Lipman

Cryptographic Module

Security Policy

For NURIT 202 PIN PAD

Revision History Table

Version	Date	Revision Contents	Prepared by	Approved by
1.0	4/10/02	First Version	Aleksandr Grigoryev	Levent Kilic
1.1	4/24/02	Clarified definition of CO and technician role	Aleksandr Grigoryev	Andrey Tikhonov
1.2	5/06/02	Added the description of "Show status"	Aleksandr Grigoryev	Andrey Tikhonov
1.3	5/17/02	Added password changes and key zeroization	Aleksandr Grigoryev	Andrey Tikhonov
1.4	5/23/02	Added description of "DESMAC/TDESMAC" tests during self-test.	Aleksandr Grigoryev	Andrey Tikhonov
1.5	5/24/02	Deleted all appendixes, combined User and CO roles, updated Table 2 and 3, removed a few (non-security) services and updated some phrasing.		
1.6	2/9/03	Updated 8.3 to include CO/User. Removed Full Factory Test from requiring an Authenticated role in section 2.1, Table 7, and section 8.3	Rolf Salomon	
1.7	3/19/03	Minor clarifications of CO/User role, Added Product Introduction Section, Clarified Self-Test Service.	Rolf Salomon	
1.8	5/4/03	Changes to Copyright statement and Definition of DUKPT Future Keys.	Rolf Salomon	
1.9	6/15/03	Added section defining approved colors and country codes to Cryptographic Module Description.	Rolf Salomon	

Cryptographic Module Security Policy For NURIT 202 PIN PAD

This Technical Document is published by **Lipman Electronics Engineering Ltd.,** without any warranty. Improvements and changes to this Technical Document necessitated by typographical errors, inaccuracies of current information, or improvements to programs and/or equipment, may be made by **Lipman Electronics Engineering Ltd.** at any time and without notice. Such changes will, however, be incorporated into new editions or this Technical Document.

All rights of this document are owned by **Lipman Electronics Engineering Ltd**. This Technical Document may be reproduced only in its entirety without revision.

Contents

1. Cryptographic Module Description

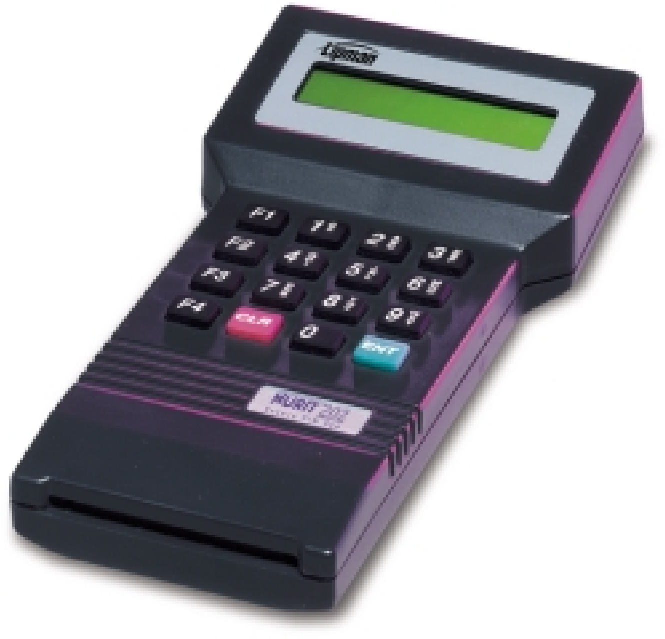

Figure 1 The NURIT 202 Secure PIN Pad

The NURIT 202 is an easy- to- use PIN Pad for diverse businesses enabling reliable PIN entry for both debit and credit transactions.

The NURIT 202 offers a high level of security, meeting stringent international requirements. The unit complies with ISO and ANSI encryption standards for PIN block encryption and key management.

Compact and lightweight, the NURIT 202 fits snugly into the palm of the hand, and can be easily and securely used. The rugged, field- tested design assures continuous, dependable service in even the most difficult environments. The unit is compatible with all Lipman NURIT Point Of Sale terminals, electronic cash registers (ECRs), and third party POS Systems.

Security Standards
Standards include DES (Data Encryption Standard), Triple DES, DUKPT (Derived Unique Key Per Transaction), and ANSI key management standards. The optional security shield assures complete user privacy and confidentiality.

FIPS 140-1 Validated Module Part Numbers
The NURIT 202 FIPS 140-1 validated module part number is 0202-XXX-M21-YYY where XXX is the country code in which the NURIT 202 is deployed and YYY is the color code for the enclosure.
The NURIT 202 is identical for each country code except for the possible change in language printed on the keypad. All country codes are valid.
The following color codes are valid:

CODE	COLOR
GRY	Gray
BLU	Blue
BLK	Black
RED	Red

2. Security Level

The cryptographic module meets the requirements for **Security Level 2** of **FIPS 140-1**.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module	**2**
Module Interfaces	**2**
Roles and Services	**2**
Finite State Machine	**2**
Physical Security	**2**
Software Security	**2**
Operating System Security	**N/A**
Key Management	**2**
Cryptographic Algorithms	**2**
EMI/EMC	**2**
Self Test	**2**

3. Roles and Services

The cryptographic module supports two operator roles. These operator roles are:

- Cryptographic Officer (CO) / User role
- Technician role

The cryptographic module separates roles using role-based operator authentication. A User / Cryptographic officer and a Technician operator must select required service and enter a password. If the password is correct, the operator will get the access to the service.

3.1 Technician Role

The Technician role provides the service necessary for testing and setting up the Pinpad. The technician has 2 (two) variable passwords to access services:

1. A password to enter in Diagnostic menu. This password may be changed by <CLR+F3>.
2. A password to enter in Diagnostic Level 2 menu. This password may be changed by <CLR+F2>

The Diagnostic Menu includes the following security services:

- *Run Diagnostic Self-Test:* This service allows the Technician role to select and run a Self Test. The available self-tests are
  - *One Time RAM test:* This self-test is a single RAM memory test. All keys will be zeroized during this test. If this test fails, the Pinpad will transition to the *Error state.*
  - *Continuous RAM test:* This self-test is a continuous RAM memory test. All keys will be zeroized during this test. If this test fails, the Pinpad will transition to the *Error state.*
  - *ROM checksum test:* This self-test is the ROM check sum test. All keys will be zeroized during this test. If this test fails, the Pinpad will transition to the *Error state.*
  - *Keyboard test:* This self-test is a keypad reliability test.
  - *Display test:* This self-test verifies that the display is working properly.
  - *UART Loop back test:* This self-test checks the receiver–transmitter circuitry.
  - *Cryptographic Algorithm test:* This self-test performs the known answer tests (KATs) for DES, DESMAC, Triple-DES and Triple-DESMAC algorithms. If any of these tests fail, the Pinpad will transition to the *Error state.*

- *Serial Number check:* This service allows the Technician role to displays the serial number stored in EEPROM.

The Diagnostic Level 2 Menu includes the following security services:

- *EEPROM test:* This service allows performing nonvolatile PROM test. All keys will be zeroized during this test. If this test fails, the Pinpad will transition to the *Error state.*
- *Change Between Master Session and DUKPT modes:* This service allows the Technician role to change between Master Session and DUKPT modes. See the **Cryptographic Key Management** section for details on these two modes of operation.
- *Erase Keys:* This service allows the Technician role to erase all of Master keys and DUKPT Future keys from EEPROM.

The password services:

- *Change Manual Diagnostic password:* This service allows the Technician role to change the password for the Manual Diagnostic Menu.
- *Change Diagnostic Level 2 password:* This service allows the Technician role to change the password for the Diagnostic Level 2 Menu.

3.2 Cryptographic Officer and User Role

The Cryptographic Officer and User roles share the same services. The Cryptographic Officer / User role provides access to the services necessary to work with keys and interact with the Terminal. In addition to the key management service the CO/User has access to all the Technician role services as defined in section 'Technician role'.

There is the individual password for the CO/User role. The CO/User can change it by <CLR+F1> (see below the *Change CO Password*).

This includes the following security services:

Pinpad Activation: This service allows the CO/User to activate the Pinpad. While the Pinpad is inactive, the Com-port is disabled. To activate the Pinpad, the CO/User should enter the CO password.

Manual Master key Entry: This service allows the CO/User to enter the Pinpad's Master keys manually. The CO/User first selects the index of the master key. If a key already exists in the selected index, the Pinpad requires the old Master key to be input. If the entered master key matches the old Master key or if the selected index was empty, the Pinpad allows a new master key to be entered.

Change CO Password: This service allows changing the CO password stored in EEPROM.

CO/User services available over the Serial Link include:

Transfer Master Key: This service allows the Crypto Officer / User role to enter a master key into the module. If the Pinpad is in DUKPT mode, this service selects Master Session mode.

Check Master Key: This service allows the Crypto Officer / User role to check for a Master Key in a particular index. This service is disabled when the module is in DUKPT mode.

Select Master Key: This service allows the Crypto Officer / User role to select the active Master Key. This service is disabled when the module is in DUKPT mode.

Request PIN Entry: This service allows the Crypto Officer / User role to direct the Pinpad to accept a PIN from the keypad. This entered PIN is formatted into a PIN block. If the Pinpad is in DUKPT mode, the PIN block is encrypted with a pre-existing Future Key. If the Pinpad is in Master Session mode, the Request PIN Entry service request should include a protected working key. In Master Session mode, the PIN block is encrypted with the provided Working Key or the current Master Key if no Working Key was provided.

Load Initial Key Request: This service allows the Crypto Officer / User role to load the DUKPT Initial Key. If the Pinpad is in Master Session mode, this service selects DUKPT mode.

Request MAC: This service allows the Crypto Officer / User role to direct the Pinpad to generate and output a MAC for provided data.

Run Self-Tests: This service allows the Crypto Officer / User role to run all the known answer tests (KATs for DES, DESMAC, Triple-DES and Triple-DESMAC algorithms), the Display test, the one time RAM test, the continuous RAM test, the ROM checksum test, the keyboard test, the serial number check, and the UART Loop back test.

3.3 Show Status

Show Status is a service, which allows the operator to identify the status of the Pinpad by external indications like displayed messages, sound signals or a combination of sounds and messages in accordance with the selected role.

Table 2. Show status

Screen Messages	Beeps	Tech	CO / User
TOTAL $ X.XX Enter your P.I.N	1		X
To end hit <ENT> *****			X
PINPAD INACTIVE: ……	1		X
Pinpad ACTIVATE: PINPAD ACTIVATE: FAILURE SUCCESS			X
Diagn. Password: …..	1	X	X
Diagn.L2 Psword: ………	1	X	X
CO Password: ……	1		X
SELECT FROM MENU 0: Togl. PAD/PAL 5: Display test 1: One RAM test 6: Show serial # 2: Cont RAM test 7: SUART loop 3: ROM check sum 8: Algorithm test 4: Keyboard test	1	X	X
Keys will be or Erasing keys or Erasing keys Erased!CLR-abort In progress SUCCESS		X	X
Data will be or Erasing data or Erasing data Erased!CLR-abort In progress SUCCESS		X	X
RAM test: or RAM test: or RAM test: In progress SUCCESS FAILURE	2-3	X	X
ROM test: or ROM test: or ROM test: In progress SUCCESS FAILURE	2-3	X	X
KEYBOARD TEST or KEYBOARD TEST (Hit any keys) XXXXXXXXXXX	1	X	X
,,*,*,*,*,*,*, or 000000000000 or ___________ ,*,*,*,*,*,*,*,* 000000000000 *	1	X	X
SERIAL NUMBER: XXXXXXXXXXX	1	X	X
SUART test: or SUART test: or SUART test: In progress SUCCESS FAILURE		X	X
SELECT FROM MENU 1: DES 2: 3-DES	1	X	X
DES algor.test: or DES algor.test: or DES algor.test: In progress SUCCESS FAILURE	2-3	X	X
3DES algor.test: or 3DES algor.test: or 3DES algor.test: In progress SUCCESS FAILURE	2-3	X	X
EEPROM test: or EEPROM test: or EEPROM test: In progress SUCCESS FAILURE	2-3	X	X
Keyboard test:		X	X

Press XX			
SELECT FROM MENU 1: EEPROM test 2: Set Language 3: Set baudrate 4: Ms/Ss - DUKPT 5: Erase keys 6: Keys password	1	X	X
SELECT FROM MENU or SUCCESS 1: ENGLISH Language set. 2: RUSSIAN 3: HEBREW 4: LATVIAN 5: TURKISH	1	X	X
SELECT FROM MENU or BAUDRATE 0: Show baudrate XXXX 1: Set to 300 2: Set to 600 3: Set to 1200 4: Set to 2400 5: Set to 4800 6: Set to 9600 7: Set to 19200	1	X	X
Now using Ms/Ss (DUKPT) Yes: Hit <ENT> Change to DUKPT (Ms/Ss)? No: Hit <CLR>	1	X	X
SUCCESS Now using DUKPT (Ms/Ss)		X	X
Full test code: ….	1	X	X
RS-232 test: or RS-232 test: In progress FAILURE	3	X	X
RS-232: Ok Next test: <CLR>		X	X
LCD display test or If LCD is Ok Watch with <Ent> hit <9>: else <CLR>		X	X
Display test: Failure	3	X	X
Manufacture test Success	2	X	X
Enter new psword or Reenter password …… ……	1		X
Password changed or ERROR Success Psw mismatch	1		X
Enter Master key or Enter old Mkey X Number (0 to 9) Digit #X:	1		X
Enter new Mkey X or ReEnter new Mkey Digit #X: Digit #X:	1		X
SUCCESS or ERROR New Mkey entered Mkey mismatching			X

3.4 Full Factory Test

Full Factory test: This service allows an operator who has not assumed a role to perform the full factory test set, which is includes the ROM, RAM, EEPROM, COM-port, keyboard and display tests. All secret data will be zeroized, and the Pinpad will become inactive. If the test fails, the Pinpad will transition to the Error state.

4. Software Security

All software is implemented using a high-level language C, C++, except that Start-up module, ROM test, RAM test and registers setting up are written on Assembler language.

5. Physical Security

5.1 Embodiment of cryptographic module

The entire Nurit 202 Pinpad is defined as a multi-chip standalone cryptographic module. There is one RJ11C port:

- pin 1 - Ground
- pin 2 – RxD (Received Data)
- pin 3 – TxD (Transmit Data)
- pin 4 - +9V DC

The interface is an RS-232 port with 7 bit data, ‘Even’ parity and 1 stop bit (7E1) data format. The baud rate can be set from 300 bps to 19200 bps using menu options.

5.2 Cryptographic Boundary

The cryptographic boundary for the Nurit 202 Pinpad is defined as the outer case of the device.

5.3 Physical Security Mechanisms

The Nurit 202 Pinpad is produced as a printed circuit board using production-grade quality integrated chips and components. The circuit board is passivated using a hard epoxy coating. The Epoxy coating is opaque within the visible spectrum.

The module is entirely contained within a hard plastic production-grade casing. The case is sealed with a hard acrylic adhesive in four places:

- The bottom and top end of the enclosure
- A screw that holds the two halves together which is also adhered by the adhesive material
- A plastic cube extruding from the back enclosure half and adhered to the front enclosure half.

The adhesive is stronger than the ABS case ensuring tamper evidence by forcing the visible breakage of the case in case of forced opening of the enclosure. To further ensure visible breakage of the case to occur in case of forced opening, two grooves have been provided in the front enclosure half to guide any breakage to occur across the keypad, evident to the end-user.

6. Definition of Security Relevant Data Items

The following are security relevant data items contained in the module:

- Checksum: This is a Checksum of the ROM, stored in the EEPROM. The checksum is compared with the ROM checksum during the power-up self-test. If the result is negative, all information stored in the EEPROM will be erased.
- CO Password (COP): This is a CO password.
- Manual Diagnostic Password (MDP): This is a technician password to enter to Diagnostic Menu.
- Diagnostic Level 2 Password (DL2P): This is a technician password to enter to Diagnostic Level 2 Menu.
- Key Serial Number Register (KSNR): This is variable stored in the EEPROM. It consists of an Initial Key serial number register and Encryption counter. At first it is received from the Host then is changed by each transaction.
- Future keys (FK): These are 21 keys for the DUKPT mode. They are calculated by using Initial key and Key Serial Number Register. The future keys are not directly generated within the module, rather they are agreed upon using the DUKPT key agreement protocol.
- Working key (WK): This is public key for Master Session mode received from the Host.
- Master key Index: This is a Master key number of memory location. The value of the Index may change from 0 to 9.
- Master keys (MK): These are 10 keys for the Master Session mode. They may be entered manually or received from the Host.

7. Definition of SRDI Modes of Access

Table 2 defines the relationship between access to SRDIs and the different module services. The modes of access shown in the table are defined as follows:

- Generate Checksum: This operation takes the checksum of ROM and stores it into EEPROM.
- Verify Checksum: This operation compares Checksum with the ROM checksum during power-up self-test.
- Change COP: This operation changes the CO password.
- Verify COP: This operation verifies the CO password.
- Destroy COP: This operation erases the CO password from EEPROM.
- Change MDP: This operation changes the technician password of Diagnostic Menu.
- Verify MDP: This operation verifies the technician password of Diagnostic Menu.
- Destroy MDP: This operation erases the technician password of Diagnostic Menu from EEPROM.
- Change DL2P: This operation changes the technician password of Diagnostic Level 2 Menu.
- Verify DL2P: This operation verifies the technician password of Diagnostic Level 2 Menu.
- Destroy DL2P: This operation erases the technician password of Diagnostic Level 2 Menu from EEPROM.
- Update KSNR: This operation changes Key Serial Number register for DUKPT mode.
- FK Agreement: This operation uses DUKPT to agree on new Future keys.
- Destroy FK: This operation erases all Future keys from EEPROM.
- Unwrap WK: This operation decrypts Working key using current Master key.
- Select MK Index: This operation selects current Master key.
- MK entry: This operation initializes or changes one of Master keys.
- Destroy MK: This operation erases all Master keys from EEPROM.

8. Service to SRDI Access Operation Relationship

Table 3. Services Versus SRDI Access

User Services	SRDI Access operation																Role	
	Generate Checksum	Verify Checksum	Change COP	Verify COP	Destroy COP	Change MDP or DL2P	Verify MDP	Verify DL2P	Destroy MDP or DL2P	Update KSNR	FK Agreement	Destroy FK	Unwrap WK	Select MK Index	MK entry	Destroy MK	CO role / User	Technician role
Pinpad Activation				X													X	
Manual Master key Entry				X										X	X		X	
Change CO Password			X	X													X	
Transfer Master Key															X		X	
Check Master Key																	X	
Select Master Key														X			X	
Request PIN Entry										X			X				X	
Load initial Key Request											X						X	
Request MAC																	X	
Run Self-Tests	X	X			X				X			X				X	X	

Run Diagnostic Self-Test	X	X			X		X		X			X				X	X	X
Serial Number check							X										X	X
EEPROM test								X				X				X	X	X
Change Between MS and DUKPT modes								X									X	X
Erase Keys								X				X				X	X	X
Full Factory test					X				X			X				X		
Change Diag. Password						X	X										X	X
Change Diag.L2 Password						X		X									X	X

9. Cryptographic Key Management

There are Pinpad modes: DUKPT and the Master Session. All keys cannot be output from the cryptographic module in plaintext form.

9.1 DUKPT Mode

There are 21 Future Keys. Future Keys are DES keys that are used to protect PIN blocks. Future keys are initialized with the Load Initial Key service. The Host sends an Initial key and Key Serial Number register. Future Keys are negotiated using these values.

9.2 Master Session Mode

There are 10 Master Keys.

Master keys may be entered or changed manually by the CO/User or over the serial link (using the Transfer Master key service). If the Master key is manually entered, a manual key entry conditional test is performed.

Master Session mode supports two algorithms – DES and Triple-DES. PIN blocks are encrypted using either a supplied Working Key (the Working Key is entered in protected form). If the supplied working key is all zeros, it encodes the PIN block using the current Master key.

9.3 Key Destruction (Zeroization)

Key destruction is performed by overwriting and invalidating all keys and other SRDIs in the following cases.

- When Checksum does not equal the ROM checksum during the power-up self-test.
- When the Pinpad transitions to the *Fatal Error state.*
- When the Crypto Officer/User or Technician erases all keys through the *Erase Keys* service.
- When one of the following services is run: One Time RAM test, Continuous RAM test, ROM checksum test, EEPROM test and Full Factory test. The Pinpad warns the operator before entering any service that results in zeroization.

10. Cryptographic Algorithm

The cryptographic module employs the DES (Data Encryption Standard) and Triple-DES cryptographic algorithms.

11. Self-Tests

11.1 Power-up self-test

A self-test is performed when the Pinpad is powered up. It consists of the following tests:

(a) DES cryptographic algorithm test

This test performs Known Answer Tests for the DES and DES MAC (Message Authentication Code) algorithms.

(b) Triple-DES cryptographic algorithm test

This test performs Known Answer Tests for the Triple-DES and Triple-DES MAC (Message Authentication Code) algorithms.

(c) Internal ROM test

The internal ROM is tested calculating CRC and comparing the result to a calculated value that was loaded when the module was factory initialized.

(d) Internal RAM test

This test performs full RAM test.

(e) Internal EEPROM test

The PROM is tested writing, reading and comparing data array.

In the event that any of the above tests fail, the self-test will transition to the Error state. This state halts all further operation by entering an infinite loop that performs no operations. The exit from it is only one - power off.

11.2 Manual Key Entry Test

When Master keys are manually entered into a Pinpad, the keys use duplicate entries in order to verify the accuracy of the entered keys. The Pinpad verifies duplicate entries and displays the success or failure of the entry process.