



SPEC 272 / S

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

N30i/N30ig - 135/136

Meter

V.VAISSIERE / F. TORCHE

 Research & Development		SUIVI DES REVISIONS APPROBATION, DIFFUSION		SPEC.272	
ORIGINE :					
SUIVI DES REVISIONS :					
		See "Changes History", page 3			
Ce document annule et remplace le précédent qui doit être détruit. Les versions précédentes peuvent être consultées au service Documentation.					
VERIFICATION - APPROBATION					
		<i>DATE</i>	<i>VISA</i>	<i>NOM</i>	
Le rédacteur				Véronique VAISSIERE	
Chef de projet				Patrick BLANLUET Fabien TORCHE	
Chef du service Electronique				Bernard MOURGUES	
Directeur Recherche & Développement				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 review)
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 V30.13 submission
P	14/12/05	VV	Update for N30I / 135 FIPS submission
Q	10/04/06	VV	Update due to M. Downs/INFOGARD remarks
R	03/10/06	VV	Update due to M. Downs/INFOGARD remarks
S	17/11/06	VV	New meter version – V50.2 and change the ink color

Table of Contents

1. Introduction.....	5
1.1. Scope.....	5
1.2. References.....	5
1.3. Glossary of Names and Acronyms.....	6
2. Security Level.....	8
3. NSD Overview.....	9
3.1. Components & Communication Interfaces.....	9
4. Roles.....	11
4.1. Neopost Administrator.....	11
4.2. Customer.....	11
5. Services.....	13
5.1. Authorization (Registration).....	13
5.2. Generate Indicium.....	13
5.3. Funding.....	14
5.4. Audit.....	15
5.5. Withdrawal Transaction.....	16
5.6. Update Registration Transaction.....	16
5.7. Other Services.....	17
5.7.1. Status.....	17
5.7.2. Self-Tests Transaction.....	17
5.7.3. Adjust RTC Transaction.....	17
5.7.4. Zeroization.....	18
5.8. 1 Roles Vs. Services Matrix.....	18
6. Security Rules.....	19
6.1. General Requirements.....	19
6.2. Power-Up Security Requirements.....	19
6.2.1. CPU and Volatile Memory Self-Tests.....	19
6.2.2. Cryptographic Self Tests.....	20
6.2.3. Conditional Self Tests.....	21
6.3. Cryptographic Operations.....	21
6.4. Key Management.....	22
7. Physical Security.....	23
8. Critical Security Parameters (CSP's).....	24
Definition of CSP Modes of Access.....	26
9. Other Access Controlled Data Items.....	28

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 an electronic device developed by Neopost which stores customer postal revenue. 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 a 2D barcode, which is referred to as an indicium, which can be determined to have originated from a particular meter at a particular point in time. The 2D barcode contains a cryptographic message authentication code (MAC), which provides data integrity and a mechanism to verify the imprint originator; the MAC algorithm employed is a 6-byte truncated 3DES - MAC.

The NSD contains an electronic memory which registers the amount of revenue remaining to be disbursed, as well as other critical security parameters (CSPs) necessary to secure and validate that revenue amount.

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

Hardware Part Number	Firmware Version	Commercial Models	Modifications
4127205W	4132525N V50.0 and 4134515L V50.02	N30i/N30iG/135/136	Software changes to support two indicia, new report for presorted mode (specific for Thesis machine).

Firmware and Hardware 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 presents the FIPS 140-2 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] Federal Information Processing Standards Publication 113
- [3] Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-2.
- [4] A comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, National Institute of Standards and Technology Special Publication 800-29.
- [5] Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2
- [6] Secure Hash Standard, Federal Information Processing Standards Publication 180-2
- [7] Federal Information Processing Standards Publication 46-3
- [8] ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation

1.3. Glossary of Names and Acronyms

3DES: Triple Data Encryption Algorithm

CSP : Critical Security Parameter

DAR: Device Audit Response

DSA: Digital Signature Algorithm

ECDSA: Elliptic Curve Digital Signature Algorithm

EDC: Error Detection Code

FIT: Factory Initialization Tool

FRAM: Ferro-electric random access memory is non-volatile but operates in other respects as RAM.

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 referred 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
- RAM:** Random Access Memory
- Request Message:** A message sent from the base to the meter requesting that a service be performed.
- Reset System:** It is the system used for the funding service with the meter (POC for Neopost and TMS for Hasler).
- 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.
- Transaction:** A series of one or more request/response message pairs comprising the performance of a single service.

2. Security Level

The NSD is a Multiple-Chip Embedded Cryptographic Module as defined in reference [3], Security Requirements for Cryptographic Modules, FIPS Publication 140-2. The NSD meets the overall requirements for FIPS 140-2 Level 3 security, as defined in reference document [3]. As per USPS requirements, the module, in addition to meeting the FIPS 140-2 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 140-2:

Security Requirements Section	FIPS 140-2 Security Level
Cryptographic Module	3
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Machines	3
Physical Security	3 + EFT**
Software Security	3
Operating System Security	N/A
Cryptographic Key Management	3
Cryptographic Algorithms	3
EMI/EMC	3
Self Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

N/A = not applicable

** Per USPS PCIBI-C requirement, the NSD shall provide a tamper detection wrapper with tamper response circuitry and shall also comply with FIPS 140-2 EFT requirements.

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 indicium onto an envelope or label with water fast blue 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 server (called the Reset 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 Reset System, and the Reset System debits the customer's account at Neopost. The customer ultimately pays Neopost for the revenue dispensed via the printed indicia.

The meter has only a FIPS mode; it does not support any non-FIPS mode of operation. The meter is not designed to mitigate specific attacks outside of FIPS 140-2 [3].

3.1. Components & Communication Interfaces

The Cryptoboundary is defined as the 16.3cm x 12cm printed circuit board (PCB) containing all components. The meter (FIPS 140-2 cryptographic module) consists of a main microprocessor, main working RAM, secured RAM (for cryptographic keys and other CSP storage), Flash memory, and FRAM (for postal related data storage) contained on a potted protected area within the PCB. The module meets FIPS 140-2 Level 3 physical security requirements by encasing the module components inside a tamper response 'envelope' and a hard, opaque epoxy potting material. The tamper response envelope is an active-circuit tamper mesh that protects the security related module components and corresponding circuit board from attack on all four sides. This tamper resistant wrapper is encased with an opaque, tamper evident hard epoxy, which forms the protected area within the cryptographic boundary of the module.



Figure 1 - NSD

The cryptographic boundary excludes all components outside of the potted protected area from the requirements of FIPS PUB 140-2. All excluded components and printed wiring assembly (PWA) are connected in such a way that:

- The component or PWA does not process CSPs, plaintext data, or other information that if misused could compromise the module
- The component or PWA is not connected with security relevant components of the module that would allow inappropriate transfer of CSPs, plaintext data, or other information that if misused could compromise the module
- A malfunction of a component could not lead to the release of CSPs, plaintext data or other information.
- All excluded components are for the handling of power, communication or printing control.

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’s interface is defined as the 96-pin serial interface external to the cryptographic boundary. This path provides the FIPS 140-2 interfaces for data input, data output, control input, status output and power.

The meter uses the following FIPS approved algorithms:

- DSA – DSS FIPS 180-2
- TDES – FIPS PUB 46-3, ANSI X9.52
- SHA-1 – SHS FIPS 180-2
- PRNG – ANSI X9.31
- TDES MAC

4. Roles

The cryptographic module shall support two distinct operators, the Neopost Administrator and the Customer. The module supports the Crypto Officer and User Roles as defined in FIPS 140-2 (reference [3]). Both the Crypto Officer and User roles are accessed by the Neopost Administrator; for the sake of brevity the remainder of this document shall reference the Neopost Administrator when discussing the Crypto Officer and User roles, as both authenticate to the module in the same manner and have access to the same set of services.

4.1. Neopost Administrator

The Neopost Administrator is responsible for providing services to initialize and maintain the parameters within the NSD that are necessary for interaction with the Neopost metering infrastructure.

The Neopost Administrator communicates with the meter by signing transactions using its unique Neopost DSA private key. This provides identity-based authentication to this role.

The following services are available to the Neopost Administrator:

Authorization	Prepares the module for a particular customer. Puts the module into the <i>Installed</i> state.
Update Registration	Updates customer's parameters within the module
Withdrawal	Puts the meter into the <i>Pending Withdrawal</i> state for removal out of service
Funding Transaction	Downloads funds into the module
Audit	Verifies the module's register values and resets the module's watchdog timer. If the module is in the <i>Locked-For-Audit</i> state it will return the module back into the <i>Installed</i> state
Get Status	Returns the status of the meter
Perform Self-Tests	Runs the self-tests
Adjust RTC	Allows the adjustment of the internal clock to match the particular time zone the module will be located in.
Zeroize	Performs zeroization of all CSPs

4.2. Customer

The Customer services are available on behalf of the Neopost Administrator. These services are made available by the Neopost Administrator and require the meter to be in its appropriate state:

General Postal Services	General non-security related services such as cleaning print heads, or setting postal rates etc. Also services requesting the Neopost Administrator authenticate to the meter and perform appropriate authenticated services (e.g. PVD, Authorization, Withdrawal)
Generate Indicium	Request to perform Indicium creation
Get Status	Returns the status of the meter
Perform Self-Tests	Runs the self-tests (by powering up the meter)
Adjust RTC	Allows the adjustment of the internal clock up to ± 3 hours
Load Slogans*	Load slogans into the meter

*Slogans are loaded into the module using a private Slogan DSA key and verified by the meter using its public counter part.

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. Authorization (Registration)

This service prepares the meter for installation at a customer site and notifies the Neopost Administrator to activate the customer's account. The Authorization service is obtained when the meter is either connected directly to the Neopost Administrator using the FIT or via the base's modem. All communication occurs over the meter's 96-Pin serial interface. The Authorization may only be performed by Neopost Administrator. The meter verifies the role by the DSA signature using the Neopost X.509 certificate, which was loaded by the Neopost Administrator during Initialization.

The Authorization transaction performs the following functions:

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

5.2. Generate Indicium

This service allows a Customer on behalf of the Neopost Administrator 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 Barcode data in the indicia includes a truncated 3DES MAC to allow them to be verified as valid indicia.
- The meter assembles the indicium, which includes the Barcode data and the signature.
- The meter sends the indicium to the base print head using a proprietary data format.

5.3. Funding

This service allows the Customer on behalf of the Neopost Administrator to add more revenue to the meter so it can generate more indicia. The Customer instructs the base to begin a Funding transaction. Note that the Customer only requests that the service be initiated. The Neopost Administrator actually performs the Funding service. Funding is obtained when the meter and Neopost Administrator 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 Reset 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 Reset System.
- The Reset 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 Reset System by the base in the previous step.
- If the message from the Reset System 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 Reset System 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 status 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.

5.4. 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 Administrator 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 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 Reset system.
- The Reset System 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. 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.

5.5. Withdrawal Transaction

Once the meter has been authorized to a particular customer's account, it functions on behalf of that account only. This means that when the meter is funded, that customer's account 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 transaction number generated by the meter. The Withdrawal field is signed using the meter's private DSA key and the message is sent to the base. The base forwards the Withdrawal field to the Reset System.
- The Reset System verifies the DSA signature on the Withdrawal field, analyzes 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 validating the Neopost Administrator. 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.

5.6. Update Registration Transaction

This service changes the parameters of the customer's account. The Update Registration service is obtained when the Reset System and the meter successfully engage in an Update Registration transaction. The Update Registration may only be performed by an entity operating as the Neopost Administrator, and this role is validated by requiring that the data transferred from the Reset System 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 Neopost Administrator 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

5.7. 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 as the Neopost Administrator requests the service to the Meter through the FIT. The base and meter engage in a transaction, which provides the service.

5.7.1. Status (Non-authenticated)

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.

5.7.2. Self-Tests Transaction (Non-authenticated)

This transaction is initiated by the base upon request by the customer, by sending a Self-Test message to the meter. The meter responds by performing the 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 CSPs. 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 140-2)
- Firmware Test (as required by FIPS 140-2 and described 6.2.2.2)
- Random Number Generator Tests (as required by FIPS 140-2)

5.7.3. Adjust RTC Transaction (Non-authenticated)

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.

5.7.4. 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.

Using a FIT the Crypto-Officer authenticates to the module and can send a Zeroize command to the module. The module will erase the Saved RAM, zeroizing all CSPs.

5.8.1 Roles Vs. Services Matrix

The following table summarizes the services available to the two roles supported by the meter.

Services	Neopost Administrator	Customer
Postal Services		
Authorization	X	
Generate Indicium		X
Funding Transaction	X	
Device Audit	X	
Withdrawal	X	
Registration/Update	X	
General Postal Services		X
Zeroization	X	
Load Slogans		X
General Services		
Get Status	X	X
Perform Self-Tests	X	X
Adjust RTC	X	X*

*RTC adjustment is limited to +/- 3h for customer

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 CSPs from fraud and component failure.

6.1. General Requirements

6.1.1. The meter shall contain a CSP 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 CSPs.

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 every time 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 fails, 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. RSA: The meter shall perform a "known answer" test in which the CPU shall calculate the RSA encryption (using OAEP method padding) 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.

6.2.2.1.3. RNG: The meter shall perform a "known answer" test in which the CPU shall exercise the DRNG by using known fixed parameters to generate a number and compare this number result to a known answer. 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 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.

6.2.2.1.5. 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.

6.2.2.1.6. SHA-1: The meter shall perform a "known answer" test in which the CPU shall generate a SHA hash and then compare hash result to a known answer. If the hash is correct, 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 32-bit 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 140-2 Level 3 module under FIPS 140-2 (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. 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 140-2 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. 3DES MAC is used as an integrity check on the data included in the barcode part of the indicium.

6.3.2. The meter shall employ the Digital Signature Standard (DSA) to verify signature on all messages containing CSPs 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. For any attempt to use the authentication mechanism then the probability that a random attempt will be accepted or that a false acceptance will occur will be at least 1 in 2^{80} (equivalent to at least 12×10^{23}). The DSA key is 160 bits and is considered to have at least 80 bits of strength. This is considerably more difficult to break than the 1 in 1,000,000 requirement.

6.3.4. The minimum time to generate an authentication shall be 100ms. For multiple attempts to use the authentication mechanism then the probability that a random attempt will be accepted or that a false acceptance will occur will be 1 in 2^{80} divided by 600 (equivalent to 2×10^{21}). This is considerably more difficult to break than the 1 in 100,000 requirement.

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

6.3.6. The meter shall employ the Neopost RSA public key to encrypt the 3DES secret key before sending it to the Reset System.

6.3.7. 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 using its internally stored version of the Neopost DSA public key.

6.4. Key Management

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

6.4.2. The Neopost US 3DES secret Key used to sign indicia is stored in plaintext 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 140-2 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 wrapped by a two-sided, flexible protective copper mesh. The copper mesh is connected to the module's tamper zeroization circuitry. It is powered by an internal 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 maximum 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 four sides.

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

8. Critical Security Parameters (CSP's)

This section lists all critical security parameters and gives a short description of each.

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* and *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.

3DES Secret Key: TDESMAC secret key generated during initialization (Initialization transaction). Stored in meter cryptographic module. Used to MAC indicia data.

The following table describes each CSP maintained by the PSD:

CSP NAME	DESCRIPTION
PSD DSA private key	The PSD DSA private key used to authenticate messages and data output from the PSD.
PRNG – Vn parameter	Seed value used for Random Number Generator
PRNG – Ko parameter	Parameter used to generate the two TDES keys (for PRNG)
3DES secret key	3DES secret key is used to authenticate the 2D barcode of postage indicium. (Reference 2).

The following table describes public key parameters of the PSD:

NAME	DESCRIPTION
DSA Slogan Public Key	Public key used for the verification of authenticated slogan used (and load) in the machine.
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 Registration (Authorization) transaction
Meter Public Key	Public key to be transmitted to Reset System during initialization (Initialization transaction)
Neopost X.509 Certificate	Contains DSA Neopost public key. Loaded during initialization (Initialization transaction). This key used for the verification of authenticated messages input from the Reset System.
Neopost X.509 V3 Certificate	The X.509 V3 certificate containing the server's RSA public key, necessary to encrypt the 3DES secret key. Loaded into the meter during the Initialization transaction

Definition of CSP Modes of Access

The section describes how CSPs are accessed by the services that can be activated by an operator. The modes of access are defined as follows:

- r The data item will be read for internal use.
- e The data item will be read and exported.
- w The data item will be updated directly from an imported value.
- m The data item will be modified to a value created by an internal process.
- z The data item will be zeroed.
- s The data item will be initialised to a starting value created by an internal process.
- i The data item will be initialised to a benign value (typically zeroed).

The following table summarises the relationship between all CSPs maintained by the PSD and the services that access them:

Service Name ▾						
CSP Name ▾	Registration (Authorization)	Funding	Audit	Withdrawal	Generate Indicum	Update Registration
PSD DSA Private Key	r	r	r	r		r
PRNG – Ko parameter						
PRNG – Vn parameter	m	m	m	m	m	m
3DES Secret Key					r	

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

Service Name ▸	Registration (Authorization)	Funding	Audit	Withdrawal	Generate Indidium	Update Registration
Public Key Parameter Name ▼						
DSA Slogan Public Key						
Meter X.509 Certificate	w	e	e	e		e
Meter Public Key	r	e	e	e		e
Neopost X.509 Certificate	r	r	r	r		r
Neopost X.509 V3 Certificate						

9. Other Access Controlled Data Items

This section lists data items that are not "Critical Security Parameters" 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 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 Reset 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).

Neopost X.509 V3 Certificate:

The X.509 V3 certificate containing the server's RSA public key, necessary to encrypt the 3DES secret key. Loaded into the meter during the 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).

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.