neopost
INDUSTRIE

Recherche & Développement

113, rue Jean Marin Naudin
92220 BAGNEUX
France

☎ 33 (0)1 45 36 30 00
📠 33 (0)1 45 36 30 10

Security Policy
NSD Postage Meter

J. Modolo / F. Torché

	SUIVI DES REVISIONS APPROBATION, DIFFUSION	SPEC.272
neopost INDUSTRIE Research & Development		

ORIGINE :

SUIVI DES REVISIONS :		
		See "Changes History", page iii

Ce document annule et remplace le précédent qui doit être détruit.
Les versions précédentes peuvent être consultées au service Documentation.

VERIFICATION – APPROBATION			
	DATE	*VISA*	*NOM*
Le rédacteur			Nathalie TORTELLIER & Jerome MODOLO
Chef de projet			Patrick BLANLUET, Fabien TORCHE & Jerome MODOLO
Chef du service Electronique			Bernard MOURGUES
Directeur Recherche & Déve-loppement			Thierry LE JAOUDOUR
DIFFUSION			
Les signataires + Equipe logicielle			

Change History

Version	Date	Who	Description
Draft 1	10/19/99	PB	Initial Draft based on SMD security policy
A	03/20/00	PB	Update due to E Morris remarks
B	04/06/00	PB	Update after meeting of 03/31/00
C	09/11/00	PB	Update due to R Saunders remarks
D	10/10/00	PB	Addition of some details for FIPS approval
E	07/11/00	PB	Last update for FIPS report
F	11/27/00	RS	Final update for NIST submission (Pending re-view)
G	07/26/01	PB	Update after USPS meeting of 07/02/01
H	02/08/02	NT/ PB	Update for IBIP Meter (N18I)
I	25/04/02	NT	Update for N18I NIST Submission
J	16/01/03	JS	Update for N18I NIST comments
K	11/06/03	JS	Update for N18I NIST comments
L	25/04/04	JM/ FT	Update for N20I/165 FIPS submission
M	14/06/04	JM	Update due to A.Gandreti/CEAL remarks
N	24/06/04	JM	Update due to R.Tencati/CEAL remarks Add references for additional security modules
O	04/10/04	JM	Update for N20I/165 FIPS submission
P	04/20/05	JM	Update for postal product codes statistics man-agement
Q	10/14/05	JM	Update N22i/265 FIPS submission

Table of Contents

1. Introduction

This Security Policy document is applied to the NSD Postage Meter modules. In the rest of the document those modules will be referenced by the term "NSD". NSD stands for Neopost Security Device.

The NSD postage meter is a small electronic device developed by Neopost which stores customer postal revenue until the Franking Machine in which it is included needs it. This meter attaches to and communicates with the base via a proprietary bus. The revenue is dispensed from the meter to the external world in the form of the printing of an indicium, a unique stamp pattern with red fluorescent ink, which can be determined to have originated from a particular meter at a particular point in time. The printed indicium includes a 2D barcode containing audit information. The 2D barcode is digitally signed by the meter using ECDSA.

The NSD contains an electronic memory which registers the amount of revenue remaining to be disbursed, as well as other security related data items necessary to secure and validate that revenue amount.

The hardware release for the latest NSD Postage Meter is Rev. 4127907C-A

The following table shows the modules for which this security policy applies:

Hardware Part Number	Sofware Version	Commercial Models	Modifications
4127906B-A	"10.2"	N18i/N18iG/162/163	Initial Module
4127906B-B	"10.2"	N18i/N18iG/162/163	Change FIPS plastique Box
4127907C-A	"30.11"	N20i/N20iG/165/166	Minor software changes for support of additional peripherals Expanded memory capability of flash
4127907C-A	"30.13"	N20i/N20iG/165/166	Minor software changes to address a printing synchronization issue. No security-relevant components of the module were affected
4127907C-A	"30.15"	N20i/N20iG/165/166	Minor software changes to address a statistics management with server. No security relevant components of the module were affected
4127907C-A	"30.21"	N22i/N22iG/265/266	Minor software changes to address a wrong support target, backward compatibility timings, ink spitting improvement with dynamic weighing.

Software is identical between Neopost and Hasler commercial models.

1.1. Scope

This document contains a statement of the security policy for the NSD. The security policy specifies the security requirements under which the NSD is designed. It also discusses the FIPS 140-1 requirements to which it complies.

1.2. References

The following references provide additional information:

[1] Information Based Indicia Program, Performance Criteria for Information-Based Indicia and Security Architecture for Closed IBI Postage Metering Systems (PCIBI-C), USPS, (draft dated 01/12/99 - document number unknown).

[2] reserved

[3] Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-1.

[4] Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2

[5] Secure Hash Standard, Federal Information Processing Standards Publication 180-1

[6] Public Key Cryptography for the Financial Services Industry : the Elliptic Curve Digital Signature Algorithm, American national Standard for Financial Services X9.62 -1998

1.3. Glossary of Names and Acronyms

3DES: Triple Data Encryption Algorithm

DSA: Digital Signature Algorithm

ECDSA: Elliptic Curve Digital Signature Algorithm

EDC: Error Detection Code

FIT: Factory Initialization Tool

Base: The main part of the franking machine, which communicates with the NSD over the proprietary bus. Depending on the context, it may reference the electronics and software; or the electronics, the software and the mechanics.

MAC: Message Authentication Code.

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

Meter: Common name for the NSD (Meter comes from metering).

NSD: A product designed by Neopost, which meters revenue on a per-use basis to a base device such as a personal computer. In this document "NSD" stands for Neopost Security Device.

PCB: Printed circuit board.

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

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

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

Role: A position relative to the meter occupied by an entity requesting services from the meter.

RTC: Real-Time Clock: The RTC is a clock contained in the meter which 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 performed by the meter on behalf of an entity operating in a particular role.

SRDI: Security Relevant Data Item: A data item stored in the meter.

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

INDUSTRIE

2. Security Level

The NSD is a Multiple-Chip Embedded Cryptographic Module as defined in reference [3], Security Requirements for Cryptographic Modules, FIPS publication 140-1. The NSD meets the overall requirements for FIPS 140-1 Level 2 security, as defined in reference document [3]. As per USPS requirements, the module, in addition to meeting the FIPS 140-1 Level 3 requirements for physical security, must also include environmental failure testing (EFT) and a tamper detection envelope. The following table shows the security level requirement for each component FIPS 140-1:

Security Requirements Section	FIPS 140-1 Security Level
Cryptographic Module	2
Module Interfaces	2
Roles & Services	2
Finite State Machines	2
Physical Security	3+EFT**
Software Security	3
Operating System Security	N/A
Key Management	2
Cryptographic Algorithms	2
EMI/EMC	3
Self Tests	2

** Per USPS PCIBI-C requirement, the NSD shall provide a tamper detection envelope with tamper response circuitry and shall also provide EFT protection.

3. NSD Overview

When an operator performs an operation on the base, which requires the meter to dispense revenue, the base and meter exchange a series of messages called an Indicium transaction. The Indicium transaction causes the meter to deduct the revenue amount from its secure revenue registers, and create a stamp representing the revenue (called an indicium); it then prints the stamp onto an envelope or label with red fluorescent ink. The printed indicium is verifiable visual evidence that revenue was paid.

After having dispensed revenue over a period of time, the values stored in the meter's revenue registers will have been reduced to the point that the user will need to add more revenue to continue printing indicia. Revenue is added by executing a Funding transaction. A Funding transaction involves communication between the base and the Neopost funding computer (called the POC system), as well as between the base and meter. At the completion of the Funding transaction, the meter revenue registers are incremented by an amount specified by the POC system, and the POC system debits the user's account at Neopost. The customer ultimately pays Neopost for the revenue dispensed via the printed indicia.

3.1. Components & Communication Interfaces

The meter (FIPS 140-1 cryptographic module) consists of a main microprocessor, main working RAM, secured RAM (for cryptographic keys and other SRDI storage), Flash memory, and FRAM (for postal-related data storage) contained on a printed circuit board (PCB). The module meets FIPS 140-1 Level 3 physical security requirements by encasing the module components inside a tamper-resistant 'envelope' which uses hard, opaque epoxy potting material. In addition the module contains an active-circuit tamper mesh to protect the security-related module components and corresponding circuit board from attack on all six sides. This tamper-resistant 'envelope' is surrounded by an opaque tamper-evident hard plastic casing, which forms the cryptographic boundary of the module. The module is further housed in a metal enclosure (outside of the cryptographic boundary).

The meter communicates with the base, which is outside the cryptographic boundary, using request / response message pairs called "transactions". Services are obtained from the meter by the base by requesting the proper transactions.

The module interfaces are defined as the data paths leading to and from the main micro processor and bus-control chips which lie within the protected cryptographic boundary. These data paths provide the FIPS 140-1 interfaces for data input, data output, control input and status output. The signals from these interfaces are carried to serial interfaces, which are outside the cryptographic boundary. The secondary serial interface has two uses. The principal purpose, and the only one used during field operation is to provide a channel to write and read status information from the main micro to the printing head-set (i.e. ink color, drop counter). In this mode, secondary interface data is not interpreted by the meter and there are no services in the meter which can be activated via data sequences use on this interface. In fact any attempt to apply a command to the secondary interface is logged as a fraud attempt by the meter. The second is only active during the manufacturing process (outside the FIPS 140-1 scope) and is only available if the Factory Initialization Tool (FIT) jumper is connected after the power on AND if the Meter status is *Uninitialized, Pending Installation or Pending Withdrawal.*

3.2. Life Cycle

The life-cycle of the meter consists of the following phases:

3.2.1. Manufacturing

3.2.1.1. Initial Manufacturing

This phase of the life-cycle only happens once to a given Meter. It takes place at the Neopost Ind. factory (in France) where the Meter hardware is manufactured and the software is loaded.

As during this phase, the Meter is not a full "US NSD"; this phase is considered before the hardware becomes a FIPS module.

At the end of this phase, the Meter's tamper zeroization envelope is sealed and filled with opaque potting epoxy, but the tamper detection electronics are inactive. The Meter includes the software (without postal bitmaps), the Neopost public transport DSA key and the programming security flag is set.

3.2.1.2. Customization

This phase of the life-cycle happens once to a given Meter. It takes place at the Neopost Group factory (in Memphis) where the Meter is configured as an US Meter.

As during this phase, the Meter is not a full "US NSD"; this phase is considered before the hardware becomes a FIPS module.

The Crypto-Officer must install the meter on a special equipment (called FIT) to perform customization. He then initializes the memories to prepare it to be initialized. All transactions between the meter and the Crypto-Officer as well as any data output by the meter to the Crypto-Officer are DSA-signed using the Neopost transport key. The meter holds the DSA public key. Only the Crypto-Officer in Memphis has possession of the DSA private key.

At the end of this phase, the Meter includes the US Postal Bitmap and the US parameters (including the Neopost US 3DES key, the country public key and the User PIN code). Once the Neopost US 3DES Secret key is correctly loaded, the tamper detection electronics are active.

3.2.2. Initialization

Initialization of the meter is performed by the Crypto Officer at the Neopost Group facility (in Memphis, TN.) before the meter is placed in service. Initialization is performed using the FIT. At this time, the meter's tamper zeroization envelope is already installed and the tamper detection electronics are active. During the initialization process, the meter receives the Neopost public DSA key and generates its own DSA and ECDSA key pairs. The meter exports its public keys to the Crypto-Officer in transactions signed with the Neopost public transport key.

The initialization process enables the meter to perform as an electronic revenue metering device. At the end of the initialization process, the meter is considered to be a FIPS 140-1 module, and it can then shipped to end users.

3.2.3. Authorization (Registration)

After the meter is initialized, it must be Authorized. Authorization prepares the meter to operate in a particular customer's office, and prepares an account at Neopost for the customer. The communication occurs via the meter's secondary or primary serial interface, using the FIT or the base's modem connection to the Neopost POC.

3.2.4. Funding

After Authorization, the meter must be funded before it can dispense revenue. The customer uses the base to contact the Neopost POC computer via modem, and authorizes Neopost to debit the customer's account. After debiting the account, the Neopost POC computer sends a message to the meter through the base informing the meter of the amount of the funding. The meter records the funding amount in its non-volatile memories.

3.2.5. Indicium Dispensing

After funding the meter, the customer may use the franking machine to print a signed indicia representing the revenue contained in the meter. Each time an indicium is printed, the meter deducts the amount of the indicium from the funding amounts stored in the meter memories. When the funding level drops below a certain level, the meter refuses to issue indicia until the customer provides additional revenue.

3.2.6. Auditing

Periodically during operation, the meter must be audited. If the meter is not audited within a specified amount of time, it will refuse to print indicia. The meter is audited by allowing it to communicate with the Neopost POC system via the base's modem. The Neopost POC reads critical information from the meter's memories, then instructs the meter to allow continued printing of indicia. It also resets the time watchdog to the next Audit.

3.2.7. Withdrawal

After operating in the customer's site for a period of time, the customer or Neopost may wish to remove the meter from service. When this occurs, the meter is withdrawn and returns to the Neopost Group factory from which it may be re-initialized and authorized to another customer.

4. Roles

The meter supports the following roles:

- Crypto-Officer Role

- Customer Role (FIPS 140-1 User role)

The meter enforces the separation of roles by restricting the services available to each role.

4.1. Crypto-Officer Role

The Crypto-Officer is responsible for customizing, initializing and authorizing the meter at the Neopost Group facility. Initialization and Authorization are the main services available to the Crypto-Officer. The Crypto-Officer role is only available at the Neopost Group facility through the FIT tool and with the Meter in uninitialized, Pending Installation or pending withdrawal states. The Crypto-Officer must communicate with the meter using digitally-signed transactions. This provides identity-based authentication of the Crypto-Officer role.

The meter validates the Crypto-Officer role by requiring the Crypto-Officer to use a specific physical tool and to perform his role on a blank, uninitialized, Pending Installation or pending withdrawal meter. The meter only allows the Customization and Initialization services if the interface is used and if the programming security is set.

The Initialization service causes the meter to generate its public/private key pairs (DSA and ECDSA), export the public keys, load the Neopost X.509 certificate containing the Neopost public key. The Crypto-Officer is responsible for obtaining and loading the Neopost X.509 certificate and for archiving the meter public keys.

After initializing the meter, the Crypto-Officer may perform the authorization and remove the meter from the FIT.

Using the FIT the Crypto-Officer can send the Zeroize command to the module, causing the module to zeroize all CSPs.

Two other less significant services available to the Crypto-officer are Get Status and Set RTC.

The Crypto Officer functions that can be performed while the module is in FIPS mode are limited to Authorization of the meter and Resetting the Real Time clock more than +/- 3 hours.

4.2. Customer Role

The meter also supports a Customer (FIPS 140-1 User) role for which the following service interfaces are provided:

- Generate Indicium (uses ECDSA for signature)

- Get Status

- Perform Self Tests

- Read & Adjust RTC

- Request (trigger) the POC transactions (Authorization, Funding, Audit, Update Registration, Withdrawal) (Uses DSA for authentication)

- Connect an external printing device

The base unit is the FIPS 140-1 user. Individual meter units each have unique serial number associated with them. A user PIN number is created and installed into the module by the Crypto Officer during the Customization cycle of the manufacturing process. The user PIN number is sent to the end-user by an external process. Whenever a new module is inserted into a base unit in the field, the operator must enter its unique PIN number. The base unit thereafter stores the PIN number in its local RAM.

Prior to deriving any services, the base unit, FIPS user, must transmit its unique serial number and the user PIN to the meter. The meter verifies this serial number / PIN. In this way, the meter enforces Identity-Based authentication of the user. Until the user is authenticated, the module does not allow access to any of the user services.

Once the correct serial number / PIN code has been received, the User role services are available until the next powering off of the Meter.

5. Services

The meter provides services by exchanging messages between itself and the base (or the FIT PC). The meter supports the following Postal services:

5.1. Customization (outside FIPS 140-1)

Customization consists of the loading of the Meter parameters to transform it into a regular US Meter. Customization may only be performed by a Crypto-Officer using the FIT PC, and must be performed at the Neopost Group factory. Furthermore, the meter must be installed on a specific interface (FIT) and its programming security flag must be set before it will recognize a Customization request. Furthermore, the FIT PC shall sign its transaction using the transport private key. The following functions are performed by the Customization transaction:

- Loads the US country variant i.e. the parameters defining it as a US Meter, including the US 3DES Secret Key and the User PIN,

- Loads the US postal bitmap,

- Loads the US Country Public key,

- Puts the meter's finite state machine software into the *Uninitialized* state.

5.2. Initialization

Initialization causes the meter to generate a public/private key pair, and to export the public key. Initialization may only be performed by a Crypto-Officer using the FIT PC, and must be performed at the Neopost Group factory. Furthermore, the meter must be installed on a specific interface and its programming security flag must be set before it will recognize an Initialization request. The following functions are performed by the Initialization transaction:

- Loads the Neopost X.509 certificate, containing the Neopost public key and the DSA parameters p, q, and g, into the meter,

- Instructs the meter to generate two public/private key pairs (DSA and ECDSA),

- Instructs the meter to export its public keys,

- Puts the meter's finite state machine software into the *Pending Installation* state.

- Initializes the RTC.

5.3. Authorization (Registration)

This service prepares the meter for installation at a customer site and notifies the Neopost POC system to activate the customer's account. The Authorization service is obtained when the base and the meter successfully engage in an Authorization transaction over the meter's primary serial interface or when the FIT and the Meter successfully engage in an Authorization transaction over the meter's secondary serial interface. The Authorization may only be performed by an entity operating in the Neopost User role or Crypto-officer role, and these roles are validated respectively by requiring that the data transferred from the base to the meter be signed using the Neopost private key or by the use of the FIT. The meter verifies the signature using the Neopost X.509 certificate, which was loaded by the Crypto-Officer during Initialization.

The Authorization transaction performs the following functions:

- Loads the meter's X.509 certificates (DSA and ECDSA) into the meter.

- Loads the customer's account number and licensing information into the meter

- Loads maximum and minimum indicium revenue, and watchdog timer increment into the meter,

- Puts the meter's finite state machine software into the *Installed* state.

5.4. Generate Indicium

This service allows a Customer to obtain revenue in the form of indicia from the meter. The indicium service is obtained when, at the Customer's command, the base and meter engage in an Indicium transaction. The Indicium transaction performs the following functions:

- The meter checks to make sure that the accounting registers contain enough revenue to allow the requested indicium to be issued. When the funding level drops below a certain level, the meter refuses to issue indicia until the customer provides additional revenue. If the accounting registers do contain enough revenue,

- The meter deducts the requested revenue amount from the secure accounting registers,

- The meter signs the Barcode data to be included in the indicia using its ECDSA private key,

And either,

- The meter assembles the indicium, which includes the Barcode data and the signature.

- The meter sends the indicum to the base printhead using a proprietary data format.

Or,

- The meter sends the data necessary to build the indicia to an external device

5.5. Funding

This service allows an entity operating in the Customer role to add more revenue to the meter so it can generate more indicia. The Customer actually instructs the base to begin a Funding transaction. Note that an entity operating in the Customer role cannot authorize the Funding service, but can request that the service be initiated. The meter actually performs the Funding service. Funding is obtained when the meter and base engage in a funding transaction as follows:

- The transaction begins when the Customer instructs the base to obtain funding. The base sends a message containing the requested funding amount to the meter.

- The meter generates a message containing a PVDR (Postage Value Download Request) field to be forwarded to the Neopost POC system. The PVDR field contains the current contents of the secure accounting registers, customer licensing information, and current date and time. The message also contains a transaction serial number generated by the meter. The message is signed by the meter using the meter's private DSA key.

- The base forwards the message containing the PVDR field to the Neopost POC system.

- The POC system validates the signature on the PVDR field and returns a message to the base, which is forwarded to the meter. 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 private DSA key and the signature is verified by the meter using the public key contained in the Neopost X.509 certificate. The meter also verifies that the PVD or PVDE field contains the same transaction serial number as the PVDR field forwarded to the POC by the base in the previous step.

- If the message from the POC contains a PVD field indicating funding authorization, the secure revenue registers contained in the meter are not incremented immediately. Instead, the Meter memorizes that the transaction was successful and waits for an Audit transaction to increment the registers by the amount of the funding request. If the message contained a PVDE field indicating that the funding request was rejected, the meter does not increment the revenue registers.

- If the funding was accepted, the meter returns a message to the base, 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. If it was not successful, the Meter simply issues a state message. This status message contains the same transaction serial number as the previous funding messages, and is signed using the meter's private key. This completes the Funding transaction.

5.6. Audit

The meter 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 Neopost User may obtain the status of the meter and increment the watchdog timer, giving the meter more time to operate before the timer times out. If the timer times out before an Audit transaction is performed, the meter will transition to the *Locked for Auditing* state, in which no further operation (except for an Audit transaction) is permitted.

- The Audit transaction begins when the Customer requests an Audit or a Funding from the base. The base forwards the request to the meter.

- The meter generates a message containing a Device Audit field. The Device Audit field contains the status of the meter's revenue registers as well as a unique transaction number generated by the meter. The Device Audit field is signed using the meter's private key and the message is sent to the base. The base forwards the Device Audit field to the Neopost POC system.

- The Neopost POC 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 number as the Device Audit field, and is signed using the Neopost private key and the message is sent to the base which forwards it to the meter.

- The meter verifies the signature on the DAR field, thus validating the Neopost User role. The transaction 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 numbers are valid, the meter examines the remainder of the DAR field and resets the watchdog timer accordingly. If the meter was in the *Locked for Auditing* state, it transitions to the *Installed* state.

- If the transaction was successful and if the Meter had recently completed a Funding transaction, the revenue registers are incremented by the memorized funding amount.

- The meter sends a response message to the base confirming that the Audit transaction is complete.

5.7. Withdrawal Transaction

Once the meter has been authorized to a particular customer's account, it functions on be-half of that account only. This means that when the meter is funded, that customer's ac-count at Neopost is debited the amount of the funding plus any associated service charges. If that meter is to be reused on a different account, it must be withdrawn from its present account and re-initialized and authorized for the new account.

- The Withdrawal transaction begins when the Customer requests a Withdrawal from the base. The base forwards the request to the meter.

- The meter generates a message containing a Withdrawal field. The Withdrawal field contains the status of the meter's revenue registers as well as a unique transac-tion number generated by the meter. The Withdrawal field is signed using the me-ter's private DSA key and the message is sent to the base. The base forwards the Withdrawal field to the Neopost POC system.

- The Neopost POC system verifies the DSA signature on the Withdrawal field, ana-lyzes the data contained therein, and generates a message containing a Withdrawal Response field. The Withdrawal Response field contains the same transaction number as the Withdrawal field, and is signed using the Neopost private key and the message is sent to the base which forwards it to the meter.

- The meter verifies the DSA signature on the Withdrawal Response field, thus vali-dating the Neopost User role. The transaction number is also verified to confirm that it is the same as the one sent in the Withdrawal field. If the signature and transaction numbers are valid, the meter transitions to the *Pending Withdrawal* state.

- The meter sends a response message to the base confirming that the Withdrawal transaction is complete.

5.8. Update Registration Transaction

This service changes the parameters of the customer's account. The Update Registration service is obtained when the base and the meter successfully engage in an Update Regis-tration transaction over the meter's primary serial interface. The Update Registration may only be performed by an entity operating in the Neopost User role, and this role is vali-dated by requiring that the data transferred from the base to the meter be signed using the Neopost private key. The meter verifies the signature using the Neopost X.509 certificate, which was loaded by the Crypto-Officer during Initialization.

The Update Registration transaction performs the following functions:

- Loads the customer's account number and licensing information into the meter

- Loads maximum and minimum indicium revenue, and watchdog timer increment into the meter,

5.9. Other Services

The following additional services can be obtained in the Customer role. They are obtained when an entity operating in the Customer role requests the service from the base or if an entity operating in the Crypto-officer role requests the service to the Meter through the FIT. The base and meter engage in a transaction, which provides the service.

5.9.1. Status

The Status transaction is initiated by the base when it sends a Get Status message to the meter. The meter responds by sending a status message back to the base. The status message contains the current contents of the revenue registers, customer licensing information and some non-security related data items.

5.9.2. Self Tests Transaction

This transaction is initiated by the base upon request by the user, by sending a Self Test message to the meter. The meter responds by performing its self tests and sending the results to the base in a Self Test Response message. The details of the tests are described in section *6.2. Power-Up Security Requirements*. The Self Test transaction can be performed while the meter is in any state. The Self Test transaction shall not alter the contents of any SRDI. The Self Test message allows one or more of the following tests to be selected:

- CPU Self Test (as described 6.2.1.2)

- Volatile Memory Self Test

- Registers Memories Self Test

- Cryptographic Algorithms Tests (as required by FIPS 140-1)

- Firmware Test (as required by FIPS 140-1 and described 6.2.2.2)

- Random Number Generator Tests (as required by FIPS 140-1)

5.9.3. Adjust RTC Transaction

This transaction allows the Customer to adjust the time contained in the real-time clock (RTC) to account for errors in the clock rate, which may accumulate over time, as well as changes to and from Daylight Savings Time, etc. This transaction only allows a +/- 3 hours difference from the reference Time set-up during the initialization of the Meter.

5.9.4. Get X.509 Certificate Transaction

This transaction allows the Customer to read the contents of any of the 3 X.509 certificates stored in the meter's non-volatile memories.

5.9.5. Connect an external printing device

The device number is sent to the Meter. The authorization of the device is made by encrypting device number using the Neopost US Security key [this is also referred to as the TDES mother key] and using that key to verify MAC from device message.

5.9.6. Zeroization

In case of tampering (access attempt to the security-related part of the PCB), the zeroization function is triggered, which will erase Saved RAM, zeroizing all CSPs.

In Crypto Officer mode, using a FIT the Crypto Officer can send a Zeroize command to the module. The module will erase the Saved RAM, zeroizing all CSPs.

5.10.1 Roles Vs. Services Matrix

The following table summarizes the services available to the two roles supported by the meter. The table shows both USPS/IBIP and Cryptographic (FIPS 140-1) services.

Services	Crypto Officer	User
Postal Services		
Customization	X	
Initialization	X	
Authorization	X	
Generate Indicium		X
Trigger Funding Transaction		X
Trigger Device Audit		X
Trigger Withdrawal		X
Trigger Registration/Update		X
General Services		
Get Status	X	X
Perform Self Tests	X	X
Adjust RTC	X	X**
Connect External Device		X
Cryptographic Services		
Generate ECDSA Signature*		X
Encrypt Data w/TDES*		X
Generate DSA Signature*		X
Verify DSA Signature*		X
Create ECDSA Keypair	X	
Create DSA Keypair	X	
Install TDES Mother Key	X	
Create TDES Daughter Key*		X
Perform TDES MAC*		X
Verify TDES MAC*		X

*Not user-callable, performed as part of another function
**RTC adjustement is limited to +/- 3h for user

5.10.2 Security relevant data item access matrix

Operator	Role	Service	Security relevant data item	Access
The crypto officer	Crypto Officer	Customization (Outside FIPS)	Neopost US 3DES secret key	Write
The crypto officer	Crypto Officer	Customization (Outside FIPS)	User PIN Code	Write
The crypto officer	Crypto Officer	Customization (Outside FIPS)	State	Write
The crypto officer	Crypto Officer	Initialization (Outside FIPS)	State	Write
The crypto officer	Crypto Officer	Authorization	State	Write
The crypto officer	Crypto Officer	Zeroization	All	Set to zero (Write)

The Generate Indicium, Withdrawal Transaction, Update Registration Transaction, Self Tests Transaction, Adjust RTC Transaction, and Connect an external printing device services don't allows either operator to read or write Security Relivant data items.

Some of these services cause the module to modify Security Relivant data items based on signed data received from Neopost via the modem.

5.10.3 Other access controlled data item access matrix

Operator	Role	Service	Security relevant data item	Access
The crypto officer	Crypto Officer	Initialization (Outside FIPS)	Neopost X.509 Certificate	Write
The crypto officer	Crypto Officer	Initialization (Outside FIPS)	meter Public Key	Read
The crypto officer	Crypto Officer	Initialization (Outside FIPS)	p, q, g	Write
The crypto officer	Crypto Officer	Initialization (Outside FIPS)	Device ID	Read
The crypto officer	Crypto Officer	Authorization	meter X.509 Certificate	Write
The crypto officer	Crypto Officer	Authorization	Account Number	Write
The crypto officer	Crypto Officer	Authorization	License ID	Write
The crypto officer	Crypto Officer	Authorization	Ascending Register	Write
The crypto officer	Crypto Officer	Authorization	Descending Register	Write
The crypto officer	Crypto Officer	Authorization	Watchdog Timer	Write
The crypto officer	Crypto Officer	Authorization	Watchdog Increment	Write
The base unit	User	Funding	Descending Register	Read
The base unit	User	Audit	Watchdog Timer	Read
The base unit	User	Status	Ascending Register	Read

The base unit	User	Status	Descending Register	Read
The base unit	User	Status	License ID	Read
The base unit	User	Get X.509 Certificate Transaction	Neopost X.509 Certificate	Read

6. Security Rules

This section states the security rules, which are required to be implemented by the meter. The rules are designed to protect the contents of the SRDIs (Security Relevant Data Items) from fraud and component failure.

6.1. General Requirements

6.1.1. The meter shall contain an SRDI in non-volatile memory, which indicates the current logical state of the meter. This variable is called the *State*. Certain transactions as noted herein shall change the contents of *State*, thereby changing the logical state of the meter.

6.1.2.While in the Error state, a meter shall not perform any transaction susceptible to alter any SRDIs.

6.1.3. The meter shall initialize a Fraud Counter to zero during the Audit transaction.

6.1.4. The meter shall increment the Fraud Counter each time a signature verification fails during a funding transaction. If the resulting number is greater than 50, the meter shall enter the error state.

6.2. Power-Up Security Requirements

Each time the meter is powered up it performs a sequence of operations designed to test security and determine the current state. The following requirements shall be met each time the meter is powered up:

If all those tests succeed, the Meter will not go into the error state and will indicate that the tests have passed by accepting the request from the Base to go into working modes, otherwise the Meter will go into the error state and will not go into working modes.

6.2.1. CPU and Volatile Memory Self Tests

The meter shall perform a test designed to determine if the basic facilities contained in the CPU are functional. This test shall be performed before any other self tests. Since the CPU is being used to test itself, it is not possible to determine if the CPU is in fact functional, but it is possible to determine if it is not functional in certain aspects. In particular, the tests outlined in this section shall be performed each time the CPU is powered up.

6.2.1.1. The firmware shall perform the CPU and memory self tests each time the CPU is powered up. The CPU self test shall be performed before the memory self test is performed. The CPU and memory self tests shall be performed before any other power-up self tests are performed.

6.2.1.2. The firmware shall verify that the CPU properly determines that two internally stored identical strings of length 128 bytes or greater are in fact identical. The firmware shall also verify that the CPU properly determines that two internally stored non-identical strings of length 128 bytes or greater are in fact not identical. If either of these tests fail, the meter shall go into the error state.

6.2.1.3. The firmware shall perform a test of all volatile RAM memory devices accessible by the CPU. The test shall alternately write and read-verify bit patterns to each memory location. The patterns shall be designed so as to verify that all bits are capable of changing state, and that each memory location is capable of storing patterns consisting of all ones and all zeros. If any of these tests fail, the meter shall enter the error state.

6.2.1.4. The firmware shall perform a test of all register-storing memory devices accessible by the CPU (i.e. Flash registers, FRAM registers, Saved RAM registers). The test shall verify the validity of the EDC protecting each security-related register. If any of these tests fail, the meter shall enter the error state.

6.2.2. Cryptographic Self Tests

The meter shall perform self tests to verify the proper operation of the cryptographic functions. The following self tests shall be performed each time the meter powers up:

6.2.2.1. Cryptographic Algorithm Test:

6.2.2.1.1. DSA & SHA-1 : The meter shall perform a "known answer" test in which the CPU shall generate a DSA signature on an internally stored data field (including a fixed value for k) and then verifies the generated signature. If the signature is correct, the test passes. If not, the test fails and the meter shall go into the error state. This test also performs the required testing for the SHA-1 hash.

6.2.2.1.2. ECDSA & SHA-1 : The meter shall perform a "known answer" test in which the CPU shall generate an ECDSA signature on an internally stored data field (including a fixed value for k) and then verifies the generated signature. If the signature is correct, the test passes. If not, the test fails and the meter shall go into the error state. This test also performs the required testing for the SHA-1 hash.

6.2.2.1.3. 3DES encryption : The meter shall perform a "known answer" test in which the CPU shall calculate the 3DES encryption for internally stored data fields and then compare the generated encrypted result to a reference result stored in memory. If the two results are identical, the test passes, if not, the test fails and the meter shall go into the error state.

6.2.2.1.4. 3DES decryption : The meter shall perform a "known answer" test in which the CPU shall calculate the 3DES decryption for internally stored data fields and then compare the generated decrypted result to a reference result stored in memory. If the two results are identical, the test passes, if not, the test fails and the meter shall go into the error state.

6.2.2.2. Firmware Test: The meter shall verify the checksum of the contents of the program memory (Flash). If the verification fails, the meter shall go into the error state.

6.2.2.3. Statistical Random Number Generator Tests: These tests are not required of a FIPS 140-1 level 2 module under FIPS 140-1 (see reference [3], section 4.11.1) at power-up. The meter shall execute these tests upon demand, and if any such test fails, the meter shall go into the error state.

6.2.3. Conditional Self Tests

6.2.3.1. Keys pair-wise consistency test (for DSA and ECDSA) : During initialization, when the meter generates a public/private key pair, the meter shall test the key pair using a pair-wise consistency test as required by FIPS 140-1 section 4.11.2 (reference document [3]). If the keys fail the test, the meter shall inform the FIT of the error.

6.2.3.2. RNG Test: The meter shall test its random number generator against failure to a constant value. Each time the Meter uses the pseudo random number generator, it shall perform the continuous random number generator test as specified by FIPS 140-1 section 4.11.2 (reference document [3]). If this test fails, the meter shall go into the error state. If it fails during initialization process, it shall inform the FIT of the error.

6.3. Cryptographic Operations

6.3.1. The meter shall employ the Digital Signature Standard (DSA or ECDSA) to sign all messages containing SRDIs to be reported to external devices. Such messages shall be signed using the meter's private key. ECDSA is used to sign the SRDI included in the bar-code part of the indicium.

6.3.2. The meter shall employ the Digital Signature Standard (DSA) to verify signature on all messages containing SRDIs to be written to the meter's non-volatile memories. Such messages shall be signed using the Neopost private keys, and shall be verified using the corresponding public keys from the X.509 certificates stored in the meter memory.

6.3.3. The meter's private keys shall not be made available via any communication interface or by any other means under software control.

6.3.4. The meter shall not sign externally generated data received via either communications interface using the meter's private key unless that data was received in a valid transaction under signature from Neopost, and only after the meter has verified the signature or MAC using its internally stored version of either the Neopost DSA public key or the TDES Mother key.

6.4. Key Management

6.4.1. The meter's private keys shall be generated during initialization transaction, stored in plain text form inside the crypto-memory (Saved RAM), and shall not be accessible by any means without triggering the zeroization mechanism.

6.4.2. No Key archiving (public or private) shall take place inside the Meter.

6.4.3. The Neopost US 3DES secret Key used to identify an authorized external device shall be initialized during the customization process. It is stored in plain text form inside the crypto-memory (Saved RAM), and shall not be accessible by any means without triggering the zeroization mechanism.

6.4.4. The printing device secret Key is generated using the Neopost US 3DES secret Key during the "Connect external printing device" transaction. It is stored in plain text form inside the crypto-memory (Saved RAM), and shall not be accessible by any means without triggering the zeroization mechanism.

7. Physical Security

The NSD meter is designed to meet FIPS 140-1 Level 3 physical and environmental security requirements. In addition the meter contains a tamper detection circuit and underwent Environmental Failure Testing. The NSD is a multi-chip embedded module. The cryptographic boundary is defined as the security related part of PC board of the meter. The cryptographic boundary is completely surrounded by a two-sided, flexible protective copper mesh that contains continuity circuitry on both sides. The copper mesh is connected to the module's tamper zeroization circuitry which protects the module's SRDIs. It is powered by an external battery when the module is not powered on. The protective mesh has a serpentine circuit pattern on one side and a "checkerboard" on the other. The clearance between the serpentine and checkerboard elements is 0.45mm.

The copper mesh material is surrounded on all sides by means of an opaque polypropylene housing which covers both sides of the PC board. The polypropylene housing is injection filled during manufacture with a dark, opaque epoxy potting resin, which then hardens solid. This action completely encases the module and zeroization circuitry and permanently bonds the opaque housing creating a permanent enclosure and a protective "envelope" which monitors the module with active zeroization protection from probing or tamper on all six sides.

In addition, the module was tested for Environmental Failure Testing (EFT) requirements for voltage and temperature.

8. Security Relevant Data Items (SRDI's)

This section lists all security relevant data items and gives a short description of each.

External Device 3DES secret key: key used to generate and verify the 3DES MAC used to validate the indicium transaction with a Neopost external device. This key is also referred to as the daughter key.

Neopost US 3DES secret key: key only used to generate an external device Secret key basing on its serial number. This key is also referred to as the mother key.

State: A code number uniquely identifying the current state of the meter. See STATECHG message for a list of state codes. Set to the *Uninitialized* state during initial manufacturing. Possible states are *Uninitialized, Pending Installation, Installed, Pending Withdrawal, Faulted, Locked for Audit*

meter Private Key: Private key generated during initialization (Initialization transaction). Stored in meter cryptographic module. Always kept secret and never exported. Used to sign meter generated data during Audit, Authorization, Funding, Initialization, Status, and Withdrawal transactions.

User PIN Code: 4 digits PIN Code sent by the Base used to authenticate the Customer User Mode. Loaded during initial manufacturing into the Meter's memory.

9. Other Access Controlled Data Items

This section lists data items that are not "Security Relevant Data Items" but are still protected by the meter using access control and gives a short description of each.

Account Number: Customers account number, loaded into the meter during an Authorization transaction.

Ascending Register: Ascending revenue register value. Cleared to zero during an Initialization transaction. Incremented by revenue amount during an Indicium transaction.

Descending Register: Descending revenue register value. Cleared to zero during an Initialization transaction. Decremented by revenue amount during an Indicium transaction. Incremented by revenue amount during an Audit transaction following a successful Funding transaction. The low order digit represents fractional cents.

Device ID: meter device number, loaded into the meter during Loaded during initialization (Initialization transaction).

Fraud Counter: A counter that counts the number of times a particular secure operation is performed in error. If the Fraud Counter exceeds the Fraud Counter Limit, the meter enters the error state.

Fraud Counter Limit: A number, contained in the meter's Memory, which is used to compare against the Fraud Counter each time the Fraud Counter is incremented. (See *Fraud Counter*).

g: DSA parameter used in signature verification, signature generation and keys generation. Loaded during initialization (Initialization transaction).

License ID: 10 digit ID number. Loaded during an Authorize transaction.

Licensing ZIP Code: 5 digit ZIP code of installation location of meter Loaded into the meter during an Authorization or Update Registration Transaction.

Maximum Postage: Maximum postage that can be printed in one indicium. Loaded into the meter during an Authorization or Update Registration Transaction.

meter Public Key: Public key to be transmitted to Neopost POC system during initialization (Initialization transaction).

meter X.509 Certificate: The X.509 certificate containing the meter's public key, necessary to verify the digital signature. Loaded into the meter during the Authorization transaction.

Minimum Postage: Minimum postage (other than zero) that can be printed in one indicium. Loaded into the meter during an Authorization or Update Registration Transaction.

Neopost X.509 Certificate: Contains Neopost public key. Loaded during initialization (Initialization transaction).

Non-zero Piece Count: Non-zero Print cycle count. Cleared to zero during Initialization transaction. Incremented by each Indicium transaction that dispenses non-zero revenue amount.

p: DSA parameter used in signature verification, signature generation and keys generation. Loaded during initialization (Initialization transaction).

Previous Funding Date/Time: The date and time of the most recent Funding transaction. Stored at the end of each Funding Transaction.

Previous Funding Postage Value: Amount of postage added to the descending register during the most recent Funding transaction. Stored at the end of each Funding Transaction.

q: DSA parameter used in signature verification, signature generation and keys generation. Loaded during initialization (Initialization transaction).

Software ID: An ID code to be inserted into the indicium. Stored in software Flash memory when the flash is created at the Neopost Ind. factory.

Transaction ID: An ID code identifying each transaction.

Watchdog Increment: Number of days between inspection time-outs. This value is used to initialize the Watchdog Timer during an Audit Transaction. Value is initialized by Authorization and Update Registration Transaction.

Watchdog Timer: Number of days to next watchdog time-out. Initialized to the watchdog increment during an Authorization Transaction. Reinitialized to the same value by an Audit Transaction.