Neopost Online Secure Metering Device
SMD or SMDII Security Policy

Neopost Online Inc.

3400 Bridge Parkway, Ste. 201
Redwood City, CA 94065

Last Revised: 10/18/00

Change History

Date	Who	Description
10/25/99	ALP	Initial Draft
12/2/1999	EAS	Remove redundancies and inconsistencies
12/6/99	ALP	Organized roles & services, added key management
2/17/2000	EAS	Revised and removed unnecessary information
3/22/2000	ALP	Minor working revisions throughout document
10/18/2000	EDM	Minor changes for submission

Prepared for Neopost Online By:

Pion & Simon Electronics

and

Atlan
LABORATORIES

1. INTRODUCTION 4

1.1. Scope 4

1.2. Reference Documents 4

1.3. Glossary of Names and Acronyms 4

2. OVERALL SECURITY REQUIREMENTS 6

3. PHYSICAL CONSTRUCTION AND SECURITY 7

3.1. Cryptographic Boundary 7

3.2. Tamper Evident Enclosure 8

3.3. Tamper Detection Mechanism 8

3.3.1. Security Threat Detection 8

4. ROLES 9

4.1. Site Security Officer (SSO) Role 9

4.2. User Role 9

4.3. Role Based Authentication 9

5. SERVICES 10

5.1. Initialization Transaction 10

5.2. Authorization Transaction 10

5.3. Funding Transaction 11

5.4. Indicium Transaction 11

5.5. Audit Transaction 12

5.6. Withdrawal Transaction 12

5.7. Self Tests 13

5.8. Get X.509 Certificate Transaction 13

5.9. Enable, Disable, and Configure Auxiliary Serial Port 13

5.10. Check or Change PIN 13

5.11. Set, Read, or Change RTC 13

5.12. Get or Send Aux Port Data 14

5.13. Get Status or User Information 14

6. KEY MANAGEMENT 15

6.1. Neopost Online public key 15

6.2. Controlling Authority public key....15

6.3. SMD public/private key pair....15

6.4. SSO and User PINs 15

7. ROLES VS. SERVICES MATRIX 16

1. Introduction

The Secure Metering Device, here after referred to as simply the SMD or SMD II, is an electronic device developed by Neopost Online that stores revenue and dispenses it to a host computer, such as a PC compatible, under control and direction of a Neopost Online customer (herein called the “user”). The SMD attaches to and communicates with the host computer via a serial interface. The revenue is dispensed from the SMD to the host computer in the form of a digitally signed indicium, a unique bit pattern that can be determined to have originated from a particular SMD at a particular point in time.

Each time the SMD dispenses an indicium it deducts the revenue amount contained in the indicium from a set of secure internal registers. These registers represent the user’s stored revenue. When the revenue in the registers is depleted the user may initiate a transaction between the SMD and a remote Neopost Online server to obtain more revenue. The Neopost Online server deducts the amount of revenue credited to the SMD from the user’s account at Neopost Online and sends the user a periodic bill.

The SMD is expected to see application immediately as a postage-dispensing unit (loosely termed “meter” for historic reasons). In this application, the indicium dispensed by the SMD will be formatted into a 2D bar code by a PC compatible computer and printed on an adhesive backed label or directly on the user’s envelope. An agreement between Neopost Online and the USPS will allow such printed indicia to legally pass as bonafide postage. Other potential applications are possible and are currently being considered.

1.1. Scope

This document sets forth a precise specification of the security rules under which the SMD’s cryptographic module must operate, including rules derived from FIPS140-1 (reference [2]) as well as the additional security rules imposed by Neopost Online, Inc.

1.2. Reference Documents

The following documents provide additional information and are referred to in the body of this text:

[1] Schematic Diagram, Neopost Online SMD.

[2] Security Requirements for Cryptographic Modules, FIPS Publication 140-1.

[3] Digital Signature Standard, FIPS Publication 186-2

1.3. Glossary of Names and Acronyms

Digital Signature: A bit pattern appended to a digital message that uniquely identifies the message as having originated from a particular individual or device. A digital signature is generated using a private key known only to the signer of the message. The resulting signature is unique in that signing exactly the same message twice will result in two different signatures. A signature may be verified by the recipient of the message using the signer’s public key. If the signature verifies, it validates the message as having been originated by the signer.

DSA: Digital Signature Algorithm: The algorithm used to generate public/private key pairs, and to sign and verify digital signatures in the SMD.

DSS: Digital Signature Standard: The federal cryptographic standard that defines the algorithms used by the SMD to generate public/private key pairs, and to generate and verify digital signatures.

Host: A computer system which communicates with the SMD over the SMD's host serial port.

Message: A group of data bytes sent from either the SMD to the host or from the host to the SMD. Messages are sent between the host and SMD in pairs. First, the host sends the SMD a request message, and the SMD responds with a response message. Each such pair is referred to as a request/response message pair.

PCB: Printed circuit board.

POC: Postage on Call: A name trademarked by Neopost Online for the funding service used with the SMD.

Private Key: A DSS key which is used to generate a digital signature for a message. This key is kept secret by its owner to prevent an unauthorized person or device from signing a message with the signature of the key's owner.

Public Key: A DSS key which may be used to verify the digital signature of a message. This key is made public by the owner to allow other people or devices to verify the signature of a message originated by the key's owner.

Request Message: A message sent from the host to the SMD requesting that a service be performed.

Response Message: A message sent from the SMD to the host, informing the host of the status of the performance of the service requested by the last request message.

Role: A security related position relative to the SMD occupied by a person or entity requesting services from the SMD.

RTC: Real-Time Clock: The RTC is a clock contained in the SMD that keeps track of the current date and time. It is used to provide time stamps for messages and as a watchdog timer to force periodic Audit transactions.

Service: An operation perfomed by the SMD on behalf of a person or entity operating in a particular role.

SMD: Secure Meter Device: A product designed by Neopost Online, Inc. which meters revenue on a per-use basis to a host device such as a personal computer.

SRDI: Security Relevant Data Item: A data item stored in the SMD and possibly readable and/or writtable by an external device.

SSO: Site Security Officer: A person or device designated by Neopost Online to initialize the SMD. The SSO is one of the two roles supported by the SMD. The other is the User role.

Transaction: A series of one or more request/response message pairs comprising the performance of a single service.

User: A user of the SMD, usually Neopost Online or a Neopost Online customer. One of the two roles supported by the SMD. The other is the Site Security Officer role, or SSO.

2. Overall Security Requirements

The SMD is a Multiple-Chip Standalone Cryptographic Module as defined in reference [2], Security Requirements for Cryptographic Modules, FIPS publication 140-1.

The SMD uses Digital Signature Standard (DSS) public key cryptography to enforce security. The DSS standard is described in reference document [3].

The SMD is intended to meet the overall requirements for FIPS-140 Level 2 security as well as level 3 physical security requirements with EFP/EFT, as defined in reference document [2].

The following table shows the security level requirement for each component of the SMD:

Security Requirements Section	**FIPS-140 Security Level**
Cryptographic Module	2
Module Interfaces	2
Roles & Services	2
Finite State Machines	2
Physical Security	3
EFP/EFT	4
Software Security	2
Operating System Security	N/A
Key Management	2
Cryptographic Algorithms	2
EMI/EMC	3
Self Tests	2

3. Physical Construction and Security

This section describes the physical construction of the SMD and the mechanical and electronic security provisions of the device.

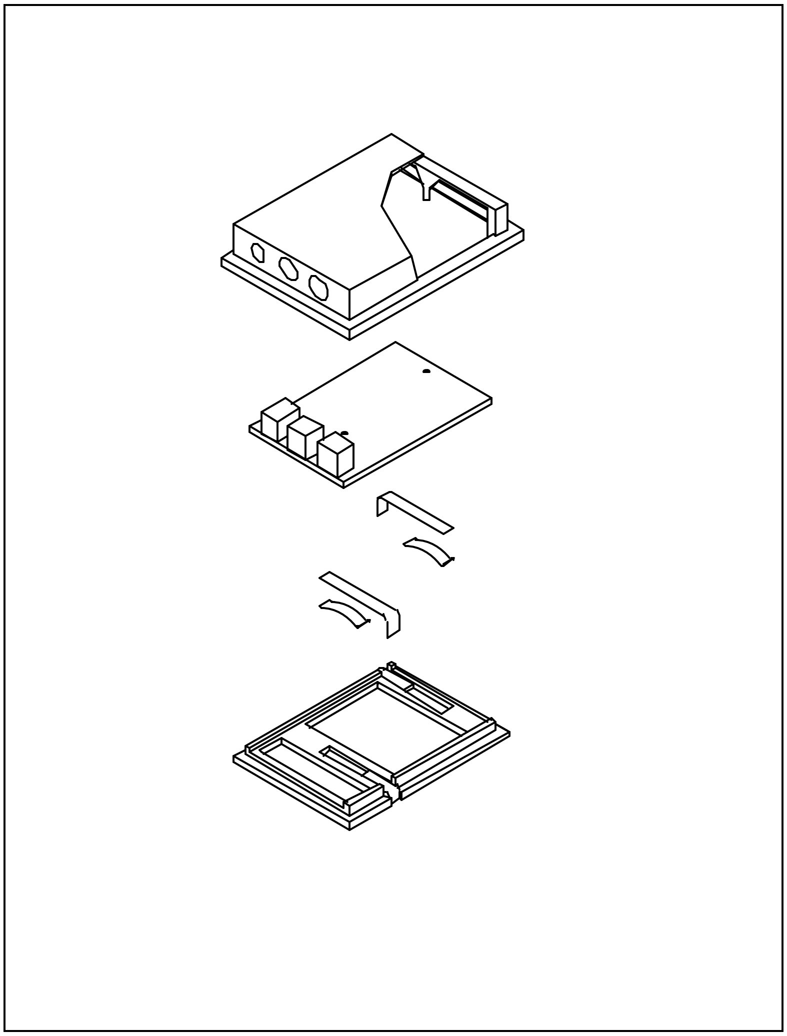

Figure 1

The SMD consists of the following elements:

- A tamper evident metallic case comprising the Cryptographic Boundary
- A tamper detection mechanism and auxiliary power supply
- A communications processor, memory, and real-time clock
- A cryptographic engine and it's secure memory
- Serial ports and power supply conditioning circuitry.

3.1. Cryptographic Boundary

The SMD contains a single printed circuit board (PCB), to which all of the SMD's electronic components are attached. The PCB is housed in a tamper evident enclosure. The SMD's cryptographic boundary for the purposes of FIPS 140-1 certification is the tamper evident enclosure that surrounds the SMD printed circuit board. Interfaces are accessible from openings in the enclosure to facilitate serial communication and power supply.

The power connector accepts 9 to 12 volts DC and is protected against overvoltage and reverse voltage. One of the serial connectors accepts RS-232 level secure communications with a host computer while the other acts in a "pass-through" mode to replace the serial port on the host.

3.2. Tamper Evident Enclosure

The enclosure of the SMD is a metallic case that is sealed by ultrasonic welded plastic at all joints. This case is designed such that it cannot be opened without destroying the module and leaving tamper evidence. The enclosure is sealed by the Site Security Officer (SSO) at the Neopost Online factory after initial factory testing.

3.3. Tamper Detection Mechanism

The SMD contains a tamper detection circuit, together with software in the communications and cryptographic processors, which is activated by a tamper switch inside the enclosure if an attempt is made to open the enclosure after it has been sealed. When such an attempt is made, the switch contacts close causing the SMD to erase its private key and all passwords. Since the private key is necessary to sign the messages sent between the SMD and the host during secure transaction processing, the SMD will no longer be able to operate as a revenue dispensing mechanism once the key is cleared. The tamper detection circuit causes the private key to be zeroized after the enclosure is opened, having previously been sealed by the SSO at the Neopost Online factory.

The tamper detection circuit operates even when the main power supply is switched off or disconnected from the SMD's power connector. This power is supplied by batteries that are attached to the SMD's PCB and are enclosed inside the cryptographic boundary.

3.3.1. Security Threat Detection

The SMD contains several security threat detection mechanisms, including the tamper detection mechanism and periodic software checks. If any of these mechanisms detect that someone is tampering with the SMD's security, the SMD transitions to the Faulted state. The SMD can transition to the Faulted state from any state except Uninitialized. Once faulted, the SMD may not be returned to normal operation via any communication over the host or auxiliary serial I/O port, will not issue indicia, and will not accept any other secure transaction request.

4. Roles

The SMD supports the following roles:

- Site Security Officer Role
- User Role

The SMD enforces the separation of roles by restricting the services available to each role. Members of each role must log on using separate Personal Identification Numbers (PIN).

4.1. Site Security Officer (SSO) Role

The SSO is responsible for sealing the SMD's enclosure at the Neopost Online factory and for personalizing and initializing the SMD. The services available in the SSO role are shown in table in section 7.

4.2. User Role

The end user operates the SMD under license from Neopost Online, Inc. in the User role. The end user usually operates the SMD to obtain funding, indicium and audit services. Neopost Online representatives may also operate the SMD from the user role to perform various operations including authorization, withdrawal, and testing. The services available in the User role are shown in table in section 7.

4.3. Role Based Authentication

The SMD uses role-based authentication, which satisfies the FIPS 140-1 level 2 authentication requirements. There are separate 12 byte PINs for SSO and User role.

The SSO and User PINs consist of a constant initial value known to the SSO (called the "initial PIN value"), immediately after the SMD is manufactured. The SSO must log in using the initial PIN value and immediately change the SSO and User PINs to new unique values.

The SSO enters its PIN by issuing a CHECK PIN message to the SMD. The SMD responds by checking the PIN and if valid will unlock the SSO services. The SSO PIN must be presented correctly before the SMD will allow access to the SSO services. Once the PIN is provided, the SMD will continue to allow SSO services until either another PIN is presented or the SMD's power is turned off.

Similarly, the User PIN must be presented correctly before the SMD will allow access to User services.

The SMD's Check PIN function allows no more than 3 consecutive failures to verify a PIN. After 3 consecutive failures the PIN is blocked and can no longer be verified. The SSO PIN cannot be unblocked, but the User PIN can be changed using the Change PIN function while in the SSO role.

5. Services

5.1. Initialization Transaction

SMD initialization is performed in the factory after the SMD has been assembled, powered up and given the initial factory testing. The Initialization service is obtained when the host and the SMD successfully engage in an Initialization transaction over the SMD's host serial port.

The SMD is in the Unitialized state immediately after manufacture, and the SSO and User PINs contain the initial PIN value. The SSO logs into the SMD using the initial PIN value and immediately sets a new unique SSO PIN and a unique User PIN.

After setting the PINs the SSO performs an Initialization transaction with the new SMD. The Initialization transaction proceeds as follows:

- The SMD verifies that the SSO is signed in using the SSO’s PIN.
- The SMD receives a message from the host that contains the SMD serial number, software ID, and Neopost Online public key.
- The SMD initializes its internal accounting registers and generates a public/private key pair. The SMD stores these keys in a secure internal memory.
- The SMD signs the public key using the private key and exports the public key to the host using an initialization reply message. At this time the SMD transitions from the Uninitialized state to the Initialized state.
- Finally, the SSO issues a Real Time Clock setting message to the SMD to set the SMD’s clock. The clock is used to time-stamp indicia as well as to determine if a watchdog timeout has occurred.
- After completing these operations, the SSO powers down the SMD. This automatically logs the SSO out.

5.2. Authorization Transaction

An Authorization transaction requires that the SMD be in the Initialized state and that a valid SSO or User PIN has been entered.

This service installs the SMD at a customer site and notifies the Neopost Online POC system to activate the customer’s account. The Authorization service is obtained when the host and the SMD successfully engage in an Authorization transaction over the SMD's host serial port. The Authorization is validated by requiring the data transferred from the host to the SMD be signed using the Neopost Online private key. The SMD verifies the signature using the Neopost Online public key contained in the X.509 certificate, which was loaded by the SSO during Initialization.

The Authorization transaction performs the following functions:

- The SMD verifies that the SSO or User is signed in using the appropriate PIN.
- Loads the SMD’s X.509 certificate into the SMD. The SMD includes this certificate in each signed indicium.
- Loads the customer’s account number and licensing information into the SMD,
- Loads maximum and minimum revenue, and watchdog timer increment into the SMD,
- Loads the controlling authority’s X.509 certificate into the SMD. A controlling authority (such as the USPS) provides a certificate to the SMD containing the authority’s public key so the SMD can verify signature on messages signed by the authority. (At the time of this writing there are no Controlling Authority messages).

- The SMD transitions from the Initialized to the Unfunded state.

5.3. Funding Transaction

This service allows an entity operating in the SSO or User role to add more revenue to the SMD so it can generate more indicia. Funding is obtained when the SMD and host engage in a funding transaction as follows:

- The User or SSO instructs the host computer to obtain funding. The host sends a message containing the requested funding amount to the SMD.
- The SMD verifies that the SSO or User is signed in using the appropriate PIN. It also verifies that the SMD is in either the Unfunded or Funded states.
- The SMD increments its internal transaction ID counter. The SMD generates a message containing a PVDR (Postage Value Download Request) field to be forwarded to the Neopost Online POC system. The PVDR field contains the transaction ID, current contents of the secure accounting registers, customer licensing information, and current date and time. The message is signed by the SMD using the SMD's private key.
- The host forwards the message containing the PVDR field to the Neopost Online POC system.
- The POC system, acting in the role of Neopost Online User, validates the signature on the PVDR field and returns a message to the host, which is forwarded to the SMD. The message contains either a PVD (Postage Value Download) field to authorize the funding, or a PVDE (Postage Value Download Error) field to reject the funding. The PVD or PVDE field is signed using the Neopost Online private key, and the signature is verified by the SMD using the public key contained in the Neopost Online X.509 certificate. The SMD also verifies that the PVD or PVDE field contains the same transaction ID number as the PVDR field forwarded to the POC by the host in the previous step.
- If the message from the POC contains a PVD field indicating funding authorization, the secure revenue registers contained in the SMD are incremented by the amount of the funding request. If the message contained a PVDE field indicating that the funding request was rejected, the SMD does not increment the revenue registers.
- In either case, the SMD returns a message to the host which is forwarded to the POC containing a PVDS (Postage Value Download Status) field, indicating the status of the revenue registers after the processing of the PVD or PVDE fields. This status message contains the same transaction ID number as the previous funding messages, and is signed using the SMD's private key.
- If the SMD was in the Unfunded state at the beginning of the Funding transaction, it transitions to the Funded state. If the SMD was in the Funded state at the beginning of the Funding transaction it remains in the Funded state. This completes the Funding transaction.

5.4. Indicium Transaction

This service allows a User or SSO to obtain revenue in the form of indicia from the SMD. The indicium service is obtained when the host PC and SMD engage in an Indicium transaction. The Indicium transaction performs the following functions:

- The SMD verifies that the SSO or User is signed in using the appropriate PIN.
- The SMD checks to make sure that the accounting registers contain enough revenue to allow the requested indicium to be issued. The SMD must be in the Funded state unless the requested value is zero, in which case the SMD may be in either the Initialized, Unfunded, or Funded states.

- The SMD deducts the requested revenue amount from the secure accounting registers.
- The SMD assembles the indicium bit pattern and signs it using the private key generated during the Initialization transaction.
- The SMD sends the signed indicium to the host computer.

5.5. Audit Transaction

The SMD contains a timer, called the "Watchdog Timer", which will allow it to perform services for a fixed period of time. An Audit transaction is defined, by which a User or SSO may report the status of the SMD to Neopost Online. Upon receipt of a proper status report, Neopost Online sends a message to the SMD which causes the SMD to increment the watchdog timer by a fixed amount. This gives the SMD more time to operate before the timer times out. If the timer times out before an Audit transaction is performed, and if the SMD is in either the Unfunded or Funded states, the SMD will transition to the Timed-Out state, and no further operation (except for an Audit transaction) will be performed by the SMD.

The Audit transaction proceeds as follows:

- The Audit transaction begins when the User or SSO requests an Audit from the host. The host forwards the request to the SMD.
- The SMD verifies that the SSO or User is signed in using the appropriate PIN and that the SMD is in either the Unfunded, Funded, or Timed-Out states.
- The SMD increments its internal transaction ID counter. It then generates a message containing a Device Audit field. The Device Audit field contains the status of the SMD's revenue registers and the transaction ID number. The Device Audit field is signed using the SMD's private key and the message is sent to the host. The host forwards the Device Audit field to the Neopost Online POC system.
- The Neopost Online POC, operating in the Neopost Online User role, verifies the signature on the Device Audit field, analyzes the data contained therein, and generates a message containing a DAR (Device Audit Response) field. The DAR field contains the same transaction ID number as the Device Audit field, and is signed using the Neopost Online private key and the message is sent to the host which forwards it to the SMD.
- The SMD verifies the signature on the DAR field, thus validating the Neopost Online User role. The transaction ID number is also verified to confirm that it is the same as the one sent in the Device Audit field. If the signature and transaction ID are valid, the SMD examines the remainder of the DAR field and resets the watchdog timer accordingly.
- The SMD sends a response message to the host computer confirming that the Audit transaction is complete. If the SMD was in the Timed-Out state, it transitions to either the Funded state if it was in the Funded state before timing out, or to the Unfunded state if it was in the Unfunded state before timing out. Otherwise, if the SMD was in the Funded or Unfunded state at the time of the audit, the SMD remains in the Funded or Unfunded state.

5.6. Withdrawal Transaction

Once the SMD has been authorized to a particular customer's account, it functions on behalf of that account only. This means that when the SMD is funded, that customer's account at Neopost Online is debited the amount of the funding plus any associated service charges. If that SMD is to be reused on a different account, it must be withdrawn from its present account and reauthorized for the new account. This service is obtained via the Withdrawal Transaction.

The Withdrawal Transaction proceeds as follows:

- The Withdrawal transaction begins when a User or SSO requests a Withdrawal from the host. The host forwards the request to the SMD.

- The SMD verifies that the SSO or User is signed in using the appropriate PIN and that the SMD is in either the Unfunded or Funded states.
- The SMD increments its internal transaction ID counter and then generates a message containing a Withdrawal data field. The Withdrawal data field contains the status of the SMD's revenue registers as well as the transaction ID number. The Withdrawal data field is signed using the SMD's private key and the message is sent to the host. The host forwards the Withdrawal field to the Neopost Online POC system. The SMD then transitions to the Initialized stae.

5.7. Self Tests

The self-tests are run every time the SMD is powered up and upon certain conditions (DSA key generation and random number generation). The self-tests does not alter the contents of any SRDI. The module performs the following self-tests.

- Cryptographic Algorithm Tests
- Firmware Checksum Test
- Statistical Random Number Generator Tests
- Key Generation Pairwise Consistency Test
- Continuous RNG Test

5.8. Get X.509 Certificate Transaction

This service allows an entitity operating in the User or SSO role to read the contents of any of the three X.509 certificates stored in the SMD's non-volatile memories. The SMD verifies that either the SSO or User is signed in and then sends a message containing the appropriate X.509 certificate to the host.

5.9. Enable, Disable, and Configure Auxiliary Serial Port

These services allow the Customer to connect the host to a device via the SMD's auxiliary serial port, and to configure the port's baud rate and line parameters. The User or SSO must be signed in.

5.10. Check or Change PIN

The CHECK PIN service allows a User or SSO to assume the appropriate role by entering the appropriate USER or SSO PIN. The SMD will check the PIN and if it matches the stored PIN, the entity entering the PIN will be granted the appropriate role.

The CHANGE PIN service allows an entity logged in to the User role, to change the User PIN. It allows an entity logged into the SSO role to change the pin for either the User or SSO role.

5.11. Set, Read, or Change RTC

The SET RTC service allows an SSO to enter the initial value of the real-time clock. This service is only available to an entity signed in using the SSO PIN, and only while the SMD is in the Uninitialized or Initialized states.

The READ RTC service allows an entity singed in using the SSO or User PIN to read the current contents of the real-time clock.

The CHANGE RTC service allows an entity signed in using the SSO or User PIN to adjust the RTC plus or minus 5 hours to compensate for normal clock variation or time-zone changes.

5.12. Get or Send Aux Port Data

This service allows an entity signed in using the SSO or User PIN to transfer data via the host data port to or from the auxilliary data port.

5.13. Get Status or User Information

The GETVALIDID1 service instructs the SMD to provide data that uniquely identifies that SMD, and is available to an entity signed in using either a SSO or User PIN.

The GET STATUS and GET SIGNED STATUS services instruct the SMD to provide status information. One service provides the information in an unsigned format and the other service signs the information using the SMD private key. This service is available to an entity singed in using either the SSO or User PIN.

USERINFO services accept data from the host, add SMD data and sign the result, then send the result and signature to the host. This provides the host with a means to verify that it is communicating with a particular SMD. . This service is available to an entity signed in using either the SSO or User PIN.

6. Key Management

The SMD uses the DSS keys for signing and encrypting data and PINs for verification of Roles.

6.1. Neopost Online public key

The Neopost Online X.509 public key certificate is loaded into the SMD during the Initialization Transaction. This key is used to verify Neopost Online signed messages using DSA. This key remains in the SMD until replaced during another Initialization Transaction. Normally, only one such transaction is preformed during the life of the SMD.

6.2. Controlling Authority public key

The Controlling Authority X.509 public key certificate is loaded into the SMD during the Authorization Transaction. This key is used to verify signed messages from the authority. This key remains in the SMD until replaced during another Authorization Transaction. At the time of this writing there are no such messages sent by the Controlling Authority or recognized by the SMD.

6.3. SMD public/private key pair

During the Initialization transaction, the SMD is instructed to generate a new DSS public/private key pair. The SMD exports its public key to the SSO, signed using the SMD private key. The X.509 certificate for this public key is loaded into the SMD during the Authorization Transaction and is included in the bit pattern of each signed indicium.

The private key is stored in the SMD's secure memory inside the cryptographic module. The SMD private key is never exported (there is no service to do so), and no person inside or outside the Neopost Online factory ever knows the contents of any SMD's private key. This private key is used to sign indicia and other messages from the SMD. Any attempt to open the SMD's enclosure triggers the tamper detection circuitry, which causes the SMD to clear the private key.

6.4. SSO and User PINs

The SSO and User PINs are set to an initial PIN value upon the first power-up after manufacture. The SSO sets new SSO and User PINs immediately upon signing in for the first time.

7. Roles Vs. Services Matrix

Services	**Roles**	
	Site Security Officer	**User**
Initialization Transaction (INIT1 Message)	X	
Authorization Transaction (AUTHORIZE1, AUTHORIZE3 and AUTHORIZE4 Messages)	X	X
Indicium Transaction (INDICIUM1 Message)	X	X
Funding Transaction (FUND1, FUND3, and FUND5 Messages)	X	X
Audit Transaction (AUDIT1 and AUDIT3 Messages)	X	X
Withdrawal Transaction (WITHDRAW1 Message)	X	X
SELFTEST Message	X	X
ACCESS REQUEST Message	X	X
CHANGE SSO PIN Message	X	
CHANGE User PIN Message	X	X
CHANGE RTC Message	X	X
CHECK PIN Message	X	X
CONFIG AUX PORT Message	X	X
ENABLE AUX PORT Message	X	X
GET AUX DATA Message	X	X
GET STATUS Message	X	X
GET SIGNED STATUS Message	X	X
GETVALIDID1 Message	X	X
GET X.509 CERTIFICATE Message	X	X
PWITHDRAW1 Message	X	X
READ RTC Message	X	X
SEND AUX DATA Message	X	X
SET RTC Message	X	
USERINFO1 Message	X	X
USERINFO3 Message	X	X