REV	EN NO.	SECTION	DESCRIPTION	BY	DATE
A	CO14985	All	Initial Release	David Collings	3/30/2007

PRODUCT CODE NO. CSO		**Pitney Bowes**	
APPROVALS			
BY	DATE	TITLE	**Pitney Bowes Cryptographic Coprocessor for Virtual Meter (CCV) Security Policy**
		PREPARED David Collings	DATE 3/30/2007
		CHECKED	DATE
SHEET 1 OF 13 SHEETS		EN NO. CO14985	DWG NO. K100001A

TABLE OF CONTENTS

1. MODULE OVERVIEW 3
1.1 Scope 3
2. SECURITY LEVEL 3
3. MODES OF OPERATION 4
4. PORTS AND INTERFACES 4
5. ROLES AND SERVICES 5
5.1 CCV Roles &Services 5
5.2 IBM Roles & Services 5
6. ALGORITHMS 6
7. SELF-TEST 6
8. OPERATIONAL ENVIRONMENT 7
9. SECURITY RULES 7
10. CSPS AND PUBLIC KEYS 8
11. DESCRIPTION OF MODES OF ACCESS 8
12. PHYSICAL SECURITY POLICY 11
13. MITIGATION OF OTHER ATTACKS POLICY 11
14. REFERENCES 11
15. DEFINITIONS AND ACRONYMS 11
15.1 Acronyms 11
16. CHANGE HISTORY 13

Table of Figures

Figure 1 - Top View of IBM 4764 Cryptographic Boundary 3
Figure 2 - Bottom Image of 4764 Cryptographic Boundary 3

Table of Tables

Table 1 - Module Security Level Specification 4
Table 2 - Role and Authentication Type 5
Table 3 - Authentication Strength Table 5
Table 4 - Approved Algorithms 6
Table 5 - Table of CCV CSPs 8
Table 6 - Table of CCV Public Keys 8
Table 7 – Roles, Services and CSPs 9

1. Module Overview

The cryptographic module is the Pitney Bowes Cryptographic Coprocessor for Virtual Meter (CCV). The CCV consists of the FIPS 140-2 validated IBM eServer Cryptographic Co-Processor Security Module (IBM CCM, Certificate #661) (Model 4764–001; HW P/Ns 41U0438 and 12R8561; Miniboot Firmware version 1.25), Segment 2 FW v1.3 (Linux OS MCP) and the CCV application (FW v03.02.05).

Figure 1 - Top View of IBM 4764 Cryptographic Boundary

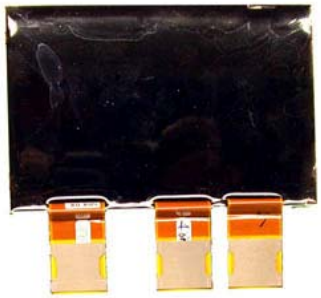

Figure 2 - Bottom Image of 4764 Cryptographic Boundary

1.1 Scope

This document describes the security policy for the CCV. Where appropriate, this document references the security policy for the previously validated IBM eServer Cryptographic Co-Processor Security Module (Cert. #661).

2. Security Level

The CCV cryptographic module embodiment is classified as a multi-chip embedded module as defined by FIPS 140-2. The physical cryptographic boundary is defined by the outer metal enclosure on five of the module's six sides and the epoxy surface on the sixth side. The encapsulated module is mounted on a PCI-X card.

The cryptographic module shall meet the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Machine	3
Physical Security	4
Operational Environment	N/A
Key Management	3
EMI/EMC	3
Self Test	3
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

The module shall not be designed with a non-FIPS Approved mode of operation. Hence, the module as configured for the current validation will always be in a FIPS Approved mode of operation.

4. Ports and Interfaces

The module communicates with its host through a PCI-X bridge chip, hosted on a PCI-X main board. Three flex-cable connectors connect the secure module to the PCI-X board; these connectors carry the following signals:

- PCI-X bus data/addresses (the module is a PCI-X master)
- PCI-X control signals
- Power, 3.3 V from PCI-X bus
- Power from batteries mounted on the PCI-X main board
- RS-232 signals
- Ethernet connector signals
- External warning control

The flex-cable connectors support the power interface and the following logical interfaces: data input, data output, control input and status output.

The module does not support a maintenance interface.

The logical interface for the CCV is command based where each command contains authentication/authorization elements to the application.

Please see the IBM eServer Cryptographic Coprocessor Security Policy (Cert. #661) for more details.

5. Roles and Services

The CCV application supports two distinct roles, the PB Crypto-Officer and the User. The module authenticates the Crypto-Officers and Users per service request. This is performed by verifying the Triple-DES MAC of the message. The message type specifies the key to be used.

Table 2 - Role and Authentication Type

Role	Authentication Method	Authentication Type
PB Crypto-Officer	2 Key TDES MAC Verification	Identity-based
PB User	2 Key TDES MAC Verification	Identity-based

Table 3 - Authentication Strength Table

Authentication Mechanism	Strength Mechanism
2 Key TDES MAC	Based on the number of protected bits in key or MAC, the probability is 1 in 2^x tries where x is the number of protected bits. The cryptographic key provides 80 bits of key strength. The MAC provides a probability of random success of 1 in 2^{64}. The module can execute 4,800 transactions per minute therefore the probability of a success in a one minute period is approximately 1 in 3.84×10^{15}

5.1 CCV Roles &Services

All services available to each role are listed in Table 7 – Modes of Access.

5.2 IBM Roles & Services

The IBM CCM (cert. #661) provides additional roles and services. The roles supported by the IBM CCM include the following:

- Crypto Officer 1
- Crypto Officer 2
- Crypto Officer 3

These roles are authenticated by the IBM eServer Cryptographic Co-Processor Security Module using DSA Signatures.

For additional information regarding the IBM eServer Cryptographic Co-Processor Security Module roles, services and authentication policy please refer to the security policy for Certificate # 661.

6. Algorithms

The cryptographic module uses the following FIPS approved algorithms provided by the IBM 4764 crypto card (certificate #661):

Table 4 - Approved Algorithms

Algorithm	Certificate	Usage
TDES	215	Encryption, decryption, message verification
SHS	194	Message hash for authentication
DSA	147	Message Signature, Message verification
RNG	132	Key generation

The module also includes the following non-approved algorithms:

- A hardware non-deterministic random number generator per IBM CCM design used for seeding the approved RNG.
- DES MAC used in the EDC calculation for the software/firmware integrity power up self-test

The IBM eServer Cryptographic Co-Processor Security Module supports other algorithms. However, the module as configured does not provide for the use of these algorithms, including:

- DES
- AES
- RSA
- MD5

7. Self-Test

The Cryptographic Module provides power-on and conditional self-tests as required by FIPS 140-2.

The module performs the following self-tests:

1. Power up tests
   a. Cryptographic algorithm tests, including:
      - AES: ECB and CBC encryption/decryption (128/192/256-bit key sizes)
      - TDES: ECB and CBC encryption/decryption (128/192-bit key sizes)
      - DES: ECB and CBC encryption/decryption

- SHA-1 hashing
- DSA: Signature/verification (1024-bit key size)
- RSA: Signature/verification (512-bit key size)
- DRNG KAT

b. Software/Firmware Integrity test: A 16-bit checksum is performed on Segment 0 firmware. An EDC calculated as a DES MAC is verified on Segments 1 through 3.

c. Critical functions test:

- RAM test
- EEPROM test
- Statistical random number generator tests are performed on the NDRNG at power up
- Interactive communications tests of the IBM 4764-001 bus
- Continuous integrity tests on modular math hardware for RSA and DSA
- Cross-checks between redundant, independent DES and TDES implementations
- Bi-directional consistency checks on AES encryption and decryption (results are run through the reverse operation to verify that the original input is restored properly)

2. Conditional tests

a. Pairwise consistency tests for RSA and DSA key pair generation

b. Continuous tests on outputs of NDRNG and DRNG

c. Software/firmware load test (DSA signature verification)

8. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements for the CCV are not applicable because the operational environment is non-modifiable.

9. Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this module.

1. The cryptographic module shall provide the PB Crypto-Officer Role.
2. The cryptographic module shall provide the User Role.
3. The cryptographic module shall provide identity-based authentication.
4. The IBM eServer Cryptographic Co-Processor Security Module shall provide all required power-on self-tests.

5. CCV shall not input or output plaintext CSPs.

10. CSPs and Public Keys

Table 5 - Table of CCV CSPs

Key	Description
Communication Key	TDES MAC key used to authenticate the PB Crypto-Officer. UNIQUE_VPSD_AUTH_COMM_3DES2_SECRET KDVAC
Key Encryption / Update Key	TDES key used for data confidentiality. UNIQUE_VPSD_PRIVACY_KEY_ENCRYPTION_3DES2_SECRET KDVPU
VPSD Record Encryption Key	TDES key used for data confidentiality. UNIQUE_VPSD_PRIVACY_UPDATE_3DES2_SECRET KDVPA
VPSD Record Signature Key	TDES MAC key used for data integrity. UNIQUE_VPSD_AUTH_DISTR_3DES2_SECRET KDVAA
VPSD IBIP Private Key	DSA private key used to sign IBIP messages. UNIQUE_VPSD_AUTH_DISTR_DSA1024_PRIVATE P'UVPA-DRD
VPSD Authentication Key (VPSD Comm Key)	TDES MAC key used for data integrity. UNIQUE_VPSD_AUTH_NONE_3DES2_SECRET KUVPA-NAD1
VPSD User Key	TDES MAC key used to authenticate the User. UNIQUE_VPSD_AUTH_USER_3DES2_SECRET KUVPA-USD1

Please see the IBM eServer Cryptographic Co-Processor Security Module Security Policy (Cert. #661) for a list of CSPs supported by the IBM CCM module.

Table 6 - Table of CCV Public Keys

Public Keys	Description
VPSD IBIP Public Key	DSA public key

Please see the IBM eServer Cryptographic Co-Processor Security Module Security Policy (Cert. #661) for a list of public keys supported by the IBM CCM module.

11. Description of Modes of Access

The table below provides a cross correlation between all roles, services, and CSPs.

Table 7 – Roles, Services and CSPs

Role			Service	Cryptographic Keys and CSPs Access Operation						
C.O.	User	Unauthenticated		KDVAC	KDVPU	KDVPA	KDVAA	P'UVPA-DRD	KUVPA-NAD1	KUVPA-USD1
x	x	x	Get Audit Status				e			
x	x	x	Get Status							
x	x	x	Get Key Information	e*						
x	x	x	Read Time	e*						
x	x	x	Prepare Device (IBIP) Audit	e*		e	e	e		
x	x	x	Create Freshness Record				e			
x	x	x	Finish Freshness Record Creation	e*						
x	x	x	Generate Freshness Data Export Request	e*						
x	x	x	Get Last Freshness Response	e*						
x	x	x	Get Last IBIP Response	e*						
x			Update TDES Key	er	er	r	r			
x			Zeroize CCV Keys	ez	z	z	z	z	z	z
x			Synchronize Time	e						
x			Set CCV Node ID	e						
x			Export Freshness Record Counters	e						
x			Import Freshness Record Counters	e						
x			Update CCV Freshness Counter	e			e			
x			Update VPSD Freshness Record	e			e			
x			Initialize VPSD Freshness Record	e			e			
x			Overwrite Stale Freshness Record	e			e			
x			Overwrite VPSD Record Freshness Counter	e			e			
x			IBIP Initialize	e	e	e	e	gre	gr	
x			Authorize VPSD	e		e	e			
x			Refill			e	e		e	
x			Refill Error			e	e		e	
x			Audit Device (Process Audit Response)			e	e		e	

Role			Service	Cryptographic Keys and CSPs Access Operation						
C.O.	User	Unauthenticated		KDVAC	KDVPU	KDVPA	KDVAA	P'UVPA-DRD	KUVPA-NAD1	KUVPA-USD1
x			Rekey VPSD	e	e	e	e	gr	gre	
x			Set Authorization Parameters			e	e		e	
x			Disable VPSD			e	e		e	
x			Enable VPSD			e	e		e	
x			Cancel VPSD			e	e		e	
x			Withdraw			e	e	e	e	
x			Generate User Key	e	e	e	e			gr
x			Update VPSD Certificate	e		e	e			
	x		Prepare Refill			e	e	e		e
	x		Dispense Indicium			e	e	e		e
	x		Dispense Correction Indicium			e	e	e		e
	x		Dispense Correction Indicium2			e	e	e		e
x	x	x	XcAdapterCount.							
x	x	x	XcOpenAdapter							
x	x	x	XcCloseAdapter							
x	x	x	XcMBOpenAdapter							
x	x	x	XcMBRequest							
x	x	x	XcRequest[1]	e	e	e	e	e	e	e

* - Note: The module uses the command key to calculate a MAC on the reply. CSPs are not modified, substituted or disclosed in the process.

e = Employed for encryption, decryption, MAC or signature generation / verification

g = Generated

r = Replaced

z = Zeroized

[1] XcRequest is a service provided by the IBM segement 2 code. This service passes application level commands to the CCV application.

12. Physical Security Policy

The cryptographic module contains tamper detection and response mechanisms and an EFP mechanism.

Please see the IBM eServer Cryptographic Co-Processor Security Module security policy for a full description of the physical security mechanisms employed by the module.

13. Mitigation of Other Attacks Policy

Please see the IBM eServer Cryptographic Co-Processor Security Module security policy for a full description of the physical security.

14. References

The following documents are referenced by this document, are related to it, or provide background material related to it:

1. Security Policy for IBM eServer Cryptographic Coprocessor Security Module - Model 4764–001 - Firmware (MiniBoot) version 1.16, Certificate #661.
2. Data Encryption Standard – FIPS PUB 46-2, March 28, 1994
3. Digital Signature Standard (DSA) – FIPS PUB 186, 1992
4. Financial Institution Retail Message Authentication – ANSI X9.19, August 13, 1986
5. Performance Criteria for Information-Based Indicia and Security Architecture for Information-Based Indicia Postage Metering Systems (PCIBISAIBIPMS), August 19, 1998
6. Performance Criteria for Information-Based Indicia and Security Architecture for Open IBI Postage Evidencing Systems (PCIBI-O), June 25, 1999
7. Secure Hash Standard – FIPS PUB 180-1, April 17, 1995
8. Security Requirements for Cryptographic Modules – FIPS PUB 140-2

15. Definitions and Acronyms

15.1 Acronyms

ANSI	American National Standards Institute
BBRAM	Battery Backup Random Access Memory
CM	Cryptographic Module
CSP	Critical Security Parameter
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standards
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing

EMC	Electromagnetic Compatibility
EMI	Electromagnetic interference
FIPS	Federal Information Processing Standards
FRDI	Funds Relevant Data Items
HMAC	A hashing algorithm used for message authentication
IBI	Information Based Indicia
ISO	International Standards Organization
MAC	Message Authentication Code
NVM	Nonvolatile Memory
PB	Pitney Bowes
PCN	Product Code Number
PKCS	Public Key Cryptography Systems
PSD	Postal Security Device
PSN	Postal Serial Number (Indicia Serial Number)
PVD	Postage Value Download
SDR	Signed Data Record
SHA	Secure Hash Algorithm
SKR	Signed Key Record
TDEA	Triple Data Encryption Algorithm
UIC	User Interface Controller
VPSD	Virtual Postal Security Device

16. Change History

Version	Section	Date	Author	Description
A	All	12/8/06	David Collings	Initial Revision of previous document for new hardware
	Multiple	12/20/06	David Collings	Revisions based on InfoGard review
	Multiple	3/15/07	David Collings	Final Revisions to Public Policy from Private
	Multiple	3/30/2007	David Collings	Changed photos and added IBM services to services and tables