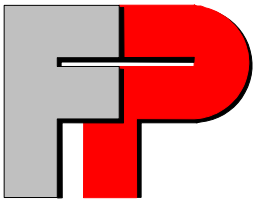

Security Policy
Postal Revenector Canada
Version 1.11

Hardware P/N: 58.0036.0001.00 Version 06

Firmware Version: 90.0036.0009.00/00

Francotyp-Postalia GmbH
- Development Department -
Clemens Heinrich
Triftweg 21-26
D-16547 Birkenwerder

Table of Contents

Figures

Tables

1 Introduction

1.1 Scope

This is a Cryptographic Module Security Policy for the *Postal Revenector Canada* as part of the FIPS 140-2 validation. This Security Policy specifies the security rules under which the *Postal Revenector Canada* must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 and additionally, those imposed by Francotyp-Postalia. These rules, in total, define the interrelationship between

- The module operators,
- Module services, and
- Critical security parameters (CSP) / postal relevant data items (PRDI).

1.2 Overview

The *Postal Revenector Canada*, shown in Figure 1-1, consists of a microprocessor controlled custom circuitry which is mounted on a printed circuit board (PCB).

The *Postal Revenector Canada* is typically used in hosting systems of Francotyp Postalia like the Postage Meter *mymail*, *ultimail* and *optimail*. The *Postal Revenector Canada* performs all of the Postage Meter cryptographic and postal security functions and protects both CSPs and PRDIs from unauthorized access.

Figure 1-1: View of *Postal Revenector Canada*

1.3 Implementation and Cryptographic Boundary

The *Postal Revenector Canada* is implemented as a multi-chip embedded cryptographic module defined by FIPS 140-2. The cryptographic boundary includes all hardware components, with the exception of the battery, the connector and the LEDs, located on the *Postal Revenector Canada*. These components are

excluded for manufacturing reasons. All excluded components are connected to the circuitry inside of the cryptographic boundary in such a way that:

- A malfunction of these excluded components cannot cause a potential release of any critical security Parameters (CSPs), plaintext data, or other information that if misused could lead to such a compromise.
- The excluded components do not process CSPs, plaintext data or other information that if misused could lead to compromised security.
- The excluded components are not connected with security relevant components of the module in such a way that would allow inappropriate transfer of CSPs, plaintext data, or other information that if misused could lead to a compromise.
- The excluded components do not in any way impact the equipment to which the module is connected.

The circuitry contained within the cryptographic boundary is enclosed within a tamper detecting hull and potted with hard opaque potting material. These elements both protect the electronic circuitry from unauthorized access and provide tamper evidence, detection and response. All *Postal Revenector Canada* software/firmware is included within the cryptographic boundary.

2 Security Level

The *Postal Revenector Canada* is designed to meet the FIPS 140-2 security level 3 overall as shown in Table 2-1.

Table 2-1: 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 + EFP
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	Electromagnetic Interference/ Electromagnetic Compatibility (EMI/IMC)	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

3 Security Rules

The *Postal Revenector Canada* shall enforce the following security rules. These rules are separated into two categories,

- Those imposed by FIPS 140-2 and,
- Those imposed by Canadian Postal Corporation (CPC) through the digital meter indicia specification [1].

3.1 FIPS 140-2 Related Security Rules

1. The *Postal Revenector Canada* shall support the following logically distinct interfaces sharing one physical port:
    - Data input interface
    - Data output interface
    - Control input interface
    - Status output interface
    - Power interface
2. The *Postal Revenector Canada* shall inhibit all output via the data output interface during self-tests and whenever an error state was entered.
3. The *Postal Revenector Canada* shall logically disconnect the output data path from the processes while performing key generation and zeroization.
4. Critical security Parameters (CSPs) are not permitted to enter the module in an unprotected form.
5. The *Postal Revenector Canada* shall not permit the output of critical security parameters in unprotected form.
6. The *Postal Revenector Canada* shall enforce identity-based authentication.
7. The *Postal Revenector Canada* shall support the following authorized roles: Operator, User and Cryptographic Officer.
8. The *Postal Revenector Canada* shall not retain authentication of an operator when it is powered-up after being powered off.
9. The *Postal Revenector Canada* shall not support a bypass mode.
10. The *Postal Revenector Canada* shall be protected using a hard opaque potting material as coating.
11. The *Postal Revenector Canada* shall be protected by a tamper enclosure.
12. The *Postal Revenector Canada* shall implement environmental failure protection for temperature and voltage.
13. The *Postal Revenector Canada* shall implement all software using a high-level language, except the limited use of low-level languages to enhance performance.
14. The *Postal Revenector Canada* shall protect critical security parameters from unauthorized disclosure, modification and substitution.
15. The *Postal Revenector Canada* shall provide means to ensure that a key entered into or stored within is associated with the correct entities to which the key is assigned.
16. The *Postal Revenector Canada* shall deny unauthorized access to plaintext secret and private keys contained within the *Postal Revenector Canada*.
17. The *Postal Revenector Canada* shall provide the capability to zeroize all critical security parameters contained within the *Postal Revenector Canada*.
18. The *Postal Revenector Canada* shall support the following FIPS approved security functions:
    - Triple DES Encrypt, Decrypt (ECB and CBC mode)
    - RSA Sign, Verify as specified in PKCS#1
    - SHA-1 as specified in FIPS 180-2
    - HMAC SHA-1 as specified in FIPS 198

- ECDSA using domain parameters for curve NIST P-192 as specified in FIPS 186-2

19. The *Postal Revenector Canada* shall support the following non-approved security functions:
    - Diffie-Hellman key agreement as specified in ANSI X9.42
20. The *Postal Revenector Canada* shall support a FIPS approved pseudo random number generator (PRNG) as specified in FIPS 186-2 Appendix 3.1
21. The *Postal Revenector Canada* shall conform to the EMI/EMC requirements specified in FCC Part 15, Subpart B, and Class B.
22. The *Postal Revenector Canada* shall perform the self tests during power on and on demand listed in section 4
23. The *Postal Revenector Canada* shall output an error indicator via the status interface whenever an error state is entered due to a failed self-test.
24. The *Postal Revenector Canada* shall not perform any cryptographic functions while in an error state.
25. The *Postal Revenector Canada* shall not support multiple concurrent operators.
26. The *Postal Revenector Canada* shall only provide a FIPS mode of operation.

3.2 Postal Related Security Rules

The *Postal Revenector Canada* shall protect the postal relevant data items (PRDIs) against unauthorized substitution or modification.

1. PRDIs are not security relevant and shall never be zeroized by the *Postal Revenector Canada*.
2. The *Postal Revenector Canada* shall comply with the specifications given in the digital meter indicia specification [1].
3. The *Postal Revenector Canada* shall provide mechanisms to disable the Accounting-Service when it is not connected to its infrastructure on a regular basis.
4. The *Postal Revenector Canada* shall provide mechanisms to disable the Accounting-Service when it detects its physical removal from its hosting system.
5. The *Postal Revenector Canada* shall provide a service mode which dumps out the PRDIs even if the microprocessor is inoperable.

4 Self-Tests

The following section lists self-tests, which are performed on power up, on demand and continuously. All FIPS approved and non-approved security functions that are used in the *Postal Revenector Canada* are listed, too.

Table 4-1: Self-Tests

Name	Type	Description
Software firmware integrity test		
Persistent data consistency	Power Up	Try to load all persistent objects from NVRAM into RAM to check whether their contents, sizes and checksums are correct.
System Exceptions	Power Up	Check internal system exceptions (tamper event, battery power alarm, NVRAM power fail)
Software integrity test	Power Up & On Demand	Check CRC16 of internal system software
Critical function test		
Register consistency test	Power Up & on Demand & continuously	Check the consistency of the postal registers. The function is called continuously before each register manipulation as a precondition of the following manipulation (finance function).
Big Number function test	Power Up & on demand	Checks the import/export functionality for big numbers using known values
Cryptographic algorithm test		
Security Function tests	Power Up (except statistical PRNG) & and on Demand	For details see Table 4-2.

Table 4-2: Security Functions

Security Function (SF)	Approved SF	Type of self-test	Conditional test
TDES	Yes, NIST certificate #391	KAT of all modes on power up and on demand.	Odd parity and weak key check.

Security Function (SF)	Approved SF	Type of self-test	Conditional test
SHA-1	Yes, NIST certificate #400	KAT on power up and on demand.	None.
RSA	Yes, NIST certificate #109	Known answer test (KAT) on power up and on demand.	On key generation: See FIPS 140-2 section 4.9.2 pair wise consistency test 3.
ECDSA, NIST P-192	Yes, NIST certificate #20	KAT of all modes on power up and on demand.	On key generation
Diffie-Hellman Key Agreement	No. Implementation according to ANSI X9.42	KAT on power up and on demand.	On key generation: See FIPS 140-2 section 4.9.2 pair wise consistency test 2.
HMAC	Yes, NIST certificate #132	KAT on power up and on demand.	None
PRNG	Yes, NIST certificate #148	KAT on power up and on demand.	On usage: See FIPS 140-2 section 4.9.2 Continuous RNG test 1.

5 Roles and Services

The *Postal Revenector Canada* shall support three distinct roles. These roles are:

- Cryptographic Officer
- User
- Operator

All services which do not read, update, modify or generate critical security parameters (CSPs) do not require authentication. These are the following Services:

Echo	This service receives arbitrary bytes and returns a copy of them back to the sender.
Reboot Device	This service reboots the module.
Get Status	This service requests status output (e.g., PRDIs and self-test result).
Invalidate Software	This service invalidates the loaded FIPS 140-2 validated software. During the next start-up of the device the device enters the FIPS approved Revenector mode (see. FIPS 140-2 Validation Certificate 361). In the Revenector mode the Postal Revenector Canada firmware can be updated according to the rules of the Revenector mode.
Creation	This service enters initial postal parameters (PRDIs).
Scrap	This service explicitly zeroizes all CSPs and sets the module out of operation.
Self-Test	The service runs the self tests and returns the result.
Setup Parameters	This service allows entering parameters used by other services.
Get Log Information	This service requests status (logged events).
Lock Out	This service explicitly disables the Accounting-Service until the PVD-Service was performed successfully.
Reset HS-Loop	This service re-enables the Accounting-Service after being moved between host systems
Get Certificate	This service requests status (stored certificates of public keys)

5.1 Cryptographic Officer and User

The *Cryptographic Officer* is authenticated using an identity based authentication method. This method is based on two pairs of asymmetric keys and distinguished names. The public parts and distinguished names are known to each other party. The *Postal Revenector Canada* and the *Cryptographic Officer* are able to identify and authenticate themselves by verifying the exchanged distinguished name and signature of each other. In addition the Diffie-Hellman key agreement protocol can be used to agree on secret keys for further key encryption and continuous authentication of data exchange.

The *User* is also authenticated using an identity based authentication method. This method is based on two pairs of asymmetric keys and distinguished names. The public parts and distinguished names are known to each other party. The *Postal Revenector Canada* and the *User* are able to identify and authenticate themselves by verifying the exchanged distinguished name and signature of each other. In addition the Diffie-Hellman key agreement protocol can be used to agree on secret keys for further key encryption and continuous authentication of data exchange.

The Cryptographic Officer and User Role shall provide those services necessary to initialize, authorize and validate the *Postal Revenector Canada*. Furthermore these roles apply to all services that enter, modify or generate critical security parameters.

The Francotyp Postalia Infrastructure Server assumes the Cryptographic Officer and User roles. The following services are provided in these roles and require authentication:

Remote Login	This service carries out the Cryptographic Officer authorization process. The subsequently listed services demand an authorized connection established beforehand.
Enter PKM Certificate	This service enters the country specific infrastructure certificate. PKM stands for Public Key Management. The country specific infrastructure certificate is typically abbreviated as PKM certificate.
Initialization	This service performs the postal Initialization-Function as specified by the postal authority (setup of PRDIs). It initially prepares the *Postal Revenector Canada* for operation in a Host System.
Authorization	This service performs the postal Authorization-Function as specified by the postal authority (setup of PRDIs). It prepares the *Postal Revenector Canada* for operation at a customer site by entering customer specific PRDIs and disables the Authorization-Service.
Postage Value Download	This service audits the PRDIs of the module and on success downloads postage from the country specific infrastructure.
Postage Value Refund	This service audits the PRDIs of the module and on success refunds the remaining postage of the module back to the country specific infrastructure.
Re-Initialization	This service changes the internal lifecycle state of the module (PRDI). It re-enables the module for another postal Authorization-Function.
Re-Authorize	This service updates postal parameters in the security device (registration postal code and province).
Renew PKM Certificate	This service re-enters the country specific infrastructure certificate.
Reenter FP-MAC Key	This service enters the FP-MAC Verification Key in encrypted format.
Rekey PSD[1] Key	This service re-keys the *Postal Revenector Canada* Key inside of the module.
Secure Echo	This service is used for authenticated testing purposes.
Secure Get Status	This service requests authenticated status output.
Secure Set Time	This service updates the internal time in the security device.
Secure Set Parameter	This service updates postal parameters in the security device (minimum and maximum accounting amount)

5.2 Operator

The *Operator* performs services on behalf-of the User and Cryptographic Officer role.

The *Operator* is the end user of the postal meter that shall perform postal related services.

[1] PSD is the abbreviation for Postal Security Device. The term PSD is typically used by the postal authorities.

The following services are provided to the *Operator* Role:

Account Administration	This service supports customer privilege levels to access postal specific services as listed below.
Accounting	This service requests to perform postal indicia creation *by* modifying the PRDIs in accordance to the requirements of the postal authority.
Redate	This service requests to perform postal indicia creation *without* modifying the PRDIs in accordance to the requirements of the postal authority.
Verify MAC	This service performs verification of data which was provided to the module.

6 Strength of Authentication

To meet the requirements for strength of authentication, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur.

This requirement is met by the above-specified authentication methods as follows:

The size of the RSA key used to authenticate each role is at least 1024 bits.

For multiple attempts to use the authentication mechanism during a one-minute period the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur. In order to satisfy this requirement, the module must enforce a limit of 1667 attempts per second or a minimum time delay of 0,6 ms between two attempts. This time is granted by the implementation by a time delay of 0,6 ms after a false attempt.

7 Critical Security Parameters

The *Postal Revenector Canada* protects several critical security parameters described in Table 7-1.

Table 7-1: CSPs protected by the Postal Revenector Canada

Name	Abbr.	Type of Key	Purpose
PSD[1] Transport Signing (private) Key	TSK	1024 bit RSA key	Serves to properly recognize devices of type *Postal Revenector Canada* after they have been shipped to their destination country and establish initial secure session (Crypto Officer Login) to upload the first PSD[1] Key certificate.
PSD[1] Signing (private) Key	PSK	1024 bit RSA key	Serves to setup regular secure sessions (Crypto Officer Login) for communication between the *Postal Revenector Canada* and the FP Data Center.
MAC Verification Key	MVK	112 bit TDES key	Serves to derive a Record Verification Key.
Ephemeral Diffie-Hellman	EDH	2048 bit DH key agreement	Serves to derive session keys for the Cryptographic Officer (secure session)
Session Authentication Key	SAK	160 bit HMAC SHA-1 key	Serves to authenticate data during a secure session.
Session Encryption Key	SEK	112 bit TDES key	Serves to encrypt and decrypt data during a secure session.
State of Pseudo Random Number Generator	RNGS	N/A	Internal state of the Pseudo RNG. The value is changed by every random generation of the *Postal Revenector Canada*.
Indicia Signing Key	ISK	192 bit ECDSA key (NIST P-192)	Used as specified in the postal specification [1].
Security Code Secret	SCS	160 bit HMAC-SHA-1 key	Serves to derive the human readable security code in the indicia.

8 Service to CSP Access Relationship

The *Postal Revenector Canada* distinguishes between the following modes of access:

Table 8-1: Modes of CSP Accesses

Mode	Description
I	The CSP will be initialized
U	The CSP will be internally used (optional on demand)
M	The CSP will be modified and written
E	The CSP will be entered
G	The CSP will be generated
Z	The CSP will be zeroized
D	The CSP will be derived using other CSPs

Table 8-2 shows the authorized service in relation to the modes of access of critical security parameters.

Table 8-2: Service to CSP Access Relationship

CSP / Authorized Service	TSK	PSK	ISK	SCS	MVK	EDH	SAK	SEK	RNGS	CO Role	User Role	Operator
Renew PKM Certificate							U			x		
Enter PKM Certificate										x		
Secure Echo							U	U		x		
Secure Set Time							U			x		
Secure Set Parameter							U	U		x		
Postage Value Download			G,M	G,M			U	U	M	x		
Postage Value Refund							U	U		x		
Reenter FP-MAC Key					M		U	U		x		
Re-key PSD[1] Key		M,U					U		M	x		
Initialization	U	G,U			E		U	U	M	x		
Authorization							U	U		x		
Re-Initialization							U	U		x		
Re-Authorize							U	U		x		
Accounting			U	U					M			x
Redate			U	U					M			x
Verify MAC					U							x
Get Secure Status							U	U		x		
Scrap	Z	Z	Z	Z	Z				Z	x	x	x
Remote Login		U				D,G,U	D	D	M	x		
Logoff						Z	Z	Z		x	x	x

9 References

[1] Digital Meter Indicia Specification, Canada Post Specification 3457, V1.2, 2003