FIPS 140-2
Security Policy

Data Pac Mailing Systems Corp.
AMERICA2 (PSD)

Hardware Version 1.0.25.5

Firmware Version 1.0.20.5

Document Date: 2/24/2007
Document Version: 1.7

Table of Contents

1. Introduction

1.1 Overview

This is a Cryptographic Module Security Policy for the Data-Pac Mailing Systems AMERICA2 (PSD). The purpose of this policy is FIPS 140-2 validation of the AMERICA2 (PSD) as outlined by the U.S. Governments requirements for cryptographic modules in [FIPS PUB 140-2].

The AMERICA2 (PSD) 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 a valid postal indicia and account for the request

The AMERICA2 (PSD) creates the HMAC code, which is embedded into part of the IBI Light Symmetric method for printing indicia. When the AMERICA2 (PSD) receives a request for postage from the Host, a FIPS-approved HMAC-SHA-1 algorithm is used. The algorithm uses the AMERICA2 (PSD)'s secret HMAC key to produce and return the corresponding HMAC, in lieu of the digital signature used in traditional IBI franking.

The AMERICA2 (PSD) provides data protection by keeping the Critical Security Parameters (CSPs) secret and data integrity protection for Postal Relevant Data Items (PRDIs).

1.2 Scope

This document describes the security policy for the Data-Pac Mailing Systems AMERICA2 (PSD). It is intended to describe the requirements for the secure cryptographic module only and not the entire postage system.

1.3 References

Table 1: References

Document	Description
FIPS PUB 140-2	Security Requirements for Cryptographic Modules (05-25-2001)
FIPS PUB 46-3	TDES Standard/Specification (10-25-1999)
FIPS PUB 180-2	Secure Hash Standard (08-01-2002)

1.4 Glossary

Table 2: Glossary

Term/Acronym	Description
AMERICA2 (PSD)	Data-Pac Mailing Systems Postage Security Device
Provider	Data-Pac Mailing Systems Data Center / Infrastructure
Host	Data-Pac Mailing Systems Postage Metering System

2. Implementation Architecture

2.1 Overview

The AMERICA2 (PSD), shown below in Figure 1, is implemented as a multi-chip embedded cryptographic module defined by [FIPS 140-2]. It consists of proprietary firmware and custom circuitry including a secure micro-controller, battery backed RAM, and a tamper detection and response system. The AMERICA2 (PSD) is typically used in hosting systems manufactured by Data-Pac Mailing Systems Corp. The AMERICA2 (PSD) performs all of the postage meter cryptographic and postal security functions and protects the CSPs and PRDIs from unauthorized access.

Figure 1: Photo of AMERICA2 (PSD)

2.2 Crpytographic Boundary

Shown below in figure 2 is a block diagram of the AMERICA2 (PSD). It illustrates what components are confined within the cryptographic boundary (The cryptographic boundary is represented by the dotted line in figure 2). Included within the boundary are all the major components such as the firmware, the Secure Micro-Controller, the Volatile RAM, the Non-Volatile RAM, and the Tamper Detection and Operating Environmental Monitoring System. The circuitry contained within the cryptographic boundary is enclosed within a sturdy plastic case surrounded by a tamper response wrap. This infrastructure protects the AMERICA2 (PSD) from unauthorized access and provides tamper evidence, detection and response. In the event the tamper resistant wrap is breeched the AMERICA2 (PSD) will zeroize its CSPs.

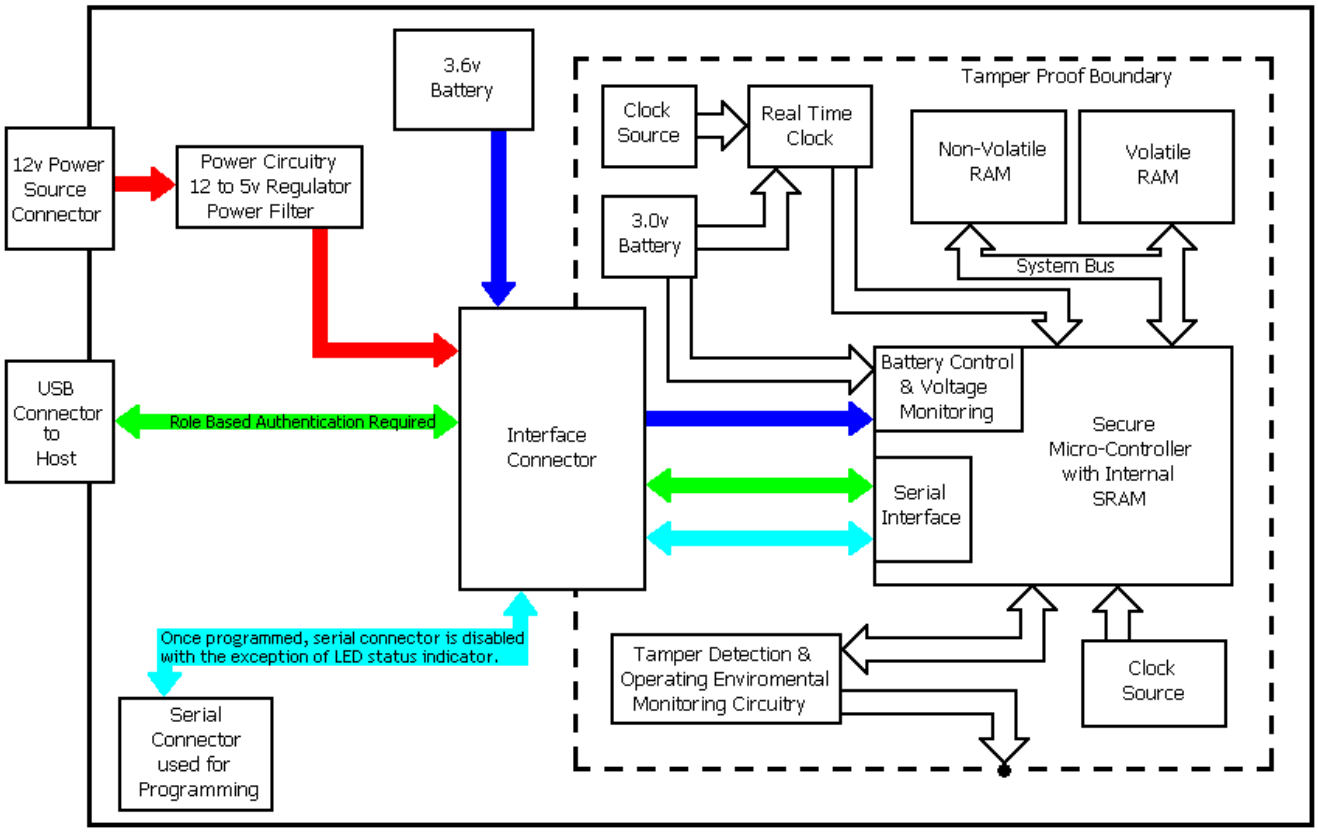

Figure 2: Block Diagram of Cryptographic Boundary

3. Security Level

The AMERICA2 (PSD) is a multi-chip embedded cryptographic module as defined in [FIPS PUB 140-2]. The AMERICA2 (PSD) meets the overall requirements for Level 2 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	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services and Authentication	2
4	Finite State Model	2
5	Physical Security	3+EFT
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	(EMI/EMC)	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

4. Roles and Services

4.1 Overveiw

The AMERICA2 (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)

4.2 Cryptographic Officer and User Roles

The Cryptographic Officer is authenticated using a role based authentication method. A unique Admin ID Login password is included in a login message, which is used by the AMERICA2 (PSD) to authenticate the Crypto Officer. One attempt at guessing the Crypto Officer password has the probability of success of one in 18e+18. In addition to exceed 1 in 100,000 attempts within one minute, an attacker has to try 18e+13 random attempts within one minute. Given the physical limitations, this many attempts are impossible.

The User is also authenticated using a role based authentication method. A User ID Login password is included in a login message, which is used by the AMERICA2 (PSD) to authenticate the User. One attempt at guessing the User password has the probability of success of one in 18e+18. In addition to exceed 1 in 100,000 attempts within one minute, an attacker has to try 18e+13 random attempts within one minute. Given the physical limitations, this many attempts are impossible.

The Cryptographic Officer and User Role shall provide those services necessary to activate, authorize and validate the AMERICA2 (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.

4.3 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 two services of the Auxilliary do not affect the security of the module (as the “Request Connection to Provider” command is a mandatory precursor to the “Login Administrator” command, and the “Set AMERIC2 (PSD) Clock” is used to correct clock skew).

4.4 Services

Table 4 lists the services performed by the AMERICA2 (PSD) and the role required to perform each service.

Table 4: Services and Roles

Service	State	Role	Result
Initialize AMERICA2 (PSD)	Non-Initialized	None	Done at the factory only under restricted access. The Data-Pac infrastructure loads the HMAC secret keys, Serial number, User ID, Admin ID, Origin zip, and Postage type.
Login User	Inactive	None	AMERICA2 (PSD) enters the Active State for services to be performed
Login Administrator	Inactive	None	AMERICA2 (PSD) enters the Administration State for services to be performed by the Crypto Officer.
Request Connection to Provider	Inactive	Auxiliary	Provider authenticates Connection Request and responds with the Administrator Login message.
Set AMERIC2 (PSD) Clock	Inactive	Auxiliary	Synchronizes the AMERICA2 (PSD) clock with the Host clock.
Status Admin	Administration	Crypto Officer	AMERICA2 (PSD) will send a signed status message to the Provider.
Reset Request	Administration	Auxiliary	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	AMERICA2 (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	Auxiliary	Provider authenticates Refund Request and responds with the Refund message.
Refund	Administration	Crypto Officer	AMERICA2 (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.
New HMAC Keys	Administration	Crypto Officer	Provider will perform a field initialization and set new HMAC secret keys.
Zero Keys	Administration	Crypto Officer	Zeroizes all CSPs. This includes the HMAC secret keys, the Triple DES keys, and the Admin ID.
Exit Admin	Administration	Crypto Officer	AMERICA2 (PSD) will exit the Administration State and return to the Inactive State.
Status User	Active	User	AMERICA2 (PSD) will send a status message to the Host.
Perform Self-Tests	Active	User	Performs the module self-tests.
Subtract	Active	User	Request for postage to be printed, registers will be adjusted accordingly.
Exit Active	Active	User	AMERICA2 (PSD) will exit the Active State and return to the

5. Algorithms

5.1 Overview

The AMERICA2 (PSD) cryptographic module implements the following FIPS approved algorithms:

- HMAC-SHA-1
- TDES
- SHA-1

5.2 Hashing Algorithms

SHA-1 is used to hash data for generation of message authentication.

5.3 HMAC

HMAC-SHA-1 is used for generating HMAC.

5.4 Decryption

TDES is used for decryption purposes.

5.5 Key Exchange

TDES is used for decryption during cryptographic key distribution. The secret Triple DES key is used to encrypt the cryptographic keys being loaded into the AMERICA2 (PSD) module. The secret Triple DES key is used by the AMERICA2 (PSD) module to decrypt the new cryptographic keys.

The existing HMAC-SHA-1 cryptographic keys are used to verify the message carrying the new cryptographic keys. On decryption of the new cryptographic keys, the existing cryptographic keys are overwritten within the AMERICA2 (PSD) cryptographic module.

No cryptographic keys are ever output from the AMERICA2 (PSD) cryptographic module in any form.

6. Security Rules

6.1 Overveiw

This section describes the security rules enforced by the AMERICA2 (PSD) to implement the security requirements of this module.

6.2 FIPS 140-2 Related Security Rules

- The AMERICA2 (PSD) supports the following logically distinct interfaces on three different physical ports:

Logical Port	Physical Port
Data input interface	USB Connector
Data output interface	USB Connector
Control input interface	USB Connector
Status output interface	USB Connector, LED interface
Power interface	Power Source Connector

- The AMERICA2 (PSD) authenticates operators using role-based authentication to protect authentication data from unauthorized disclosure, modification, or substitution.
- The AMERICA2 (PSD) inhibits all output via the data output interface during self-tests and while in an error state.
- The AMERICA2 (PSD) logically separates the data output path from the processes performing key management.
- The AMERICA2 (PSD) does not permit the output of critical security parameters.
- The AMERICA2 (PSD) supports the following authorized roles: User and Cryptographic Officer.
- The AMERICA2 (PSD) does not retain authentication of an operator when it is powered up after being powered off.
- The AMERICA2 (PSD) does not support a bypass mode.
- The AMERICA2 (PSD) is protected by a tamper enclosure.

- The AMERICA2 (PSD) protects critical security parameters from unauthorized disclosure, modification and substitution.

- All keys that are stored in the AMERICA2 (PSD) are associated with the crypto officer.

- The AMERICA2 (PSD) denies unauthorized access to plaintext secret keys contained within the AMERICA2 (PSD).

- The AMERICA2 (PSD) provides the capability to zeroize all critical security parameters contained within the AMERICA2 (PSD).

- The AMERICA2 (PSD) supports the following FIPS approved security functions:

  - Triple DES Decrypt (ECB mode)
  - HMAC SHA-1 as specified in FIPS 198
  - SHA-1

- The AMERICA2 (PSD) conforms to the EMI/EMC requirements specified in FCC Part 15, Subpart B, Class A.

- The AMERICA2 (PSD) performs self-tests during power up as listed in section 7.

- The AMERICA2 (PSD) does not perform any cryptographic functions while in an error state.

- The AMERICA2 (PSD) always operates in a FIPS-Approved manner.

- Because a logical separation is kept in the code via different routines, the AMERICA2 (PSD) is able to maintain a distinct separation between data and control for input, and data and status for output.

- The AMERICA2 (PSD) does not provide any security critical functions beyond those required.

- The AMERICA2 (PSD) does not allow firmware loading.

- The AMERICA2 (PSD) supports multiple concurrent operators and there are no restrictions for the concurrent operators.

6.3 Postal Related Security Rules

- The AMERICA2 (PSD) protects the postal relevant data items (PRDIs) against unauthorized substitution or modification.
- PRDIs are not security relevant and are never be zeroized by the AMERICA2 (PSD).
- The AMERICA2 (PSD) provides mechanisms to disable the Print Postage command when it is not connected to its infrastructure on a regular basis.
- The AMERICA2 (PSD) provides mechanisms to disable the Print Postage command when it detects its physical removal from its hosting system.

7. Self-Tests

7.1 Overwiew

The AMERICA2 (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 these 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. There is an LED interface on the module that will indicate whether the self-tests passed or failed. (Green indicates passed and Red indicates they failed.)

7.2 Firmware Tests

Table 5 lists the firmware integrity test. The CRC32 (EDC) is implemented as the firmware integrity test. The length of the CRC in the integrity test is 32 bits.

Table 5: Firmware Self-Test

Name	When	Description
Firmware Integrity Test	On power Up.	Check CRC32 of internal system firmware

7.3 Critical Function Tests

Table 6 lists the Critical Function tests.

Table 6: Critical Function Self-Test

Name	When	Description
None	None	None

7.4 Cryptographic Algorithm Tests

Table 7 lists the Cryptographic Algorithm tests. SHA-1 has it's own known answer test. The module's calculated answer must equal the module's stored answer or the power-up cryptographic algorithm self-test will fail. The module does not implement cryptographic algorithms whose outputs vary for a given set of inputs. The module does not continually compare the outputs of two, independent implementations of the same cryptographic algorithm.

Table 7: Cryptographic Algorithm Self-Test

Algorithm	FIPS Approved	Type of Self-	Conditional Test
TDES	Yes, FIPS PUB 43-6	KAT on power up.	None.
HMAC SHA-1	Yes, FIPS PUB 198-a	KAT on power up.	None.
SHA-1	Yes, FIPS PUB 180-2	KAT on power up.	None.

8. Items Protected by the AMERICA2 (PSD)

8.1 Overview

This section describes the Critical Security Parameters and the Postal Relevant Data Items protected by the AMERICA2 (PSD).

8.2 Critical Security Parameters

Table 8 lists the CSPs that are protected by the AMERICA2 (PSD). These keys are subject to zeroization either by command or by the module's active tamper detection and response system.

Table 8: CSPs Protected by the AMERICA2 (PSD)

Name	Type	Usage
Data Center Secret Key	160 Bit HMAC SHA-1 Key	Serves to authenticate messages being received from the Data-Pac Mailing Systems Provider.
AMERICA2 Secret Key	160 Bit HMAC SHA-1 Key	Serves to sign messages being sent to the Data-Pac Mailing Systems Provider for authentication. In addition used to create HMAC for indicia.
TDES Key	112 Bit TDES Key	Used to decrypt new HMAC Keys sent from the Data-Pac Resetting System.
Admin ID Login	64 Bit	Serves to authenticate the Crypto Officer login.
User ID Login	64 Bit	Serves to authenticate the User login.

8.3 Postal Relavent Data Items

Listed below are the PRDIs that are protected by the AMERICA2 (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

9. CSP Modes of Access

Table 9: Modes of CSP Accesses

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

Table 10: Service to CSP Access Relationship

CSP / Service	Data Center Secret Key	AMERICA2 Secret Key	TDES Key	Admin Login	User Login	Crypto Officer Role	User Role	Auxiliary Role	None
Initialize AMERICA2	2	2	2	2	2				X
Login User					1				X
Login Administrator		1		1					X
Request Connection to Provider		1						X	
Status Admin		1		1		X			
Reset Request		1						X	
Add Funds	1			1		X			
Refund	1			1		X			
New HMAC Keys	1,2	1,2	1	1		X			
Exit Admin				1		X			
Status User					1		X		
Subtract	1				1		X		
Exit Active					1		X		
Zero Keys	3	3	3	1,3	3	X			
Perform Self-Tests					1		X		
Set AMERICA2 (PSD) Clock								X	
Refund Request		1						X	

10. Factory Intialization

10.1 Inventory

On completion of the manufacturing process, the AMERICA2 (PSD) module contains no program code and has not been initialized, and as such is not a usable cryptographic device.

After an AMERICA2 (PSD) is manufactured it is delivered to the Data Center for programming and processing into inventory. The boot loader application is used to load the program code via the boot loader port. On successful program load, the boot loader port is locked.

The AMERICA2 (PSD) is then read by PAT (PSD Administration Tool) for the purpose of adding it to inventory. The PAT application is an application written by Data-Pac for the purpose of reading the manufacturer serial number and creating the required records within the DPReset and DPStaging databases. The PSD is then available for initialization within the Reset System. At this time the PSD is physically placed in Data-Pac inventory storage at the Data Center under restricted access.

10.2 Initialization/Distribution

When a customer order is being filled, an AMERICA2 (PSD) is physically taken out of inventory and interfaced to the PAT application within the Data Center. Authorized Data-Pac personnel then initialize the PSD for the required customer and account through PAT. The initialization process generates unique cryptographic keys and a unique serial number (generated by the PAT) for the new AMERICA2 (PSD) service life and loads these keys and initialization data into the AMERICA2 (PSD). These values are also archived within Data-Pacs's secure DPReset database in encrypted form.

Each AMERICA2 (PSD) service life is assigned its own unique set of cryptographic keys and CSPs (indicated in Table 8), generated by PAT.

There is only one Triple DES Secret Key (TDES key). The TDES key is generated (outside the module) in a sucure fashion and stored only in a cryptographic device, which is attached to the machine running the PAT application at the Data Center under restricted access, and in each AMERICA2 (PSD). It is loaded into the AMERICA2 (PSD) during initialization and cannot be changed thereafter.

Additionally, the AMERICA2 (PSD) postage type (live or specimen), and origin ZIP code are stored in the AMERICA2 (PSD) and in the DPReset database.

After initialization, the AMERICA2 (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 AMERICA2 (PSD) is not capable of producing any HMAC for indicia until it is installed and a reset is performed to load funds (live or specimen) into the AMERICA2 (PSD). The Host can only communicate with the AMERICA2 (PSD) if the Host supplies the correct User ID Login password to facilitate login to the

AMERICA2 (PSD) User Mode. This protects the customer in the event the PSD is lost or stolen in transit.

11. Tables

12. Change History

Table 11: Versions and Changes

Version	Date	Author	Changes
1.0	3/6/2006	Ken Yankloski	First Draft
1.1	3/20/2006	Ken Yankloski	Second Draft
1.2	4/7/2006	Ken Yankloski	Initial submission to Atlan.
1.3	6/14/2006	Ken Yankloski	Added hardware and firmware versions to cover page. Changed Admin ID Login in table 8. Changed Account-Services to Print Postage command in section 6.3. Removed persistent data consistency from table 5. Removed system exceptions from table 5. Changed figure 2 to reflect serial port is inside the outer case. Added User ID Login to table 8 and removed it from the PRDI,s. Added clarification as to where the cryptographic boundary is in section 2.2. Added SHA-1 KAT to table 7. Changed table 3 to reflect proper levels of FIPS validation. (Submitted to Atlan)
1.4	7/23/2006	Ken Yankloski	Removed the Register Consistency test from table 6. Removed all references to the test mode. Added logical a physical port correlation to section 6.2. Added bullet 22 in section 6.2. Changed the wording of bullet 3 in section 6.2. Added statement that the operator cannot change roles without proper login procedures in section 4.1. Changed section 6.2 bullet 18 to FCC Class A. Added probability of guessing password attempts to section 4.2. Changed section 6.2 bullet 15 to read that all stored keys in the PSD are associated with the crypto officer. In section 7.1 added that all cryptographic functions are inhibited while the module is in an error state. In section 7.1 added the fact that there is a LED to indicate whether the self-tests passed or failed. In section 7.4 added more detail on the algorithms KAT's. In section 7.2 added more detail to the software/firmware integrity test. Added section on Factory Initialization. (Submitted to Atlan)

1.5	7/27/2006	Ken Yankloski	Added bullet 23 in section 6.2. Made changes to Table 10. (Submitted to Atlan)
1.6	9/22/2006	Ken Yankloski	Made final changes at Atlan's request for submission to NIST. (Submitted to Atlan)
1.7	2/24/2007	Ken Yankloski	Made final changes to address CMVP comments