Security Policy, N18D Postage Meter

Neopost Industrie

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	Update for NIST submission
G	1/2/01	RS	Clarifications to address NIST Questions

Prepared By:

P. Blanluet

_____

Approved By:

_____

_____

Table of Contents

1. Introduction

The N18D is a small electronic device developed by Neopost which stores customer 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 N18D 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.

1.1. Scope

This document contains a statement of the security policy for the N18D. The security policy specifies the security requirements under which the N18D is designed.

1.2. Conventions

1.3. References

The following references provide additional information:

[1] Information Based Indicia Program, Performance Criteria for Information-Based Indicia and Security Architecture for IBI Postage Metering Systems, USPS, (draft dated 08/19/99 - document number unknown).

[2] reserved

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

1.4. Glossary of Names and Acronyms

FIT: Factory Initialization Tool

Base: The main part of the franking machine, which communicates with the N18D over the proprietary bus. Depending on the context, it may reference the electronics and software; or the electronics, the software and the mechanics.

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 N18D (Meter comes from metering).

N18D**:** A product designed by Neopost, which meters revenue on a per-use basis to a base device such as a personal computer.

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 and inspections.

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 and possibly readable and/or writable by an external device.

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

2. Security Level

The N18D is a Multiple-Chip Embedded Cryptographic Module as defined in reference [3], Security Requirements for Cryptographic Modules, FIPS publication 140-1. The N18D shall meet the overall requirements for FIPS 140-1 Level 2 security with Level 3 Physical Security, as defined in reference document [3]. As per USPS requirements, the module shall also meet FIPS 140-1 Level 4 requirements for environmental failure testing (EFT). The following table shows the security level requirement for each component of the meter:

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

3. N18D Overview

When the user 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 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. CPUs & Communication Ports

The meter consists of a main microcontroller and a cryptographic chip contained on a printed circuit board (PCB), enclosed in a tamper-evident enclosure. There are two serial communications channels, which extend outside the enclosure, called the primary and secondary serial ports.

The meter communicates with the base over the primary serial port using request / response message pairs called "transactions". Services are obtained from the meter by the base by requesting the proper transactions over the meter's primary port.

The secondary serial port has two uses. The main one, and the only one 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 port data is not interpreted by the meter and there are no services in the meter, which can be activated via data sequences applied on the secondary port. In fact any attempt to apply a command to the secondary port is logged as a fraud attempt. The second use is only active during the manufacturing process and is only available if the 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. Initial Manufacturing

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

As during this phase, the Meter is not really a full “US N18D”; this phase is considered outside the FIPS perimeter.

At the end of this phase, the Meter’s tamper evident enclosure is sealed, the Meter includes the US software and the US parameters (including the DES key and the User PIN code) and the programming security flag is set.

3.2.2. Initialization

Initialization of the meter is performed at the Neopost factory before the meter is placed in service. At this time, the meter's tamper evident enclosure is already installed but the tamper detection electronics are inactive.

The Crypto-Officer must install the meter on a special equipment (called FIT) to perform initialization. He then initializes the memories and cryptographic chip to prepare it to perform as an electronic revenue metering device (this includes the activation of tamper detection electronics and the change to the Meter status to preclude any further access through the secondary serial port).

3.2.3. Authorization

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 primary serial port, 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 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 tells the meter when to perform 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 factory from which it may be re-initialized and authorized to another customer.

4. Roles

The meter supports the following roles:

- Crypto-Officer Role
- Neopost User Role,
- Customer 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 initializing and authorizing the meter at the Neopost factory. Initialization and Authorization are the main services available to the Crypto-Officer. The Crypto-Officer role is only available at the Neopost factory through the FIT tool and with the Meter in uninitialized, Pending Installation or pending withdrawal states.

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

The Initialization service causes the meter to generate its public/private key pair, export the public key, load the Neopost X.509 certificate containing the Neopost public key, and activate the tamper detection electronics. The Crypto-Officer is responsible for obtaining and loading the Neopost X.509 certificate and for archiving the meter public key.

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

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

4.2. Neopost User Role

The meter supports a Neopost User role, for which the following services are provided:

- Authorization
- Funding
- Audit
- Update Registration
- Withdrawal

Whenever one of the above services is requested, the meter validates that the requester is a Neopost User by requiring that the service request be signed using the Neopost private key. The meter validates the signature using the Neopost public key stored in the Neopost X.509 certificate loaded by the Crypto-Officer during initialization.

Remark : The Neopost User Role is in reality played by the Neopost POC system.

4.3. Customer Role

The meter supports a Customer role, for which the following services are provided:

- Indicium
- Status
- Self Tests
- Read & Adjust RTC
- Read X.509 Certificates
- Request (trigger) the main transactions (Authorization, Funding, Audit, Update Registration, Withdrawal)

The verification to obtain services in the Customer role takes the form of a PIN code sent by the Base during the initialization. Once the correct PIN code has been received, the Customer 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) over the meter's primary serial port. The primary serial port of the meter must be connected to a serial port on a base.

The meter supports the following services:

5.1. 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 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,
- Instruct the Meter to activate tamper detection electronics,
- Instructs the meter to generate a public/private key pair,
- Instructs the meter to export its public key via the primary serial port,
- Puts the meter's finite state machine software into the *Pending Installation* state.
- RTC Initialization.

5.2. Authorization

This service installs the meter 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 port or when the FIT and the Meter successfully engage in an Authorization transaction over the meter's secondary serial port. The Authorization may only be performed by an entity operating in the Neopost User role or Crypto-officer role, and this role is validated 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 certificate 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.

5.3. 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 and if so,

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

- The meter assembles the indicium

- The meter prints the indicium on the document.

5.4. Funding

This service allows an entity operating in the Neopost User 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 Neopost User 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 key.

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

- The POC system, acting in the role of Neopost User, 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 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.

5.5. 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, operating in the Neopost User role, verifies the signature on the Device Audit field, analyzes the data contained therein, and generates a message containing a DAR (Device Audit Response) field. The DAR field contains the same transaction 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.

5.6. 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 key and the message is sent to the base. The base forwards the Withdrawal field to the Neopost POC system.

- The Neopost POC system, operating in the Neopost User role, verifies the 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 signature on the Withdrawal Response 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 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.

5.7. 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 Registration transaction over the meter's primary serial port. The Update Registration may only be performed by an entity operating in the Neopost User role, and this role is validated 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,

5.8. 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.

5.8.1. 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.

5.8.2. 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
- Cryptographic Algorithm Test
- Firmware Test (as described 6.2.2.2)
- Random Number Generator Tests

5.8.3. 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 manufacturing of the Meter.

5.8.4. Get X.509 Certificate Transaction

This transaction allows the Customer to read the contents of any of the 2 X.509 certificates stored in the meter's non-volatile memories.

5.8.5. Zeroization

In case of tampering (opening of the cover), the zeroization function is triggered which clears the Meter private key and the internal DES secret key.

5.9. Roles Vs. Services Matrix

Services	Roles		
	Crypto-Officer	**Neopost User**	**Customer**
Initialization	X		
Authorization	X	X	
Indicium			X
Funding		X	
Audit		X	
Withdrawal		X	
Update Registration		X	
Status	X		X
Self Tests			X
Adjust RTC	X		X
Read X.509 Certificates			X

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 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 *Faulted* 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 fault.

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 error mode and will indicate that the tests have passed by accepting the request from the Base to 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 error mode.

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 fault.

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 on crypto chip : The meter shall perform a "known answer" test in which the cryptographic module 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 error mode. This test also performs the required testing for the SHA-1 hash implemented in the crypto chip.

6.2.2.1.2. SHA-1 on main micro : The meter shall perform a "known answer" test in which the main micro shall calculate the SHA-1 hash for internally stored data fields and then compare the generated hash 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 error mode.

6.2.2.1.3. DES encryption on both chips : The meter shall perform a "known answer" test in which the cryptographic chip and the main micro shall both calculate the DES encryption for internally stored plaintext data fields of 8 bytes stored in the software Flash 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 error mode.

6.2.2.1.4. DES decryption on crypto chip : The meter shall perform a "known answer" test in which the cryptographic chip shall calculate the DES decryption for internally stored plaintext data fields of 8 bytes stored in the software Flash 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 error mode.

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

6.2.2.3. Statistical Random Number Generator Tests: These tests are not required for levels 1 & 2 under FIPS 140-1 (see reference [3]). However, as such tests are available as part of the support firmware provided with the cryptographic chip employed by the meter, then meter shall execute these tests upon request, and if any such test fails, the meter shall go into error mode.

6.2.3. Conditional Self Tests

6.2.3.1. Keys pair-wise consistency test : 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 cryptographic module uses the random number generator to generate a digital signature, the cryptographic module 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 error mode. 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 to sign all messages containing SRDIs to be reported to external devices. Such messages shall be signed using the meter's private key.

6.3.2. The meter shall employ the Digital Signature Standard 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 key shall not be made available via any communication port or by any other means under software control.

6.3.4. The meter shall not sign externally generated data received via either communications port 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 public key.

Discussion:

The requirement that the meter not sign externally generated data is to prevent someone from sending phony data to the meter, getting the meter to sign and return it, and then printing that as an indicium, thereby defrauding Neopost in a manner which would be difficult to detect or prove.

6.4. Key Management

6.4.1. The meter's private key shall be generated during initialization transaction, stored in plain text form inside the crypto-processor chip, and shall not be accessible by any means without leaving evidence of tampering.

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

6.4.3. The secret Key used to identify the main micro to the crypto chip shall be initialized during the initial manufacturing process module (in plain text form through electronic communication). It is stored inside the crypto chip and the main micro memory in plain text form, and shall not be accessible by any means without leaving evidence of tampering.

7. Security Relevant Data Items (SRDI's)

This section lists all security relevant data items 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).

DES secret key: key used only internally at power-up to identify the main micro to the crypto chip. This internal authentication is an added security feature for the zeroization scheme. Loaded during initial manufacturing both into the Meter's memory and crypto chip EEPROM.

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 faults.

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. Loaded during initialization (Initialization transaction).

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

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

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

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

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.

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.

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.

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.

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 Transaction.

This section lists data items that may or may not be considered as "Security Relevant" and gives a short description of each.

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

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

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

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.

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

Transaction ID: An ID code identifying each transaction.