PROMAIL II (SIMPLY POSTAGE III)
SECURITY POLICY

Compiled By: W. HERRING
PRINCIPAL ELECTRONICS DESIGN ENGINEER

Issue D – 06.28.2001

TITLE: PROmail II SECURITY POLICY

ABSTRACT:

DATE	ISSUE	AMENDMENT DESCRIPTION
19.09.2000	A	First Issue
26.09.2000	B	Security level for 'Self Tests' (section 2) reduced from 4 to 3. Rules in Section 5 modified to reflect the existence and maintenance of 2 random number generators – one for signatures and one for private keys manufacture.
14.12.2000	C	Updated as indicated. Copyright statement changed on Infogard copy only.
28.06.2001	D	Updated to reflect changes for PROmail II.

Originator: Date:

Authorised By: Date:

CIRCULATION LIST

G. STEWARD

ORIGINATOR

CONTENTS

PROMAIL II SECURITY POLICY

1. INTRODUCTION

The PROmail II Secure Metering Module (SMM) is a unit embedded within the Neopost PROmail II postal device. Integrated within the SMM are a cryptographic processor, a real time clock, non-volatile memory, working memory, and other components.

The postal services relate to the ultimate objective of the SMM, which is to store postage funds belonging to a customer until they are needed by the indicium dispensing system. 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 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

1.3 GLOSSARY OF NAMES AND ACRONYMS

SMM	Secure Metering Module
SRDI	Security Related Data Item
NVEM	Non Volatile Electronic Memory
DSA	Digital Signature Algorithm (Reference 3)
SHA-1	Secure Hash Algorithm (reference)
X	DSA private key
Y	DSA public key
P	DSA common parameter P
Q	DSA common parameter Q
G	DSA common parameter G
I/O	Input / Output
USPS	United States Postal Service (reference 1)

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 **Roles & Services**	3 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	3

NA = not applicable

3. SMM OVERVIEW

The SMM consists of a processor cryptographic processor, a real time clock, non-volatile memory, working memory, and other components that are contained on a printed circuit board and enclosed within a tamper responsive enclosure. This enclosure constitutes the cryptographic 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 module and also non-authenticated data that has no security implications and can pass freely across the cryptographic physical boundary. The latter relates to non (cryptographic) security critical postal functions. These functions are those required by the USPS as specified in reference (1) and are postal critical.

3.1 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:

3.1.1 RS232 Port

This is a serial communication port. Secure services within the SMM can be activated by certain data sequences being applied by a remote host computer such as a PC. An auxiliary device such as a postal weigh scale can also be connected to this port.

3.1.2 USB port

This is a serial communication port. Secure services within the SMM can be activated by certain data sequences being applied by a remote host computer such as a PC.

3.1.3 Scale Interface Port

This is an analog interface port used to measure the output of the scale load cell.

3.1.4 Print Mechanism Control Port

This is a data channel used only to apply controlling data to various parts of the print mechanism in order to effect a sequence whereby an indicia is printed onto a thermal label media. These parts would include a stepper motor, a Thermal Print head, Paper detection sensors, and a print head open switch.

A Neopost Online PC can securely activate services within the SMM by communication over either the RS232 or USBports.

Finally the customer can activate certain secure services such as Postage Resetting within the SMM, that relate to the intended function of a postage dispenser, by performing actions directly on the connected PC using the PROmail Client application (user interface)

The port data channels are shared by secure and non-secure procedures. The non-secure data activity is summarised in Appendix 1.

3.1.5 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 several main overall states during its life cycle. These states are relevant to the accessibility of cryptographic services. The states are: -

Uninitialised

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

Initialised

- 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.

Unfunded & Time_out Unfunded

- The SMM has been authorized and is capable of performing postal functions, although cannot issue indicia. The SMM must be funded before it can issue non-zero value indicia. The SMM will transition to the Time_out Unfunded state if an audit transaction is not performed before the watchdog timer expires.

Funded & Time_out Funded

- The SMM has been authorized and funded and will perform postal functions including issuing indicia. The SMM will transition to the Time_out Funded state if an audit transaction is not performed before the watchdog timer expires.

Faulted

- The SMM has detected a security threat and will no longer provide any services that could affect its SRDIs.

4. ROLES AND SERVICES

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 each entity. Also some services are state dependent. The allowable operators are the Neopost Administrator (or Crypto-officer) and the Customer (User): -

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.

Where services have a state dependency then the SMM must be first placed into an appropriate life cycle state. The entities are authenticated with respect to state as shown in Appendix 1.

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

The relationship between SMM services and state is summarised in Appendix 3.

4.1 NEOPOST ADMINISTRATOR

The Neopost Administrator shall provide the services required to commission and maintain the cryptographic parameters within the SMM. These parameters 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. These shall require the identity of the operator to be provided and authenticated.

The Neopost Administration services are:-

4.1.1 Initialisation 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 Tamper Arm Service

This service will carry out the following: -

- Tests tamper detection circuitry.

- If the tamper detection line goes high, zeroizes the memory and sends out a tamper switch open detection message to the test utility software.

- This provides the temporary tamper detection till the valid private key is stored in the meter after the meter becomes "Live" in factory. (The private key is regenerated after the mete r becomes "Live").

4.1.3 Zeroise 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 3).

- Zero the private key SRDI.

4.1.4 Authorize 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’ thereby inhibiting further access to the Manufacturing role services, but enabling subsequent access to the remaining Administrator services and certain postal critical Customer services.

4.1.5 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.

4.1.6 Withdraw 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 CUSTOMER

These services are available to the Customer. They all require the SMM to be in an appropriate state. The services are: -

4.2.1 Postal Indicium Service

- This service requests printing of a postal indicium.

4.2.2 Postal Administration Request Service

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

4.2.3 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 two distinct operators, the 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 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 'Uninitialised' 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 both the private key and signature random number generators, the SMM shall perform the continuous random number generator test for as defined by reference (2). The SMM shall inhibit all data output if the test fails.

For the signature random number generator, this will be whenever the module is asked to initialise itself (i.e. at power up or error reset). For the private key random number generator, this will be when the module is requested to generate a private key.

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.

5.5 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.

<u>5.6 TAMPER RESPONSE</u>

5.6.1 The SMM shall be a multi-chip embedded module and shall be enclosed within a non-removable metal enclosure. The SMM shall also contain micro-switches as part of its tamper-response (zeroization) circuitry.

5.6.2 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 frmware 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 Factory DSA public key	Public key used for the verification of authenticated messages input from the Neopost Factory server.
Neopost Factory DSA common P	Common cryptographic DSA parameter (P) associated with the Neopost Factory services.
Neopost Factory DSA common Q	Common cryptographic DSA parameter (Q) associated with the Neopost Factory services.
Neopost Factory DSA common G	Common cryptographic DSA parameter (G) associated with the Neopost Factory services.
Neopost Factory services transaction code	Neopost factory service transaction identifier code. This is included in every input factory service message and is incremented after each factory service function so that each factory 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.

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: -

Service Name ▸ SRDI Name ▾	Tamper Arm	Initialize	Zeroise Private Key	Auhtorize	Postal Admin	Withdraw	Postal Indicium	Admin Request	General Postal	Tamper	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 Factory DSA public key											
Neopost Factory DSA common P Neopost Factory DSA common Q											
Neopost Factory DSA common G											
Neopost Factory services transaction code											
SMM DSA private key	I	s	z				r	r		z	r
SMM DSA public key		s									r
SMM life cycle state		m		m	r	m	r	r			

APPENDIX 1

The following table summarises the services permitted by each of the SMM life cycle states: -

STATE ▸ ENTITY▾		UnInitialised	Initialised	Unfunded/ Funded	Withdrawn
Neopost Administrator	Administration Services	v	v	v	v
	Customer Services			v	

The service is not permitted unless specifically indicated: -
v = permitted

APPENDIX 2

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

ENTITY ▸	NEOPOST ADMINISTRATOR	
SERVICE ▾	ADMINISTRATION SERVICES	CUSTOMER SERVICES
Tamper Arm	v	
Zeroise Private Key	v	
Initialize	v	
Authorize	v	
Postal Admin	v	
Withdraw	v	
Postal Indicium		v
Admin Request		v
General Postal		v

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

APPENDIX 3

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

LIFE CYCLE STATE ▸ SERVICE ▾	UNINITIALISED	INITIALISED	UNFUNDED/FUNDED	WITHDRAWN
Tamper Arm	v			
Zeroise	v			v
Initialize	v			
Autorize		v		
Postal Admin			v	
Withdraw			v	
Postal Indicium			v	
Admin Request			v	
General Postal	v	v	v	v

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

APPENDIX 4

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

PORT ▸ SERVICE ▾	RS232 PORT	USB PORT	BUTTON/ LEDS PORT	PRINT MOTOR DRIVE	PRINT SENSORS (PAPER OUT/HEAD OPEN)
Tamper Arm	v	v			
Zeroise	v	v			
Withdraw	v	v			
Authorize	v	v			
Postal Admin	v	v			
Withdraw	v	v			
Postal Indicium Admin Request	v	v		v	
General Postal	v	v	v		

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

EM
27.06.2001