SPEC.374/G

neopost

Research & Development

C20ND – C21ND
Secure Metering Module
SECURITY POLICY

Writers : Adriana ROSCA / Frédéric LE SCOUARNEC

TITLE: C20ND-C21ND SECURITY POLICY

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

neopost	**REVISIONS APPROVAL, DIFFUSION**	SPEC.374-G

REVISIONS

Issue	DATE	REVISION CAUSE
SPEC.374/A	29/07/2005	Document creation.
SPEC.374/B	24/08/2005	Update specification according to Keops Action Item List document.
SPEC.374/C	19/11/2005	Upgrade meter software reference.
SPEC.374/D	14/02/2006	Corrected errors in response to NIST comments
SPEC.374/E	15/02/2006	Add TDES known answer test description
SPEC.374/F	24/02/2006	Corrected errors in response to NIST comments
SPEC.374/G	15/11/2006	Add C21ND references

This document cancels and takes the place of the previous one.

It is possible to refer to the previous versions in Documentation Service.

VERIFICATION

	DATE	APPROVAL	NAME
Writers	29/07/05		A. ROSCA F. LE SCOUARNEC
Project manager			J. MODOLO

DIFFUSION

Signatories +			

CONTENTS

1 INTRODUCTION

The C20ND or C21ND Secure Metering Module (SMM) are units embedded within the Neopost KEOPS postal franking machine. Integrated within the SMM are a cryptographic sub function and postal services sub function.

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 MARKET VARIATION

This document focus on rules dedicated to Canada market. Some rules devoted to others markets aren't detailed here. However further revisions of this document shall detail these features.

1.3 SMM VERSION IDENTIFICATION

	C20ND	C21ND
Hardware	4124558P-B	
Firmware	"30.20"	"30.24"

2 REFERENCES

1. Digital Meter Indicia Specification v1.2, MAY 2003.

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. ANSI X9.62-1998 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

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

6. Test cases for HMAC-MD5 and HMAC-SHA_1, RFC 2202.

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

8. ANSI X9.31 Standard, Financial Institution Key Management (Wholesale)

3 GLOSSARY

CSP	Critical Security Parameter
DES	Data encryption standard – FIPS 46
DPOC	Neopost’s Postage-On-Call® Server for Canada
DSA	Digital Signature Algorithm (Reference 3)
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
FIPS	Federal Information Processing Standard (USA)
G	DSA common parameter G
HMAC	keyed-Hashing for Message Authentication Code
I/O	Input / Output
MTBF	Mean time between failures
NSD	Neopost Secure Device
NVEM	Non Volatile Electronic Memory
P	DSA common parameter P
Q	DSA common parameter Q
RNG	Random number generator
SHA-1	Secure Hash Algorithm (Reference 7)
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 (1). The SMM shall meet the overall requirements for Level 3 security as defined in reference (2). The following table shows the security level requirement, as defined in reference (2), for each area of the SMM:

Security Requirements Section	Level
Cryptographic Module	3
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Machine	3
Physical Security	3
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

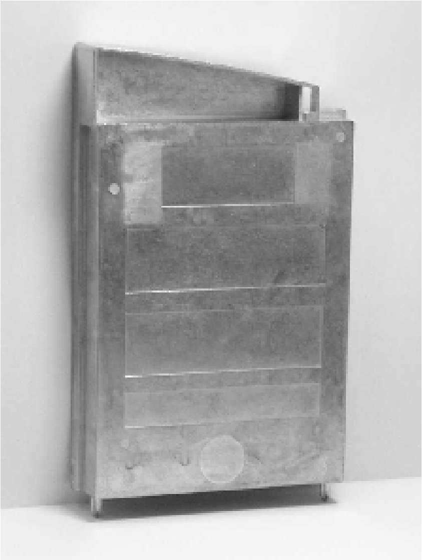

Figure 1

The SMM (figure 1) consists of a cryptographic sub function and postal services sub function sharing common hardware that is contained on a printed circuit board 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 critical security parameters 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 sub function. 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 PORT

The only port is a serial communication port NC06 communicating with the base, whose the main function is to control the transport motor, the display and the keyboard. No plaintext CSPs is transmitted through this port.

5.2 LIFECYCLE STATES

The SMM assumes one of three main overall states during its life cycle. These states are relevant to the accessibility of cryptographic services. The states are:

- **Pending Installation**
  The SMM contains the cryptographic parameters necessary to support interaction with the Neopost Postal Administration Infrastructure but has not yet been registered with this Enabled infrastructure.

- **Installed**
  The SMM is registered with the Neopost Postal Administration Infrastructure and will perform postal functions. It can go back to ‘Pending Installation’ state with a recycling operation.

- **Withdrawn**
  The SMM is registered from the Neopost Postal Administration Infrastructure and will not perform postal functions. It cannot go back to ‘Pending Installation’ state until it has undergone a factory initialisation, which will reconfigure the contents of the SMM system memory.

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

Where services have a state dependency then the SMM must be first placed into an appropriate life cycle state. The relationship between SMM services and state is summarised in Appendix 1.

The relationship between SMM services and authenticated entities are summarised in Appendix 2.

6.1 NEOPOST ADMINISTRATOR

The Neopost Administrator shall provide the services required to Initialise and 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. installation, 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. Registration 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 public key Certificate.

- Set the SMM state ‘Installed.

6.1.2. 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.

6.1.3. Withdrawal

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 ‘Withdrawn’ thereby inhibiting further access to the Administrator services and certain postal critical customer role services.

6.1.4. 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 Postal Service

This service requests 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 DSA Message authenticating signatures shall be 40-bytes 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)

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.

7.1.4 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 super-seeded by subsequent input values if required. The parameters for the Administrator and Program Support must be input after manufacture.

7.1.5 The SMM shall sign exported data with a DSA signature appended to the messages 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 The data encoded in the 2D barcode of the postage indicium is protected by ECDSA digital signature as described in reference (4).The ECDSA signature is generated in the protected area of the SMM.

7.1.9 The human readable data of the postage indicium is protected by the Security Code, a HMAC-SHA-1-30 message authentication code as described in reference (5) . The Security Code is generated in the protected area of the SMM.

7.2 CONDITIONAL SELF TEST RULES

7.2.1 If the key pair DSA is invalid then both the SMM DSA private key and DSA public key shall be erased (to zero) and the SMM shall inhibit. 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.

7.2.2 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 if its random number generator fails to a constant value.

7.2.3 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 if the test fails. (These tests are no longer actually required by NIST).

7.2.4 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. The validity of a key pair shall be determined by a pair wise consistency check, i.e. the encryption of a plaintext value and decryption of the ciphertext value. This check shall be performed at the generation of each new key pair and at power up.

7.3 POWER UP SELF TEST RULES

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

7.3.2 The SMM shall test the contents of it’s program memory area at power up by calculating the 32 bit checksum (sum of bytes) of the contents and comparing the result with a known answer. The SMM shall inhibit if the test fails.

7.3.3 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.

7.3.4 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 if the test fails.

Note that the PRNG will have two separate states, i.e. one for DSA signatures and one for key generation. The states only differ by the maintenance of separate generator seeds. Hence the test suffices for both states.

7.3.5 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 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.

7.3.6 The public key for each identity (administrator and program support) 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.

7.3.7 The SMM shall test the ECDSA algorithm at power up by performing a known answer test for both encryption of a plaintext value and decryption of the ciphertext value using predetermined data embedded into the SMM firmware.

7.3.8 The SMM shall test the HMAC algorithm at power up by performing a known answer test for both signing and verification using predetermined data embedded into the SMM firmware.

7.3.9 The SMM shall test the TDES algorithm at power up by performing a known answer test for both encryption of a plaintext value and comparison of the ciphertext value using predetermined data embedded into the SMM firmware.

7.4 CSP STORAGE

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

7.4.2 Any CSP access failure shall cause the SMM to inhibit. Exit from the inhibit condition shall require the SMM to re check access to, and the values of, all CSP.

7.5 TAMPER RESPONSE

7.5.1 The DSA private key, ECDSA private key, 3 HMAC secret keys, the random number generator seed, and the last random number, 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.

7.5.2 The DSA private key, ECDSA private key, 3 HMAC secret keys, the random number generator seed, and the last random number, 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.

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

7.6 STATUS INDICATION

7.6.1 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 Program Support/Neopost Administrator public key authorisation signature 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.

7.6.2 The following ‘module inhibited’ error conditions shall be indicated:

- DSA error (power-up self test and algorithm call detection)
- RNG error (power-up self test and algorithm call detection)
- Firmware / RAM error (permanent detection)
- High temperature detected error (permanent detection)
- ECDSA error (power-up self test and algorithm call detection)

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.

7.6.3 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.

7.7 OPERATORS/CUSTOMERS

7.7.1 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 PHYSICAL SECURITY

The C20ND/C21ND Secure Metering Module are both composed of a single electronic board enclosed in a unremovable metal cover.
The only way to get access to the electronic board (beside the single I/O connector) is by destroying the cover which would trigger a tamper detection switch.

8.1 TAMPER DETECTION

The triggering of a tamper detection switch will cut the power supply of the Crypto RAM which will erase this memory.
The software do not store the private keys in advance but read those again from the Crypto RAM each time it has to perform an operation.

9 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSP)

The following table describes each CSP maintained by the SMM:

CSP NAME	DESCRIPTION
SMM DSA private key	The SMM DSA private key used to authenticate messages and data output from the SMM.
SMM ECDSA private key	SMM ECDSA private key is used to authenticate the 2D barcode of postage indicium. (Reference 4).
SMM HMAC secret key 1	SMM HMAC secret key is used to generate a security code in order to protect human readable data of postal indicium (Reference 1 & 5).
SMM HMAC secret key 2	SMM HMAC secret key is used to generate a security code in order to protect human readable data of postal indicium. (Reference 1 & 5).
SMM HMAC secret key 3	SMM HMAC secret key is used to generate a security code in order to protect human readable data of postal indicium. (Reference 1 & 5).
HMAC Key ID	HMAC secret key current in use by SMM to authenticate the Human Readable data of the postage indicium.
PRNG – Vn parameter	Seed value used for Random Number Generator
PRNG – Ko parameter	Parameter used to generate the two TDES keys (for PRNG)

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 server.
Neopost Program Support DSA common P	Common cryptographic DSA parameter (P) associated with the Neopost Program Support services.
Neopost Program Support DSA common Q	Common cryptographic DSA parameter (Q) associated with the Neopost Program Support services.
Neopost Program Support DSA common G	Common cryptographic DSA parameter (G) associated with the Neopost Program Support services.
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 encoded in 2D Barcode.

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 ▸ **CSP Name ▾**	**Registration**	**Postal Administration**	**Withdrawal**	**Postal Indicium**	**Postal Administration Request**	**General Postal**	**Self Test**
SMM DSA private key	r	r	r		r		r
SMM ECDSA private key		r		r			r
SMM HMAC secret key 1				r			r
SMM HMAC secret key 2				r			r
SMM HMAC secret key 3				r			r
HMAC Key ID		w			w		
PRNG – Ko parameter							r
PRNG – Vn parameter	m	m	m	m	m		r

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

Service Name ▸ Public Key Parameter Name ▾	Registration	Postal Administration	Withdrawal	Postal Indicium	Postal Administration Request	General 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							
Neopost Program Support DSA common P							
Neopost Program Support DSA common Q							
Neopost Program Support DSA common G							
SMM ECDSA public key							r

10 APPENDIX 1

The following table summarises the legality of services according to the prevailing lifecycle state of an SMM:

SMM STATE ▸ Service ▾	PENDING INSTALLATION	INSTALLED	WITHDRAWN
Registration	✓		
Postal Administration		✓	
Withdrawal		✓	
Postal Indicium		✓	
Administration Request		✓	
General Postal	✓	✓	✓
Self Test	✓	✓	✓

A service is not permitted for a particular state unless indicated:
✓ = permitted

11 APPENDIX 2

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

OPERATOR ▸ SERVICE ▾	ADMINISTRATOR	CUSTOMER
Registration	✓	
Postal Administration	✓	
withdrawal	✓	
Postal Indicium		✓
Administration Request		✓
General Postal		✓
Self Test	✓	✓

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

12 APPENDIX 3

The following table summarises the relationship between roles and required identification and authentication

ROLE	TYPE OF AUTHENTICATION	AUTHENTICATION DATA
Crypto Officer	DSA	DPOC Server transactions
User	DSA	DPOC Server transactions
	ECDSA	2D barcode postage indicium data
	HMAC	Human readable postage indicium data

13 APPENDIX 4

The following table summarises the services authorised for each role.

ROLE	AUTHORIZED SERVICES
Crypto Officer	Registration
	Postal Administration Service
	Withdrawal
	Self Test
User	Postal Indicium Service
	Postal Administration Request Service
	General Postal Service

14 APPENDIX 5

The following table summarises the access rights within services.

SERVICE	CRYPTOGRAPHIC KEYS AND CSPs	TYPES OF ACCSESS
Registration	SMM DSA private key	r
	Neopost Administration DSA public key	r
	Neopost Administration DSA common P, Q, G	r
Postal Administration	SMM DSA private key	r
	Neopost Administration DSA public key	r
	Neopost Administration DSA common P, Q, G	r
Withdrawal	SMM DSA private key	r
	Neopost Administration DSA public key	r
	Neopost Administration DSA common P, Q, G	r
Self Test	SMM DSA private key SMM DSA public key SMM ECDSA private key SMM ECDSA public key	r r r r
	Neopost Administration DSA public key	r
	Neopost Administration DSA common P, Q, G	r
Postal Indicium	SMM ECDSA private key	r
	SMM HMAC secret key	r
Postal Administration Request	SMM DSA private key	r
	Neopost Administration DSA public key	r
	Neopost Administration DSA common P, Q, G	r
General Postal	N/A	N/A

15 APPENDIX 6

The following table summarises the strength of authentication mechanisms

AUTHENTICATION MECHANISM	STRENGTH OF MECHANISM
Digital signature	80 security bits or a probability de random success of 1 in 2^80
Message Authentication Code (HMAC-SHA-1)	80 security bits or a probability of random success of 1 in 2^80