neopost

N90i SECURITY POLICY

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

THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED ONLY
IN ITS ENTIRETY WITHOUT REVISION

Issue D - 25.03.2002

TITLE :   N90i SECURITY POLICY

ABSTRACT:

DATE	ISSUE	AMENDMENT DESCRIPTION
12.09.2001	A	First Issue
22.02.2002	B	Maintenance role renamed to Program Support role. Clarified definition of Program Support role in section 4.2. Included signature check in program down load rule (section 5.3.4).
22.03.2002	C	N90I references added.
25.03.2002	D	Correction made - N90I to N90i.

Originator: Date:

Authorised By: GARY STEWARD   Date: 25.03.2002

**THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED ONLY
IN ITS ENTIRETY WITHOUT REVISION**

CIRCULATION LIST

ORIGINATOR'S MANAGER

ORIGINATOR

CONTENTS

N90 i SECURITY POLICY

1.   **INTRODUCTION**

The N90i Secure Metering Module (SMM) is a unit embedded within the Neopost IJ35 (IJ45) 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   REFERENCES

1.2.1   Information Based Indicia Program (IBIP), Performance Criteria for Information Based Indicia and Security Architecture for IBI Postage Metering Systems (PCIBISAIBIPMS), The United States Postal Service (USPS), Draft August 19, 1998 (document number unknown).

1.2.2   Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-1

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

1.2.4   Secure Hash Standard, Federal Information Processing Standards Publication 180-1

Issue D – 25.03.2002

1.3 GLOSSARY OF NAMES AND ACRONYMS

DSA	Digital Signature Algorithm (Reference 3)
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
SHA-1	Secure Hash Algorithm (reference)
SMM	Secure Metering Module
SRDI	Security Related Data Item
USPS	United States Postal Service (reference 1)
X	DSA private key
Y	DSA public key

2. SECURITY LEVEL

The SMM is a multiple chip, embedded, cryptographic module as defined in reference (2). 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: -

	Level
Cryptographic Module	3
Module Interfaces	3
Roles & Services	3
Finite State Machine	3
Physical Security	3
Software Security	3
Operating System Security	N/A
Key Management	3
Cryptographic Algorithms	3
EMI/EMC	3
Self Tests	4

NA = not applicable

3. SMM OVERVIEW

The SMM 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 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 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 physic al boundary. This latter data relates to the general control and use of the franking machine in which the SMM is embedded.

3.1 I/O PORTS

A number of data channels extend outside the enclosure via specific pins on a single multi pin connector. Each of these pin groups has a predefined use (appendix 3) and are henceforth regarded as a port. The ports 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 typical use externally to the SMM: -

3.1.1 Weigh Platform 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 it is the only connection that will support a weigh platform. The port will also however support connection to either a PC or stand alone scale via an RS232 link.

3.1.2 Printer 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 it is the only connection that will support a printer. The port will also however support connection to either a PC or stand alone scale via an RS232 link.

3.1.3 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.

3.1.4 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.

3.1.5 Print Mechanism Control Port

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

3.1.6 Print Mechanism Status Port

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

3.1.7 Power Supply Port

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

3.2 LIFE CYCLE STATES

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

Not Commissioned
- This is the default at manufacture. The SMM does not contain the cryptographic parameters necessary to support interaction with the Neopost Postal Administration Infrastructure. A factory initialisation is required.

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

Customer Enabled
- The SMM is registered with the Neopost Postal Administration Infrastructure and will perform postal functions.

Customer disabled
- The SMM is de registered from the Neopost Postal Administration Infrastructure and will not perform postal functions. It cannot be re commissioned until it has undergone a factory initialisation, which will reconfigure the contents of the SMM system memory.

4. ROLES AND SERVICES

The SMM shall support three distinct operators. The SMM shall enforce separation of entities using identity-based authentication and by restricting the services available to each entity. Also some services are state dependent. The allowable operators are the Neopost Program Support, 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 Program support and 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.

4.1 NEOPOST ADMINISTRATOR

The Neopost Administrator shall provide the services required to commission 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 Administration services are:-

4.1.1 Commission Service

This service will carry out the following: -

- Input a non-authenticated message containing a Neopost X509 certificate which will include the public key (Y) and DSA common parameters (PQG) corresponding to the Administrator.

- Verify that the SMM is in the appropriate state for acceptance of a 'Commission' service request (Appendix 1).

- Extract and store the PQGY values.

- Generate and store a new SMM public (Y) key based upon the newly input PQG and the SMM private key.

- Authenticate and output a message containing the SMM public key (Y).

- Set the SMM state to 'Commissioned' so as to enable the Administrator.

4.1.2   Zeroise 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 'Commission' service request (Appendix 1).

- Zero the private key SRDI.

4.1.3   Customer Enable Service

This service will: -

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

- Verify the authentication.

- Verify that the SMM is in the appropriate state for acceptance of a 'Customer Enable' service request.

- Extract and store the postal data items.

- Extract and store the X509 SMM public key Certificate.

- Set the SMM state 'Customer Enabled'.

4.1.4   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.

4.1.5 Customer Disable Service

This service will: -

- Input an authenticated message requesting that the SMM set itself to the 'Customer Disabled' state.

- Verify the authentication.

- Verify that the SMM is in the appropriate state for acceptance of a 'Customer Disable' 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.

4.2   NEOPOST PROGRAM SUPPORT

Neopost Program Support shall provide the services required to input new or replacement program files into the SMM.

The Neopost Program Support services are:-

4.2.1 Program Download Service

This service will: -

- Input an authenticated message containing a sub section of executable program code (several messages may be required in order to assemble a complete program).

- Verify the authentication.

- Assemble the program code as a replacement (when complete) for the original program.

4.2   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: -

4.3.1   Postal Indicium Service

- This service requests printing of a postal indicium.

4.3.2   Postal Administration Request Service

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

4.3.3   General Postal Service

This service requests status output.

5.   SECURITY RULES

Rule statements are shown in Italics. Other information is included for background purposes only.

5.1   AUTHENTICATION RULES

5.1.1 The SMM shall provide three distinct operators, the Neopost Program Support, Neopost Administrator and the Customer.

5.1.2 The SMM shall provide identity-based authentication.

5.1.3 Signatures shall be 40 byte 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)

5.1.4 The cryptographic parameters (PQGY) 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.

5.1.5 The SMM shall authenticate exported data with 40 byte 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)

5.2 KEY GENERATION

5.2.1 The SMM DSA Private key shall be generated according section 3.1 and 3.3 of reference (3).

5.2.2 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.

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

5.3 CONDITIONAL SELF TEST RULES

5.3.1 The SMM shall default to the 'Not Commissioned' state if it does not possess a valid private/public key pair. 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.

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

5.3.3 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 if the test fails

.

5.3.4 The SMM shall validate the integrity of any program file being down loaded by authenticating the attached DSA signatures of all program segments received. The SMM shall not store any program segment that has an invalid authentication. The SMM shall further test the contents of the overall down loaded program file by calculating the 16 bit checksum (sum of bytes) of the contents and comparing the result with a known answer. The SMM shall refuse to execute such a program if the test fails.

5.4 POWER UP SELF TEST RULES

5.4. 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.

5.4.2 The SMM shall test the contents of it's 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 if the test fails.

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

5.4.4 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. Testing of the secure hash algorithm (SHA-1) shall be inclusive within the DSA test. The SMM shall inhibit if the test fails.

5.4.5 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 if the test fails.

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

5.5 SRDI STORAGE

5.5.1 The SMM shall detect data corruption of the value held for any particular SRDI by the incorporation of error detection data. The probability of failing to detect an invalid SRDI by this method shall be less than 1:50000.

The specified probability is also to be judged in the context that even if a data error was not detected then the resultant erroneous SRDI value should still be identified as erroneous via the self tests (see Continuous and Power Up Self Test sections). For example an erroneous public key would cause the pair wise consistency check to fail.

5.5.2 The SMM shall establish the validity of any SRDI before updating it with a new value. If erroneous the SMM shall abort the service process that caused the update to be required.
A failure may be component failure.

5.5.3 Any 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 SRDI.

5.6 TAMPER RESPONSE

5.6.1 The DSA private key shall be erased should the SMM covers be removed. At the same time the SMM shall enter an inhibited state.

5.6.2 The DSA private key shall be erased if the temperature inside the SMM covers exceeds 77 degrees Centigrade. At the same time the SMM shall enter an inhibited state.

5.6.3 The private key shall not be exported under any circumstances.

5.7 SOFTWARE

5.7.1 The source for software contained in the firmware of the SMM shall be written in C high level language. Exceptions to this shall be the use of assembler level code to implement the following time critical functions: -

-The multiply and modulus mathematical functions associated with the DSA algorithm (reference 3).

5.8 STATUS INDICATION

5.8.1 The following 'module not ready' module states shall be indicated: -

- Private key zeroed

- Private/Public key pair invalid (module not initialised)

- Tamper mechanism tampered

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.

5.8.2 The following 'module inhibited' error conditions shall be indicated: -

- DSA error

- RNG error

- SRDI access/data error

- Firmware / ram 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.

5.8.3 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.

6. DEFINITION OF SECURITY RELATED DATA ITEMS (SRDI)

The following table describes each SRDI maintained by the SMM: -

SRDI NAME	DESCRIPTION
DSA random number seed	Current status of random number
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.
Neopost Program Support services transaction code	Neopost Program Support service transaction identifier code. This is included in every input Program Support service message and is incremented after each Program Support service function so that each Program Support input message cannot be re used.
SMM DSA private key	The SMM private DSA key used to authenticate messages and data output from the SMM.
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 life cycle state	Indicates the SMM life cycle state: -
	  Not Commissioned
	  Commissioned
	  Customer Enabled
	  Customer Disabled

7. DEFINITION OF SRDI MODES OF ACCESS

The section describes how SRDI 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(s) summarises the relationship between all SRDI maintained by the SMM and the services that access them: -

SRDI Name ▼ / Service Name ▸	Commission	Zeroise Private Key	Customer Enable	Postal Admin	Customer Disable	Program Download	Postal Indicium	Admin Request	General Postal	Self Test
DSA random number seed	s						m	m		m
Neopost Administration DSA public key	w		r	r	r					
Neopost Administration DSA common P	w		r	r	r		r	r		r
Neopost Administration DSA common Q	w		r	r	r		r	r		r
Neopost Administration DSA common G	w		r	r	r		r	r		r
Neopost Program Support DSA public key						r				
Neopost Program Support DSA common P						r				
Neopost Program Support DSA common Q						r				
Neopost Program Support DSA common G						r				
Neopost Program Support services transaction code						e m				
SMM DSA private key	s	z					r	r		r
SMM DSA public key	s									r
SMM life cycle state	m		m	r	m		r	r		

APPENDIX 1

The following table summarises the legality of services according to the prevailing life cycle state of an SMM: -

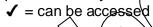| SERVICE ▼	NOT COMMISSIONED	COMMISSIONED	CUSTOMER ENABLED	CUSTOMER DISABLED
Zeroise	✓			✓
Commission	✓			
Customer Enable		✓		
Postal Admin			✓	
Customer Disable			✓	
Program down load	✓	✓	✓	✓
Postal Indicium			✓	
Admin Request			✓	✓
General Postal	✓	✓	✓	✓

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

APPENDIX 2

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

OPERATOR ➤ SERVICE ▾	ADMINISTRATOR	PROGRAM SUPPORT	CUSTOMER
Zeroise Private Key	✓		
Commission	✓		
Customer Enable	✓		
Postal Admin	✓		
Customer Disable	✓		
Program down load		✓	
Postal Indicium			✓
Admin Request			✓
General Postal			✓

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

APPENDIX 3

The following table summarises the SMM ports on which services are permitted to be active. These ports are each a specific group of pins on the single multi pin connector provided for data access to the SMM: -

PORT ▸ SERVICE ▾	WEIGH PLATFORM PORT	PRINTER PORT	MODEM PORT	UI PORT	PRINT MECHANISM CONTROL PORT	PRINT MECHANISM STATUS PORT
Zeroise	✔	✔	✔			
Commission	✔	✔	✔			
Customer Enable	✔	✔	✔			
Postal Admin	✔	✔	✔			
Customer Disable	✔	✔	✔			
Program Down load	✔	✔	✔			
Postal Indicium					✔	
Admin Request	✔	✔	✔			
General Postal				✔		

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

WJH / RT 25.03.2002

Issue D – 25.03.2002