IJ25 SECURE METERING MODULE (SMM) SECURITY POLICY

Compiled By: W.J. HERRING
PRINCIPAL ELECTRONICS DESIGN ENGINEER
NEOPOST LIMITED

Update By: L. TAYEB
SOFTWARE ENGINEER
NEOPOST INDUSTRIE

TITLE: IJ25 Secure Metering Module (SMM) SECURITY POLICY

ABSTRACT: Overview description of Secure Metering Module, unit embedded within the Neopost IJ25 postal franking machine.

DATE	ISSUE	AMENDMENT DESCRIPTION
12.09.2001	A	First Issue
05.08.2005	B	Add ECDSA cryptographic module. Update following Canada launch
06.10.2005	C	Update following FIPS recommendation
12.10.2005	D	Update soft release after Fips recommendation change
09.06.2006	E	Address NIST/CSE comments
29.09.2006	F	Fix security code computation issue and address additional NIST/CSE comments
01.06.2007	G	Add NIST/CSE comments and update document release name

Originator: Date:

Authorised By: Date:

CONTENTS

IJ25 SECURITY POLICY

1 INTRODUCTION

The IJ25 Secure Metering Module (SMM) is a unit embedded within the Neopost IJ25 postal franking machine. Integrated within the SMM are a cryptographic submodule and postal services submodule.

The postal services relate to the ultimate objective of the SMM which is to store postage credit belonging to a customer until it is needed by the indicium dispensing system of the franking machine. The indicia are dispensed in the form of a digitally signed image. This image is a unique bit pattern that can be determined to have originated from a particular SMM at a particular point in time.

The cryptographic functions are used to restrict access to postal services and to authenticate where necessary postal service output.

1.1 SCOPE

This document contains a statement of the security rules under which the SMM must operate. A number of these rules are wholly or partially a consequence of the general franking machine environment in which the SMM is intended to be placed and for this reason a brief description of this environment is included.

1.2 SMM VERSION IDENTIFICATION

Hardware	4127925W A
Firmware	4130171L K01

2 REFERENCES

1. Digital Meter Indicia specification / Canada post specification 3457 version 1.2

2. Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-2

3. Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2

4. Secure Hash Standard, Federal Information Processing Standards Publication 180-2

5. Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), American national Standard for Financial Services X9.62-1998.

6. HMAC keyed-Hashing for Message Authentication Code, RFC 2104

3 GLOSSARY

CSP	Critical Security Parameter
DSA	Digital Signature Algorithm (Reference 3)
ECDSA	Elliptic Curve Digital Signature Algorithm (Reference 5)
HMAC	Hash Function Based Message Authentication Code
FIPS	Federal Information Processing Standard (USA)
G	DSA common parameter G
I/O	Input / Output
MTBF	Mean time between failures
NVEM	Non Volatile Electronic Memory
P	DSA common parameter P
Q	DSA common parameter Q
RNG	Random Number Generator
SRDI	Security Related Data Items
SMM	Secure Metering Module
X	DSA private key
Y	DSA public key

4 SECURITY LEVEL

The SMM is a multi-chip embedded cryptographic module as defined in Reference 2. The SMM shall meet the overall requirements for Level 3 security plus EFP/EFT as defined in Reference 2. The following table shows the security level requirement, as defined in Reference 2, for each area of the SMM:

	Level
Cryptographic Module	3
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Machine	3
Physical Security	3 + EFP/EFT
Operating System Security	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

* N/A = not applicable

5 SMM OVERVIEW

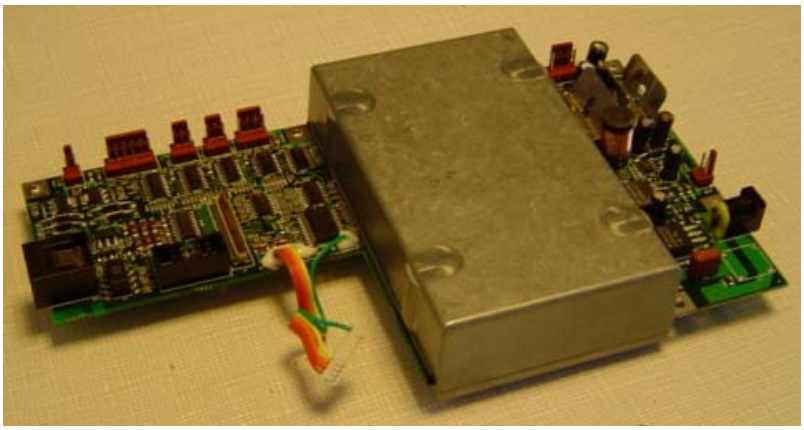

Figure 1 - SMM

The SMM consists of a cryptographic submodule and postal services submodule sharing common hardware that is contained on a printed circuit board (PCB) and enclosed within a tamper responsive enclosure. This enclosure constitutes the cryptographic physical boundary.

The SMM contains dual redundant non-volatile electronic memories which enables both security-related data items and postal related data items to be stored in duplicate if required. Duplicate storage is typically used to increase MTBF.

The SMM will input and output authenticated data that requires the services of the cryptographic subfunction. The SMM will also input and output certain other data that has no security implications and that is permitted to pass freely across the cryptographic physical boundary. This latter data relates to the general control and use of the franking machine in which the SMM is embedded.

The SMM has only a FIPS mode; it does not support any non-FIPS mode of operation. The SMM is not designed to mitigate specific attacks outside of FIPS 140-2 (Reference 2).

5.1 I/O PORTS

A number of data channels extend outside the enclosure. These are described in the following with respect to their use inside the SMM up to the point at which they enter/exit the physical enclosure. However, for convenience of reference, they are named according to their use externally to the SMM.

5.1.1 General Port

This is a serial communication port. Both authenticated and non-authenticated data will be input/output through this port.

This port is so named as externally to the SMM, its normal purpose is to interface to general peripherals via a RS232 link.

5.1.2 Modem port

This is a serial communication port whose operation and role is the same as that described for the general port.

This port is so named as externally to the SMM, its normal purpose is to interface via a Modem.

5.1.3 User Interface (UI) Port

This is a serial communication port whose operation and role is the same as that described for the General port.

This port is so named as externally to the SMM, its normal purpose is to link to a user interface unit that comprises keyboard, display and memory card reader.

5.1.4 Print Mechanism Control Port

This is an output only data channel whose only function is to output authenticated postal indicium.

5.1.5 Print Mechanism Status Port

This is an input only data channel. No authenticated data is received via this channel. The channel inputs only non-security critical indicium dispensing progress data.

5.1.6 Power Supply Port

This is an input only port which provides for the supply of power to the module.

A regulated 5 V power is supplied to the module from outside the cryptographic boundary. Although the PCB maintains regulated 5 V and 12 V, only 5 VDC is supplied to the SMM. Therefore, only 5 V power input was tested during EPT/EFT testing.

6 ROLES, SERVICES AND AUTHENTICATION

The SMM shall support two distinct operators. The SMM shall enforce separation of entities using identity-based authentication and by restricting the services available to both entities. Also some services are state dependent. The allowable operators are the Neopost Administrator and the Customer:

The Neopost Administrator incorporates both the Crypto officer and User roles referred to in Reference 2.

For identity based authentication the ID must first have been selected and then all input data must be accompanied by a cryptographic signature, which is derived from the input data, and from cryptographic parameters unique to that entity. The cryptographic parameters used must already be present in the SMM.

For the Administrator the cryptographic parameters must be input subsequent to manufacture.

The relationship between SMM services and authenticated entities are summarised in Appendix 1.

6.1 NEOPOST ADMINISTRATOR

The Neopost Administrator shall provide the services required to maintain the parameters within the SMM that are necessary for interaction with the Neopost metering infrastructure.

The Neopost Administrator shall also provide those services necessary to control, sustain, and monitor the postal operation of an SMM (i.e. postage funding, usage auditing, withdrawal, etc.). These shall require the identity of the operator to be provided and authenticated.

The Neopost Administrator services are:

6.1.1. Firmware Download

This service will carry out the following:

- Input the firmware digitally signed (i.e. DSA signature).
- Verify the signature is correct.
- Update the firmware.

6.1.2. Zeroize Private Key Service

This service will carry out the following:

- Input an non-authenticated message containing a request to zero the current private key.

- Verify that the SMM is in the appropriate state for acceptance of a ‘Zeroization’ service request.

- Zero all CSPs (i.e. including private keys).

6.1.3. Customer Enable Service

This service will:

- Input an authenticated message containing postal critical data items, plus an X509 Certificate containing a certified SMM DSA public key.

- Verify the authentication.

- Verify that the SMM is in the appropriate state for acceptance of a ‘Registration’ service request.

- Extract and store the postal data items.

- Extract and store the X509 SMM DSA public key Certificate.

- Set the SMM state ‘Customer enabled’.

6.1.4. Postal Administration Service

This service will:

- Input an authenticated message containing a postal function command and optionally accompanied by postal critical data items required by the function.

- Verify the authentication.

- Verify that the SMM is in the appropriate state for acceptance of a ‘Postal Admin’ service request.

- Perform the specified postal function using the optionally provided postal data as required.

6.1.5. Customer Disable Service

This service will:

- Input an authenticated message requesting that the SMM set itself to the ‘Withdrawn’ state.

- Verify the authentication.
- Verify that the SMM is in the appropriate state for acceptance of a 'Withdrawal' service request.
- Authenticate and output a message containing specific postal critical data items required by Neopost before an SMM is disabled.
- Set the SMM state 'Customer disabled' thereby inhibiting further access to the Administrator services and certain postal critical customer role services.

6.1.6. Self Test Service

This service will perform those self tests required by Reference 2. The SMM performs the tests automatically and no authentication is required.

6.2 CUSTOMER

These services are available on behalf of the Neopost Administrator. They all require the SMM to be in an appropriate state. The services are:

6.2.1. Postal Indicium Service

This service requests printing of a postal indicium.

6.2.2. Postal Administration Request Service

This service requests that the Neopost Administrator authenticate to the meter and perform appropriate authenticated operations.

6.2.3. General Non-Postal Service

This service requests non-postal data status output.

7 SECURITY RULES

7.1 AUTHENTICATION RULES

7.1.1 The SMM shall provide two distinct operators, the Neopost Administrator and the Customer.

7.1.2 The SMM shall provide identity-based authentication.

7.1.3 Message authenticating signatures shall be 40 byte digital signature codes derived using the DSA algorithm, as described in Reference 3, using 1024 bit common parameters (P,Q,G). Random number generation employed by the DSA shall be according to section 3.2 and 3.3 of Reference 3.

7.1.4 The cryptographic parameters (P,Q,G,Y) for each identity authenticated shall be independent and shall be stored in predetermined fixed locations within the SMM. These shall be able to be superseded by subsequent input values if required. The parameters for the Administrator must be input after manufacture.

7.1.5 The SMM shall authenticate exported data with 40 byte digital signature codes derived using the DSA algorithm, as described in Reference 3, using 1024 bit common parameters (PQG). Random number generation employed by the DSA shall be according to section 3.2 and 3.3 of Reference 3.

7.1.6 For any attempt to use the authentication mechanism then the probability that a random attempt will be accepted or that a false acceptance will occur will be at least 1 in 2^{80} (equivalent to at least 12 x 10^{23}).

The DSA key is 160 bits and is considered to have at least 80 bits of strength. This is considerably more difficult to break than the 1 in 1,000,000 requirement.

7.1.7 The minimum time to generate an authentication shall be 100ms.

For multiple attempts to use the authentication mechanism then the probability that a random attempt will be accepted or that a false acceptance will occur will be 1 in 2^{80} divided by 600 (equivalent to 2 x 10^{21}). This is considerably more difficult to break than the 1 in 100,000 requirement.

7.1.8 Stamp authenticating signature shall be ECDSA 192 curve as describe in Reference 5. The private key used to sign data is stored in a protected area. The message, the signature and a verifiable public key are directly encoded in the 2-dimensional (2D) barcode.

7.1.9 The human readable data of the postage indicium is used to compute the Security Code, an error detection code using HMAC-SHA-1-30 (non-Approved security function), which is represented by 5 ASCII printable characters as described in Reference 1.

7.2 KEY GENERATION

7.2.1 The SMM DSA Private key shall be generated according to section 3.1 and 3.3 of Reference 3 in the Neopost Factory.

> Note that there will be only one random number implementation but with two separate states maintained, i.e. one for DSA signatures and one for generation of keys.

7.2.2 The SMM DSA public key corresponding to its the private key shall be calculated according to the relationship for derivation of a DSA public key defined in Reference 3.

7.2.3 The SMM ECDSA private and public keys shall be generated according Reference 5. The initial key is generated in the Neopost Factory. The key can be generated in the field when an update is requested.

7.2.4 During private/public key pair generation all data output from the SMM shall be inhibited.

7.2.5 The SMM HMAC secret key shall be generated using a random number generator in the factory.

7.3 CONDITIONAL SELF TEST RULES

7.3.1 If one of the keys pairs (DSA or ECDSA) is invalid then both the SMM private key and public key shall be erased (to zero) and the SMM shall inhibit all data output. The validity of a key pair shall be determined by a pair wise consistency check, i.e. the calculation and verification of a signature. This check shall be performed at the generation of each new key pair and at power up.

7.3.2 For both the private key and signature random number generators, the SMM shall perform the continuous random number generator test, as defined in Reference 2 for conditional self tests, for every number generated and inhibit all data output if its random number generator fails to a constant value.

7.3.3 For the private key random number generator, the SMM shall perform the statistical tests for randomness as defined by Reference 2 upon demand (i.e. when the module is requested to generate a private key). The SMM shall inhibit all data output if the test fails. (These tests are no longer actually required by NIST.)

7.3.4 If the key pair ECDSA is invalid, then both the SMM ECDSA private key and ECDSA public key shall be erased (to zero) and the SMM shall inhibit all data output. The validity of a key pair shall be determined by a pair wise consistency check, i.e. the calculation and verification of a signature. This check shall be performed at the generation of each new key pair and at power up.

7.4 POWER UP SELF TEST RULES

7.4.1 The SMM shall test the operation of RAM areas used for secure operations at power up. The SMM shall inhibit all data output if the test fails.

7.4.2 The SMM shall test the contents of its program memory area at power up by calculating the 16 bit checksum (sum of bytes) of the contents and comparing the result with a known answer. The SMM shall inhibit all data output if the test fails.

7.4.3 The SMM shall test the accessibility and validity of all CSP values in NVEM at power up. If any are not accessible (i.e. device failure) or contain erroneous data then the SMM shall inhibit all data output.

7.4.4 The SMM shall test the DSA algorithm at power up by performing a known answer test for both signing and verification using predetermined data embedded into the SMM firmware. Known answer testing of the secure hash algorithm (SHA-1) and for the authentication random number generator (PRNG) shall be inclusive within the DSA test. The SMM shall inhibit all data output if the test fails.

7.4.5 For the signature random number generator, the SMM shall perform the statistical tests for randomness as defined by Reference 2 at power up. The SMM shall inhibit all data output if the test fails. (These tests are no longer actually required by NIST.)

If in an RNG error state the test will be repeated upon demand.

7.4.6 The public key for administrator identity shall be stored along with an authenticating signature which shall be calculated using the SMM's own key private key. If this signature fails to be verified at power up then the public key for each identity shall be erased (to zero) and the SMM shall inhibit all data output.

7.4.7 The SMM shall test the ECDSA algorithm at power up by performing a known answer test for both signing and verification using predetermined data embedded into the SMM firmware. Known answer testing of the secure hash algorithm (SHA-1) and for the authentication random number generator (PRNG) shall be inclusive within the DSA test. The SMM shall inhibit all data output if the test fails.

7.4.8 The SMM shall test the HMAC algorithm at power up by performing a known answer test using a predetermined data embedded into the firmware.

7.5 CSP STORAGE

7.5.1 The SMM shall detect data corruption of the value held for any particular CSP by the incorporation of 16 bit error detection data.

7.5.2 Any CSP access failure shall cause the SMM to inhibit all data output. Exit from the inhibit condition shall require the SMM to recheck access to, and the values of, all CSP.

7.6 TAMPER RESPONSE

7.6.1 All CSPs shall be erased (to zero) from crypto-RAM if the SMM physical cryptographic boundary is breached. At the same time the SMM shall enter an inhibited state.

7.6.2 All CSPs shall be erased (to zero) from crypto-RAM if the temperature inside the SMM covers exceeds 77 degrees Centigrade. At the same time the SMM shall enter an inhibited state.

7.6.3 The private keys shall not be exported under any circumstances.

7.7 STATUS INDICATION

7.7.1 The following 'module not ready' module states shall be indicated:

- Private key zeroed
- Private/Public key pairs invalid (module not initialised)
- Tamper mechanism tampered
- Neopost Administrator public key authorisation signature invalid.
- HMAC key index invalid

Indication will be via a unique text message output by the module suitable for viewing on an alphanumeric display device. The absence of one of these messages indicates that the module is in a 'ready' state.

7.7.2 The following 'module inhibited' error conditions shall be indicated:

- DSA error
- RNG error
- Firmware / RAM error
- High temperature detected error
- ECDSA error
- HMAC error

Indication will be via a unique text message output by the module suitable for viewing on an alphanumeric display device. The absence of one of these messages indicates that the module does not have an error condition.

7.7.3 The module shall indicate the currently active role.

Indication will be via a unique text message output by the module suitable for viewing on an alphanumeric display device.

7.8 OPERATORS/CUSTOMERS

7.8.1 Operators/customers shall be instructed to check for any errors, indicated by the status output, or for tamper evidence. Detection of any such errors or tamper evidence shall be required to be reported to Neopost such that the return of the SMM to the factory environment for withdrawal can be arranged.

8 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSP)

The following table describes each CSP maintained by the SMM:

CSP NAME	DESCRIPTION
DSA random number 1 seed	Current status of the seed value used by the random number generator during signature generation. This seed represents the state for the generation of signatures.
DSA random number 2 seed	Current status of the seed value used by the random number generator during key generation. This seed represents the state for the generation of keys.
SMM DSA private key	The SMM private DSA key is used to authenticate messages and data output from the SMM.
SMM ECDSA private key	The SMM private ECDSA key is used to authenticate data output from the SMM.
DSA K value	Current random number derived from the 'DSA random number 1 seed' by PRNG state 1 and used during DSA signature generation.
Previous DSA K value	Previous random number derived from the 'DSA random number 1 seed' and used during continuous testing of the PRNG state 1 to ensure that consecutive random numbers are not equal.
Previous DSA X value	Previous random number derived from the 'DSA random number 2 seed' and used during continuous testing of the PRNG state 2 to ensure that consecutive random numbers are not equal.
HMAC Key value	The SMM HMAC value used to generate the security code as a human readable message in the indicia

The following table describes public key parameters of the SMM:

NAME	DESCRIPTION
Neopost Administration DSA public key	Public key used for the verification of authenticated messages input from the Neopost Administration server.
Neopost Administration DSA common P	Common cryptographic DSA parameter (P) associated with the Neopost Administration services.
Neopost Administration DSA common Q	Common cryptographic DSA parameter (Q) associated with the Neopost Administration services.
Neopost Administration DSA common G	Common cryptographic DSA parameter (G) associated with the Neopost Administration services.
Neopost Program Support DSA public key	Public key used for the verification of authenticated messages input from the Neopost Program Support: Factory or country key.
SMM DSA public key	DSA Public key of the SMM. Available to any operator with a need to verify authenticated data output by the SMM.
SMM ECDSA public key	ECDSA Public key of the SMM. Available to any operator with a need to verify authenticated data output by the SMM.

9 DEFINITION OF CSP MODES OF ACCESS

The section describes how CSP are accessed by the services that can be activated by an operator. The modes of access are defined as follows:

r The data item will be read for internal use.
e The data item will be read and exported.
w The data item will be updated directly from an imported value.
m The data item will be modified to a value created by an internal process.
z The data item will be zeroed.
s The data item will be initialised to a starting value created by an internal process.
i The data item will be initialised to a benign value (typically zeroed).

The following table summarises the relationship between all CSP maintained by the SMM and the services that access them:

Service Name ▸ / Public Key Parameter Name ▾	Zeroise Private Key	Customer Enable	Postal Administration	Customer Disable	Postal Indicium	Postal Administration Request	General Non-Postal	Self-test
DSA random number 1 seed	z				m	m		m
DSA random number 2 seed	z							
SMM DSA private key	z				r	r		r
DSA K value	z				m	m		m
Previous DSA K value	z				m	m		m
Previous DSA X value	z							
SMM ECDSA private key	z				r	r		r
SMM HMAC key	z	r	r		r	r		

The following table summarises the service relationships for public key parameters maintained by the SMM:

Service Name ▸ / Public Key Parameter Name ▾	Firmware Download	Zeroize Private Key	Customer Enable	Postal Administration	Customer Disable	Postal Indicium	Postal Administration Request	General Non-Postal	Self-test
SMM DSA public key									r
Neopost Administration DSA public key			r	r	r				
Neopost Administration DSA common P			r	r	r	r	r		r
Neopost Administration DSA common Q			r	r	r	r	r		r
Neopost Administration DSA common G			r	r	r	r	r		r
Neopost Program Support DSA public key	r								
SMM ECDSA public key									r

10 APPENDIX 1

The following table summarises the relationship between services and operators for the SMM:

OPERATOR ▸ / SERVICE ▾	ADMINISTRATOR	CUSTOMER
Zeroize Private Key	✔	
Firmware Download	✔	
Customer enable	✔	
Postal Administration	✔	
Customer disable	✔	
Postal Indicium		✔
Administration Request		✔
General Non-Postal		✔
Self-test	✔	✔

Service is not accessible to a particular entity unless specifically indicated:
✔ = can be accessed

11 APPENDIX 2

The following table summarises the SMM ports on which services are permitted to be active:

PORT ▸ / SERVICE ▾	GENERAL PORT	MODEM PORT	UI PORT	PRINT MECHANISM CONTROL PORT	PRINT MECHANISM STATUS PORT	POWER SUPPLY PORT
Zeroization	✔	✔				✔
Firmware Download		✔				✔
Customer enable	✔	✔				✔
Postal Administration	✔	✔				✔
Customer disable	✔	✔				✔
Program Down load	✔	✔				✔
Postal Indicium				✔		✔
Administration Request	✔	✔				✔
General non Postal			✔			✔
Self Test	NA	NA	NA	NA	NA	✔

A service is not permitted via a port unless specifically indicated:
✔ = permitted