power up. This section describes these tests. No operator inputs or actions are required by the operator to run the self-tests. The operator can perform the self-tests on demand by cycling power to the module. If the module fails any one of these self-tests it will enter an error state. All cryptographic functions are inhibited while the module is in an error state.

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

2.7.1 Power Up Self Tests

Table 5 lists the power up self tests.

Table 5: Power-Up Self-Tests

Name	When	Description
Firmware Integrity Test	On Power Up	Check CRC32 of internal system firmware.
DSA KAT Test	On Power Up	Using known values ensure that DSA signature and verification operate correctly.
SHA KAT Test	On Power Up	Tested as part of the DSA KAT Test.
RNG KAT Test	On Power Up	Fixed value for the RNG seed and Q values produce a predicable random number.

2.7.2 Conditional Self Tests

Table 6 lists the Conditional tests.

Table 6: Conditional Self Tests

Name	When	Description
Pair Wise Consistency	A DSA key pair is generated by the PSD	When a DSA key pair is generated, a test message is signed and verified.
Continuous RNG	A random number is generated by the PSD	Occurs when a random number generated by PSD is the same as the previous random number generated by PSD

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

3. Security Rules

This section describes the security rules enforced by the iButton PSD to implement the security requirements of this module.

3.1 FIPS 140-2 Related Security Rules

- The iButton PSD supports the following logically distinct interfaces on one physical port:

Logical Port	Physical Port
Data input interface	F5 MicroCan® Contact
Data output interface	F5 MicroCan® Contact
Control input interface	F5 MicroCan® Contact
Status output interface	F5 MicroCan® Contact
Power interface	F5 MicroCan® Contact

- The iButton PSD authenticates operators using role-based authentication to protect authentication data from unauthorized disclosure, modification, or substitution.
- The iButton PSD inhibits all output via the data output interface during self-tests and while in an error state.
- The iButton PSD logically separates the data output path from the processes performing key management.
- The iButton PSD does not permit the output of critical security parameters.
- The iButton PSD supports the following authorized roles: Cryptographic Officer User, and Auxiliary.
- The iButton PSD does not retain authentication of an operator when it is powered up after being powered off.
- The iButton PSD does not support a bypass mode.
- The iButton PSD protects critical security parameters from unauthorized disclosure, modification and substitution.
- All keys that are stored in the iButton PSD are associated with the crypto officer.

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

- The iButton PSD denies unauthorized access to plaintext secret keys contained within the iButton PSD.

- The iButton PSD provides the capability to zeroize all critical security parameters contained within the iButton PSD.

- The iButton PSD supports the following FIPS approved security functions:

  - DSA (FIPS PUB 186-2)
  - SHA-1 (FIPS PUB 180-2)
  - RNG (FIPS PUB 186-2 RNG)

- The iButton PSD conforms to the EMI/EMC requirements specified in FCC Part 15, Subpart B, Class A.

- The iButton PSD performs self-tests during power up as listed in section 7.

- The iButton PSD does not perform any cryptographic functions while in an error state.

- The iButton PSD always operates in a FIPS-Approved manner.

- Because a logical separation is kept in the code via different routines, the iButton PSD is able to maintain a distinct separation between data and control for input, and data and status for output.

- The iButton PSD does not provide any security critical functions beyond those required.

- The iButton PSD does not allow firmware loading.

- The iButton PSD does not supports multiple concurrent operators; only one operator is supported at any given time.

3.1.1 Postal Related Security Rules

- The iButton PSD protects the postal relevant data items (PRDIs) against unauthorized substitution or modification.

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

- PRDIs are not security relevant and are never zeroized by the iButton PSD.

- The iButton PSD provides mechanisms to disable the Active ‘1’ meter stamp and ‘2’ shipping label commands when it is not connected to its infrastructure on a regular basis.

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

4. Items Protected by the iButton PSD

This section describes the Critical Security Parameters and the Postal Relevant Data Items protected by the iButton PSD.

4.1 Critical Security Parameters

Table 8 lists the CSPs that are protected by the iButton PSD. These keys are subject to zeroization either by command or by the module's active tamper detection and response system.

Table 7: CSPs Protected by the iButton PSD

Key Name	Key Type	Size	Usage
CMRS (DP) DSA Public Key	DSA Public Key	1024 Bit	Serves to authenticate messages being received from the Data-Pac CMRS.
Data-Pac iButton PSD DSA Private Key	DSA Private Key	160 Bit	Serves to sign messages being sent to the CMRS for authentication. In addition used to create DSA for indicia.
Data-Pac iButton PSD DSA Public Key	DSA Public Key	1024 Bit	Serves to verify messages generated by the PSD.
Admin ID Login	Password	64 Bit	Serves to authenticate the Crypto Officer login.
User ID Login	Password	64 Bit	Serves to authenticate the User login.
RNG State	Internal Secret State	160-bits	Used by the Approved-RNG

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

4.1.1 Postal Relavent Data Items

Listed below are the PRDIs that are protected by the iButton PSD. These values are not subject to zeroization either by command or by the tamper detection system.

- Ascending Register
- Descending Register
- Control Total
- Cycle Count
- Postage Type
- Origin Zip
- Serial Number

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

5. CSP Modes of Access

Table 8: Modes of CSP Accesses

Mode	Description
1	CSP will be internally used
2	CSP will be entered
3	CSP will be zeroized
4	CSP will be generated

Table 9: Service to CSP Access Relationship

CSP / Service	CMRS DSA Public Key	iButton PSD DSA Public Key	iButton PSD DSA Private Key	Admin Login	User Login	Crypto Officer Role	User Role	Auxiliary Role
Login User					1			X
Login Administrator				1				X
Get Active Challenge		1	1		1			X
Request Connection to Provider	1	1	1	1				X
Set iButton PSD Clock								X
Status Admin	1		1	1		X		
Reset Request	1	1	1	1		X		
Add Funds	1	1	1	1		X		
Refund Request	1	1	1	1		X		
Refund	1	1	1	1		X		
Zero Keys	3	3	3	3	3	X		
New iButton DSA Key Pair	1	4	4	1		X		
Exit Admin				1		X		

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

Status User					1		X	
Subtract Stamp	1				1		X	
Subtract Label	1				1		X	
Exit Active					1		X	

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

6. Factory Intialization and Secure Delivery

6.1 Factory Initialization and Inventory

On completion of the manufacturing process, the iButton PSD module contains no program code and has not been initialized, and as such is not a usable cryptographic device.

After an iButton PSD is manufactured it is delivered to the Data-Pac Data Center for a number of internal factory processes including, programming (loading the module's program code) and processing into inventory. Once in inventory, the module is available for customer fulfillment.

6.2 Initialization and Secure Distribution

When a customer order is being filled, an iButton PSD is physically taken out of inventory and put through a final factory initialization process within the Data Center. The initialization process generates a unique serial number and postal data for the new iButton PSD service life and loads these initialization data into the module. The module also generates unique cryptographic keys during this process and outputs its public key to be archived within Data-Pacs's CMRS database.

After initialization, the iButton PSD is no longer part of the Data-Pac PSD inventory. It is initialized for a particular customer, and is ready for delivery and installation. The iButton PSD is not capable of producing any DSA for indicia until it is installed and a reset is performed to load funds (live or specimen) into the iButton PSD. The Host can only communicate with the iButton PSD if the Host supplies the correct User ID Login password to facilitate login to the iButton PSD User Mode. This protects the customer in the event the PSD is lost or stolen in transit. The device is shipped to the customer's location via USPS Express mail or UPS Next Day.

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

7. Tables

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.

8. Change History

Table 10: Versions and Changes

Version	Date	Author	Changes
1.0	10/18/2010	Ken Yankloski	Initial revision.
1.1	03/11/2011	Ken Yankloski	Changed FIPS over all security level to 2 throughout the document. Changed device to multi-chip embedded throughout the document. In table 4 changed the reset request and refund request to Crypto Officer role. Removed the support for HMAC and added support for DSA. Removed TDES Support.
1.2	07/08/2011	Ken Yankloski	Added the additional self tests and conditional tests to support DSA.
1.3	08/30/2011	Ken Yankloski	Made changes based on SAIC feedback.
1.4	09/02/2011	Ken Yankloski	Made changes based on SAIC feedback.
1.5	11/15/2011	Ken Yankloski	Changed FIPS over all security level back to 3 throughout the document. Changed section 2.4.1 to reference identity based login. Added get active challenge service to tables 4 and 9 to support identity based login.
1.6	03/27/2012	Ken Yankloski	Made changes based on SAIC feedback.
1.7	09/18/12	Ken Yankloski	Removed DES entry from reference table.

Copyright © Data-Pac Mailing Systems Corporation 2012. All Rights Reserved.
This document may be freely reproduced in its entirety including this notice.