LYNKS METERING DEVICE

SECURITY POLICY

SPYRUS®

LYNKS Metering Device

Security Policy

Document # 540-100022-A8
Revision A8
29 July 1998

SPYRUS®

<info@spyrus.com>
<http://www.spyrus.com>

TRADEMARKS

Contents

REVISION HISTORY

REV. #	DATE	DESCRIPTION
A1	20 May 98	Original
A2	26 May 98	Modified user role description
A3	29 May 98	Updated functions in roles
A4	01 Jun 98	Updated overview
A5	03 Jun 98	Table correction
A6	12 Jun 98	Added role-based authentication
A7	10 Jul 98	Add self test as a service that can be run by either role when device is powered up.
A8	28 Jul 98	Firmware clarification and state cryptographic functions for user.

1 Introduction

The LYNKS Metering Device (LMD) is a small electronic device developed by SPYRUS that secures and dispenses electronic postage revenue for a host computer. The LMD communicates with the host computer via a serial interface. A second serial interface on the LMD is used to transfer weight data received from a scale to the host computer. Revenue is dispensed from the LMD to the host computer in the form of a digitally signed indicium, a unique bit pattern which can be determined to have originated from a particular LMD at a particular point in time.

The LMD 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. In order to guarantee postage integrity, accurate downloading, and to prevent fraud, SPYRUS' public key cryptographic technologies are used for digital signature, certificate processing and electronic money metering.

The SPYRUS LMD has been selected for secure electronic postage and printing as part of the Neopost® PC Stamp electronic postage meter system. These new meters are part of the United States Postal Service (USPS) Information Based Indicia Program (IBIP) to replace older mechanical systems with new generation products for directly printing stamps on envelopes with PC laser and inkjet printers. The electronic stamp is in the form of a two dimensional bar code generated from the digitally signed indicium from the LMD.

1.1 Scope

This document describes the security policy for the LMD.

2 Overview

The LMD supports a set of commands that the host computer sends to it via the serial port in the form of messages. These messages can be categorized as transactions that initialize, authorize, fund, dispense revenue, audit, and withdraw the LMD from use. Some transactions may require that the host computer communicate with a remotely located Neopost funding computer, also known as the Postage-On-Call™ (POC) system. Figure 2.1 describes the major components that interact with the LMD.

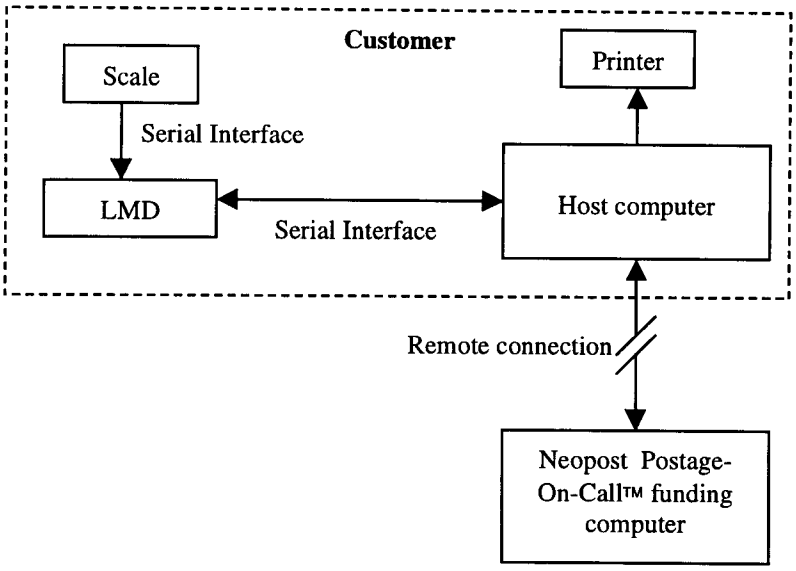

Figure 2.1 Postage Application Computer Interaction

The LMD is a multi-chip standalone module built upon the Fortezza Crypto Card, a FIPS 140-1 Level 2 certified cryptographic device. The LMD uses the same cryptographic processor as the Fortezza Card. The LMD supports the entire Fortezza API in addition to the metering interface. In the metering application, the user does not have ready access to the Fortezza API since it is utilized only for firmware update.

2.1 Self-Test

At power-up, the LMD always automatically performs an internal self-test to insure the integrity of the device. Any failure causes the LMD to enter into an error state in which no further processing occurs.

2.2 Firmware Update

Prior to any transaction processing, the LMD must be loaded with operational firmware created by SPYRUS. This capability is only available at SPYRUS or at a facility designated by SPYRUS. The result of loading the firmware is an un-initialized LMD that is ready for transaction processing. The firmware, which is digitally signed by SPYRUS, will be loaded by the LMD only if its signature can be verified. Only FIPS certified versions of the firmware should be loaded into the LMD. Any firmware modifications will require FIPS 140-1 re-validation of the LMD.

2.3 Initialization

Initialization of the LMD is the first transaction performed at the Neopost factory before the LMD is placed in service. At this time, special Neopost factory initialization software is used to initialize the LMD. The host computer loads digitally signed identification data and parameters. A serial number for the LMD and a certificate containing the Neopost public key is loaded at this time so that subsequent transactions, when required, can be validated by the LMD as originating from Neopost. The LMD generates a public-private key pair and returns the public key to the host computer.

2.4 Authorization

After the LMD is initialized, it must be authorized. Authorization prepares the LMD to operate in a particular customer's office. A certificate containing the LMD public key is loaded, as well as license identification for the customer. The LMD requires and verifies that Neopost has signed the messages received from the host computer in this transaction.

2.5 Funding

After authorization, the LMD must be funded before it can dispense revenue. The funding transaction adds revenue to the LMD. The customer uses the PC host computer to contact the Neopost POC computer via modem or network, and authorizes Neopost to debit the customer's account. After debiting the account, the Neopost POC computer returns a message to the PC host computer. The host computer then informs the LMD of the amount of the funding. Neopost digitally signs the funding transaction, which is verified by the LMD. At the completion of the funding transaction, the LMD waits for a subsequent audit transaction before incrementing its revenue register.

2.6 Indicium Dispensing

Once the LMD is funded, the user can request revenue to be dispensed via the indicium transaction. The indicium transaction causes the LMD to deduct the revenue amount from it's secure revenue registers, and send a signed bit pattern representing the revenue (called an indicium) to the host computer. The host then renders the indicium into a 2-D barcode format and prints it on a document. 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 LMD's revenue registers will be insufficient to satisfy any further requested revenue amounts. Revenue can be added by another funding transaction.

2.7 Auditing

Periodically during operation, the LMD must be audited. If the LMD is not audited within a specified amount of time, it will refuse to dispense indicia. The audit transaction requires communication with the Neopost POC system via the host computer. The LMD passes critical information to the Neopost POC, which returns a digitally signed message to the LMD that instructs it to continue printing of indicia. Any completed funding transaction amount pending is added to the LMD's revenue register at the completion of the audit transaction.

2.8 Withdrawal

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

3 Roles

The LMD supports the following roles:

- Crypto-Officer Role,
- User Role

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

3.1 Crypto-Officer Role

The Crypto-Officer is responsible for installing the firmware onto the LMD. Firmware updating is only available to the Crypto-Officer. The Crypto-Officer role is only available at SPYRUS or at a facility designated by SPYRUS.

The LMD validates the Crypto-Officer role by requiring a Personal Identification Number (PIN) in order to access it. A valid PIN must be passed to the LMD before it will accept any commands required to perform the firmware update service. In addition, the LMD verifies that the firmware is digitally signed by SPYRUS prior to loading it into the LMD. Only SPYRUS can generate and digitally sign the firmware that is loaded into the LMD. New firmware for the LMD requires FIPS 140-1 re-certification of the device.

The Crypto-officer is also responsible for the initialization of the LMD for use as a postage meter after firmware has been loaded, but prior to delivering the unit to the

customer. A valid PIN must be passed to the LMD to authenticate the Crypto-officer before it will process the initialization command.

The Initialization service causes the LMD to generate its public/private key pair, export the public key, and load the Neopost X.509 certificate containing the Neopost public key. The vendor performing the initialization at the factory is responsible for obtaining and loading the Neopost X.509 certificate and for archiving the LMD public key. The Neopost vendor public key is loaded into the LMD so that the LMD can validate subsequent transactions, when required, as originating from Neopost.

The Crypto-officer must also set the PIN phrase for the user, and may change the PIN phrase for the Crypto-officer. Only the Crypto-officer may change a PIN phrase.

3.2 User Role

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

- Authorization
- Funding
- Audit
- Indicium
- Withdrawal

The LMD validates the User role by requiring a Personal Identification Number (PIN) in order to access it. Some services input data into the LMD. The LMD further validates the requester by requiring that the service request be signed using the Neopost private key. The LMD validates the signature using the Neopost public key stored in the Neopost X.509 certificate loaded by during initialization.

Some of the LMD services only output data, such as revenue dispensing or the withdrawal of the meter from service. If one of these services is requested after the LMD has been initialized and logged into with the user PIN, the LMD simply performs the service. The messages sent to the LMD for these services are not digitally signed.

4 Services

The LMD provides services by exchanging messages between itself and a host computer over the LMD's primary serial port. The primary serial port of the LMD must be connected to a serial port on a host computer. The proper communication software must be installed on the host to access LMD services. The software is widely available to anyone who wants to purchase it, and there is no special security associated with obtaining or installing the software.

As previously stated, the services are obtained by exchanging messages between the LMD and the host computer. The messages are structured into groups called transactions. Each transaction consists of one or more request/response message pairs. A request message is a message sent from the host to the LMD. A response message is a message sent from the LMD to the host following the LMD's processing of the request message.

Services	Roles		Cryptographic Functions	
	Crypto-Officer	User	Signature Generation	Signature Verification
Self-test	X	X	X	X
Firmware Update	X			X
Initialization	X		X	X
Authorization		X	X	X
Funding		X	X	X
Indicium		X	X	
Audit		X	X	X
Withdrawal		X	X	

Figure 4.1 Services vs. Roles vs. Cryptographic Functions Matrix

The services supported by the LMD with the applicable roles, summarized in Figure 4.1, are described in the following subsections. The cryptographic functions performed by the LMD in the processing of each service is summarized in the figure and described in the following sections.

4.1 Self-test

The LMD performs self-test immediately upon power-up to insure the integrity of the device. Cryptographic and firmware checks are performed to insure that the device is operating properly prior to communicating with the host computer. Any failures will cause the LMD to go into a non-operational error state. No authentication of the Crypto-officer or user is required for this service.

4.2 Firmware Update

The firmware update service loads digitally signed firmware into the LMD. The firmware must be generated and digitally signed by SPYRUS. Firmware updating may only be performed by an entity operating in the Crypto-officer role. This role is validated by the LMD by first requiring authentication by entry of a PIN phrase. The following functions are performed when updating the LMD firmware:

- Authenticates the Crypto-Officer based upon PIN input,
- Verifies the signature of the firmware using the SPYRUS public key designated for the particular firmware load,

- Loads the digitally signed firmware if it is valid,
- Puts the LMD's finite state machine software into the *Un-initialized* state.

4.3 Initialization

Initialization causes the LMD to generate a public/private key pair, and to export the public key. The Crypto-officer performs initialization at the factory after firmware updating but prior to transferring the unit to a customer. The Neopost vendor certificate, which contains the public key used by the LMD to verify digitally signed messages from the Neopost POC, is loaded into the unit during initialization. The following functions are performed by the LMD during the Initialization transaction:

- Authenticates the Crypto-Officer based upon PIN input,
- Loads the Neopost vendor X.509 certificate, containing the Neopost public key, into the LMD,
- Loads the initialization parameters into the LMD,
- Instructs the LMD to generate a public/private key pair and return the public key via the primary serial port, and
- Puts the LMD's finite state machine software into the *Initialized* state.

The Crypto-officer then must obtain a certificate that will contain the public key returned from the LMD. The certificate will be loaded in the authorization transaction in a message that is signed by the Neopost vendor certificate loaded in this initialization transaction. Since the LMD identification is included in the indicium, an indicium generated outside of the operating hierarchy will be detected as the envelope stamped with the indicium is processed.

4.4 Authorization

This service installs the LMD at a customer site and notifies the Neopost POC system to activate the customer's account. The Authorization transaction is performed by a validated entity operating in the User role, which requires PIN authentication. The data transferred from the host to the LMD must be signed using the Neopost private key. The LMD verifies the signature using the Neopost X.509 certificate that was loaded during Initialization to validate the source.

The LMD performs the following in the Authorization transaction:

- Authenticates the User based upon PIN input,
- Verifies the signature of the input messages and processes only successfully validated authorization messages,

- Loads the input data from the authorization messages,
- Signs the return message with the LMD's private key to complete the authorization transaction.
- Puts the LMD's finite state machine software into the *Unfunded* state.

4.5 Funding

This service allows an entity operating in the User role, which is validated by the LMD using PIN authentication, to add more revenue to the LMD so it can generate more indicia. Note that even though the LMD is typically in the possession of a customer, the funding transaction contains data that must be signed using the Neopost private key. The LMD verifies the signature using the Neopost X.509 certificate that was loaded during Initialization to validate the source. This service is performed on behalf of the customer when the user's host computer communicates with the Neopost POC funding computer.

Funding is obtained when the LMD and host engage in a funding transaction as follows:

- Authenticates the User based upon PIN input,
- In response to a requested funding amount from the host, the LMD generates a message containing a funding request to be forwarded to the Neopost POC system. The message is signed by the LMD using the LMD's private key.
- The POC system validates the signature on the funding request and returns a message to the host. The host forwards the message to the LMD. The message contains either a funding response to authorize the funding, or an error to reject the funding. The message is signed using the Neopost private key.
- The LMD verifies the signature of the message from the Neopost POC using the public key contained in the Neopost X.509 certificate.
- If the verified message from the POC contains a valid funding response, the amount of the funding request is made pending. A pending amount is added to the revenue registers after an audit transaction. If the message contains an error indicating that the funding request was rejected, the LMD does not set the funding amount as pending.
- When funding is successful the LMD returns a message to the host which forwards it to the POC. The message contains a status and is signed using the LMD's private key. This completes the Funding transaction.
- The LMD transitions to the *Funded* state.

4.6 Indicium

This service allows a customer to obtain revenue in the form of indicia from the LMD. The customer operates in the User role, which is validated by the LMD using PIN authentication. The indicium service is obtained when, at the customer's command, the host and LMD engage in an Indicium transaction. The Indicium transaction performs the following functions:

- Authenticates the User based upon PIN input,
- The LMD checks to make sure that the accounting registers contain enough revenue to allow the requested indicium to be issued and if so,
- The LMD deducts the requested revenue amount from the secure accounting registers,
- The LMD assembles the indicium and signs it using the private key generated by the LMD during initialization,
- The LMD sends the signed indicium to the host computer.

4.7 Audit

The LMD 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 validated User may obtain the status of the LMD and reset the watchdog timer in the LMD. If the timer expires, the LMD will transition to the *Timed-Out* state, in which no further operation (in particular dispensing revenue) is permitted until an Audit transaction is performed. The Audit transaction also adds any pending funding amounts to the LMD revenue registers. Only a validated User, who has input a validated PIN phrase to the LMD, can perform the Audit transaction. The data transferred from the host to the LMD must be signed using the Neopost private key. The LMD verifies the signature using the Neopost X.509 certificate that was loaded during Initialization to validate the source.

- Authenticates the User based upon PIN input,
- The Audit transaction begins when the customer requests an Audit from the host. The host forwards the request to the LMD.
- The LMD generates a message containing an audit field. The audit field is signed using the LMD's private key and the message is sent to the host. The host forwards the message to the Neopost POC system.
- The Neopost POC, operating in the User role, verifies the signature on the audit field, analyzes the data contained therein, and generates a message containing an audit response field. The audit response field is signed using the Neopost private key and the message is sent to the LMD via the host.

- The LMD verifies the signature on the audit response field, thus validating the entity in the User role. If the signature and audit response data are valid, the LMD resets the watchdog timer accordingly. If the LMD was in the *Timed-Out* state, it transitions to the *Funded* state.
- If the LMD has a pending funding amount, then it is transferred to the secure revenue registers contained in the LMD. If the audit transaction contains an error, the LMD does not transfer any pending funding amount to the revenue registers.
- The LMD sends a response message to the host computer confirming that the Audit transaction is complete.

4.8 Withdrawal

Once the LMD has been authorized to a particular customer's account, it functions on behalf of that account only. This means that when the LMD is funded, that customer's account at Neopost is debited the amount of the funding plus any associated service charges. If that LMD is to be reused on a different account, it must be withdrawn from its present account and re-authorized for the new account. The Withdrawal transaction is performed by a validated entity operating in the User role, which requires PIN authentication.

- Authenticates the User based upon PIN input,
- The Withdrawal transaction begins when the customer requests a Withdrawal from the host. The host forwards the request to the LMD.
- The LMD generates a message that is signed using the LMD's private key and the message is sent to the host. The host forwards the Withdrawal message to the Neopost POC system.
- The LMD transitions to the *Initialized* state and awaits a new authorization transaction.

If the LMD must be re-initialized, then it must be returned to the factory. Only the Crypto-officer performing the Initialization process can obtain a new valid certificate for the LMD with a newly generated public key.