UniGuard-V34

Cryptographic Module Security Policy

Rev. 1.16

Communication Devices Inc.
One Forstmann Ct.
Clifton, NJ 07011
USA
Phone: 973 772 6997
Fax: 973 772 0747
Internet: support@commdevices.com

Table of Contents

Table of Figures

1 Introduction

1.1 Scope

This document sets forth the security rules under which the UniGuard-V34 cryptographic unit will operate, including rules derived from FIPS 140-1.

1.2 FIPS 140-1 Table of Security Levels

Security Requirements	FIPS 140-1 Security Level
Cryptographic Modules	2
Module Interface	2
Roles & Service	2
Finite State Machine	2
Physical Security	3
Software Security	3
Operating System	N/A
Key Management	2
Cryptographic Algorithms	2
EMI/EMC	2
Self Test	2
Overall Level	2

Figure 1 *FIPS 140-1 Table of Security Levels*

1.3 Related Documents

- UniGuard-V34 Manual
- Front End Loader Manual
- FCC Test Report
- Finite State Machine

1.4 Glossary

3DES	Triple DES
ANSI	American National Standards Institute
ANSI X9.17	KEY Exchange Standard
CSM	Cryptographic Service Module
DES	Data Encryption Standard
EIA RS232	Modem/Host Interface
EIA RS232 Signals	DCD Data Carrier Detect DTR Data Terminal Ready RTS Request to Send CTS Clear to Send GND Signal Return (Ground) DSR Data Set Ready TxD Transmit Data RxD Received Data
Front End Loader	CDI Software to manage UniGuard-V34 Units
NIST	National Institute of Standards and Technology
PC	Personal Computer
PIN	Personal Identification Number
PTSN	Public Telephone Switched Network
VAC	Voltage Alternating Current
VAC CT	Voltage Alternating Current, Center Tapped

1.5 Out of Band Management

Out of Band Management refers to products that permit secured technician access to "Network Elements" (firewall, routers, bridges, sonet switches, servers etc.) via dial up telephone lines (not in the bandwidth of the network). By far, SNMP (the Simple Network Management Protocol) network management is the industry choice for managing wide area and local area networks. This is In Band Management access via the network. SNMP is easy to use and inexpensive. It has however one inherent weakness: SNMP management information travels the same network path as the data. It uses the same WAN and LAN routers, hubs and communications links. Communication is subject to interception and the same problems that the network is currently having. When the network goes down or is severely disrupted, SNMP traffic has no way to get between the managed device and the management workstation. Quite often when a "Network Element" goes down, it loses its network connection, which renders In Band Management useless. This is where the UniGuard-V34 module always works flawlessly for Out Of Band Management.

1.6 UniGuard-V34 Application

The UniGuard-V34 is designed to protect firewall/router console port access. The device was designed to overcome the weaknesses of RADIUS and TACACS+ for remote access. The problem of the firewall/router not being able to contact the RADIUS or TACACS+ server is eliminated by the UniGuard-V34 which stores its own database of up to 150 users right on board!

The UniGuard-V34 supports speeds up to 115.2 Kbps and has a built in V.34 internal modem and can be managed by the CDI's Front End Loader.

Full Triple DES (3DES) encryption is supported with another UniGuard-V34.

1.7 Block Diagram of Hardware Components

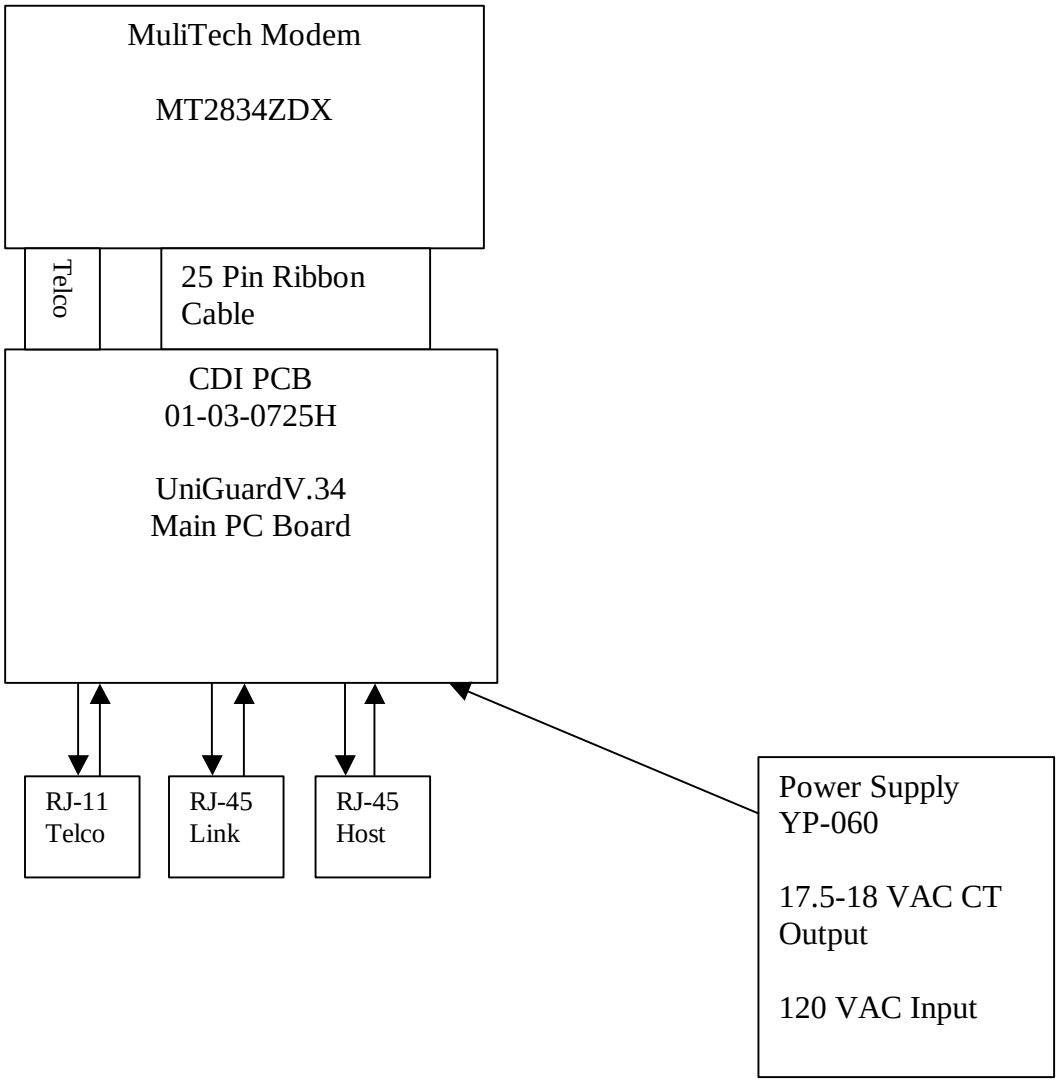

Figure 2 *Block Diagram of Hardware Components*

2 Description of Cryptomodule Boundary

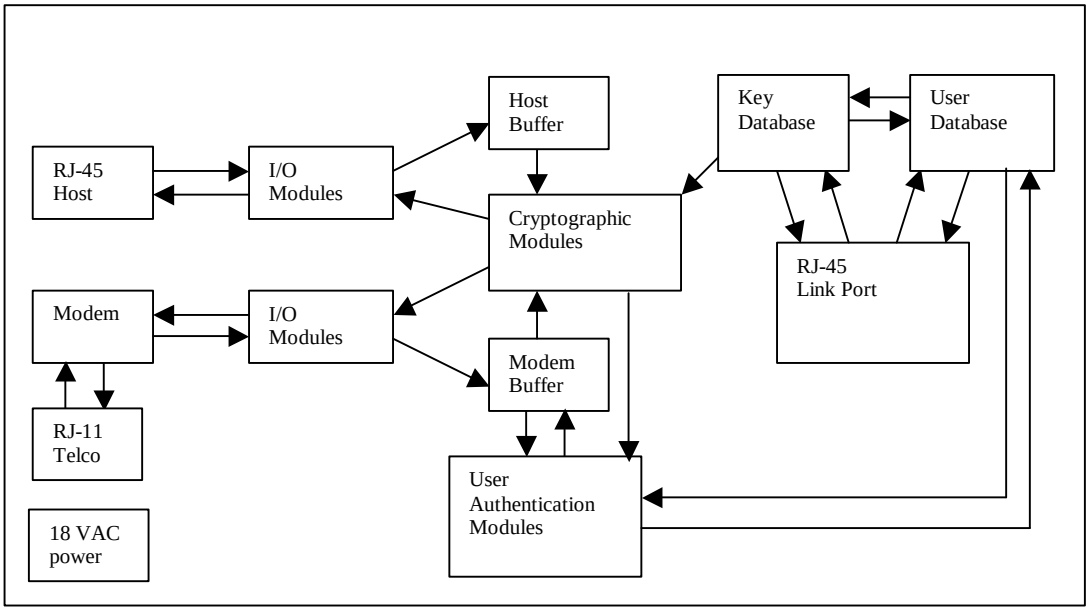

Figure 3 *Cryptomodule boundary*

2.1 Host Port RJ-45

Clear text data moves in/out of UniGuard-V34 through the RJ-45 connector Labeled Host. The RJ-45 port has the following Signals for EIA-232 interface with the RJ-45 cable and DB-25 connector. The signals are DCD, DTR, RTS, CTS, GND, DSR, TxD, and RxD.

2.2 Modem RJ-11

User **authentication** data, plaintext data, and encrypted data move in/out of the UniGuard-V34 through the modem. The RJ-11 provides standard 2 wire or 4 wire Telco interface to connect to Public Telephone Switching Network (PTSN).

2.3 Link Port

The Link Port is for use of the Crypto-officer when programming the UniGuard-V34 using the Front Loader program. This port is protected by a password set at the factory, which can be changed by the Crypto-officer.

2.4 I/O Modules

The I/O modules read and write data to the UART. Data read from a port is buffered in a circular buffer for the other modules. When a module is in control it will remove the data from the buffer. The two modules that remove data from the buffer are User Authentication module and the Cryptographic modules.

2.5 Power

Power requirements are 17.5-18.0VAC with center tap.

2.6 User Authentication

The User Authentication module will read data from the Modem Buffer to Authenticate the User. If the User ID is correct, the User Authentication module will initiate the Cryptographic Module. After the UniGuard-V34 is in Encrypted mode it will prompt and check to see if the password is correct for this user. This prevents passwords from being sent in the clear. If the password is correct for this user the UniGuard-V34 will pass control back to Encryption Modules for Encrypting/Decrypting data.

The User IDs and keys must be loaded in the UniGuard-V34 by the Crypto-Officer prior to a User Authentication, otherwise the User will be denied access and re-prompted to enter an ID. After three unsuccessful attempts, the UniGuard-V34 will disconnect the call.

2.7 Security Related Data Items

Security Related Data Items that are stored in the UniGuard-V34's tamper protected RAM are:

User IDs
Passwords
Token Keys
Token Pin Numbers
MAC Keys
Seed Keys

3 Physical Security

3.1 Physical Embodiment

The multi chip stand-alone cryptographic module consists of a number of IC chips mounted on a printed circuit board contained within a protected enclosure.

Figure 4 *UniGuard-V34 Front View*

3.2 Physical Security

3.2.1 Tamper Seals

Each of the screws (4) on the front and rear panels are covered with a “Tamper Seal” tape. This tape extends from the sides of the unit over the screws and bezel. This tape cannot be removed and replaced without it being mutilated to the point of being noticed.

Figure 5 *UniGuard-V34 with Tamper Tape seals on front and side of unit*

Figure 6 *UniGuard-V34 with Tamper Tape seals on rear and side of unit*

3.2.2 Multi-chip Cryptographic module printed circuit board.

The Multi-chip Cryptographic module printed circuit board is a two-layer fiberglass printed circuit board, which will have a modem attached to the top of the board

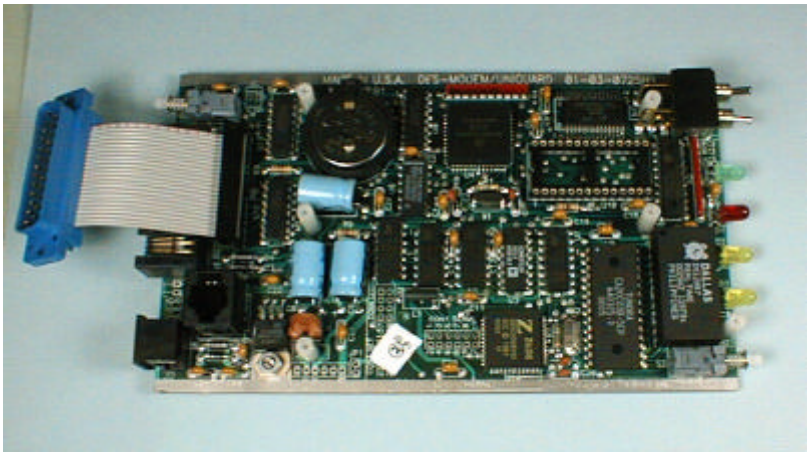

Figure 7 *Multi-Chip Cryptographic module printed circuit board*

3.2.3 The Modem Board

The Multi-chip Cryptographic module printed circuit board has the Modem mounted on top of the board and is inserted into the enclosure by means of extruded slides.

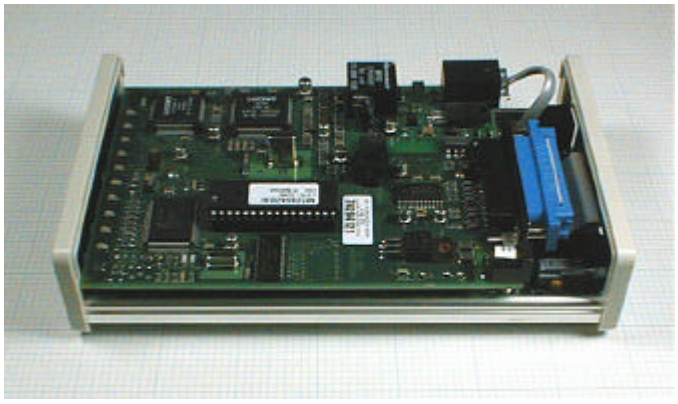

Figure 8 *Multi-chip Cryptographic module printed circuit board with modem mounted on top in an enclosure with Top removed (to show assembly).*

3.3 Enclosure

The enclosure consists of a steel top, an extruded aluminum bottom with front and rear covers with plastic bezel.

When assembled the steel top cannot be removed without first removing either the front or rear covers.

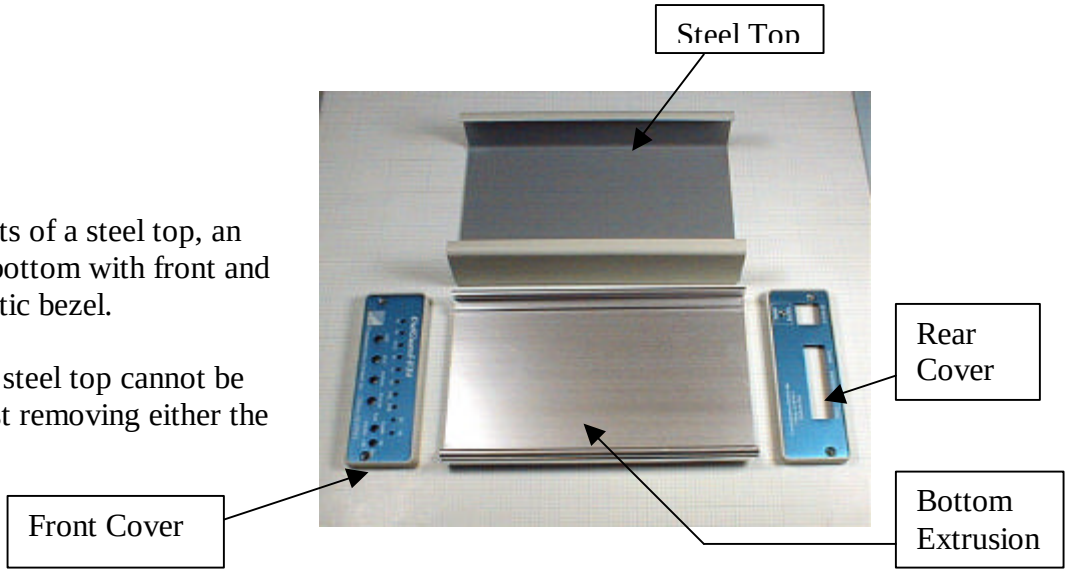

Figure 9 *Enclosure showing steel top, extruded aluminum bottom and front, rear covers. Not assembled.*

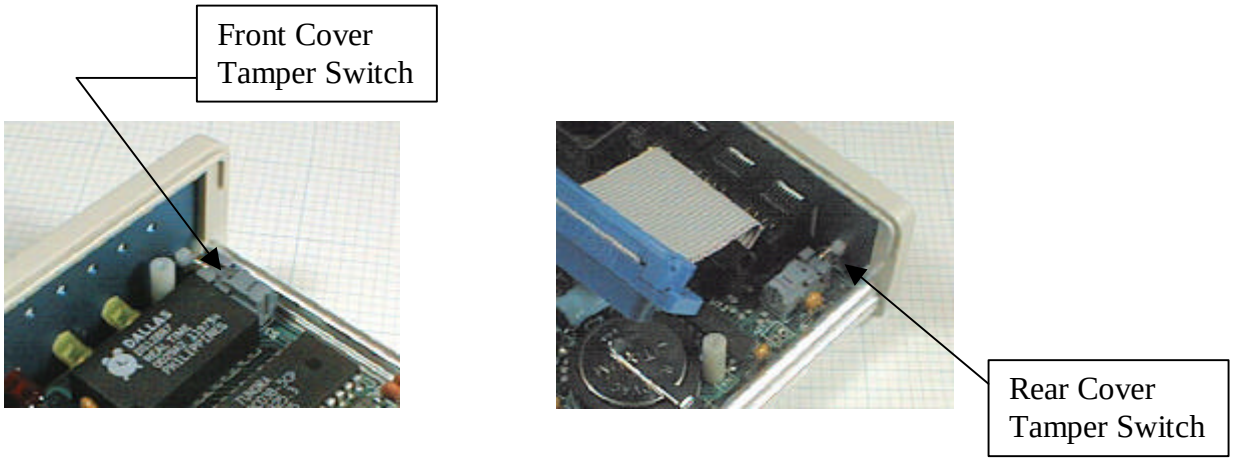

Figure 10 *Front and rear tamper switches, shown with the top cover removed and no modem installed. It is NOT possible to remove the Top cover or bottom extrusion without first removing either the front or rear covers.*

3.4 Tamper Switches

The circuit board contains tamper switches that will trip if an attempt is made to remove either the front or rear covers.

If either of these tamper switches is tripped the RAM containing all information including IDs, passwords and keys will be zeroed. The zeroization circuit will activate regardless if the unit is powered or not powered.

All IC chips are standard circuits.

4 Description of Firmware

The firmware that is executed in the UniGuard-V34 is written in 68HC11 ASSEMBLER. There is no commercial Operating System that is used in the product. The I/O code is Interrupt driven so that no input data is lost. There are timer interrupts that controls the state machine for User Authentication. This timer is based on 400 milliseconds, so every 400 milliseconds it checks and sees if a state process has to be executed. Each state will set up the next state to be processed on the next 400-millisecond timeout.

There is a real time clock that is used to control any timers in the code. Most timers are based on a 1 second granularity.

The code is divided into 4 different tasks. The tasks are the Monitor routines that Authenticates users, Cryptographic routines for encrypting/decrypting data, I/O routines for receiving and transmitting data to/from the host device and the modem, and the last task is house keeping which includes programming of the UniGuard-V34 by the Crypto-Officer with the Windows software package FrontLoader. With this software and serial port connection to the link port of UniGuard-V34 the Crypto-Officer can Add/Delete/Modify User and key information.

5 Roles And Services

5.1 Crypto-officer Role

The UniGuard-V34 supports only one Crypto-officer for the purpose of programming UniGuard-V34. The default password for the Crypto-officer is set at the factory. The Crypto-officer will use the Front Loader, a Windows package for programming purpose. The Crypto-officer will connect the serial port of the PC to the port labeled Link on the UniGuard-V34. This is the only port that can be used to program and/or modify the UniGuard-V34.

With Front Loader the Crypto-officer will be able to change the System Parameters such as the Host Port Speed, Data Bits, Parity, set time and date, change the Crypto-officer password, add/delete/modify Users and cryptographic keys. The keys will be entered in clear text, but reviewing of the keys will not be possible. The Crypto-officer will be able to review and delete audit trail activity of users with a CDI Front Loader program.

5.2 User Role

A User does not have access to the Link port of UniGuard-V34 that is used by the Crypto-officer. The User only has access to the modem and Host ports though the cryptographic modules of UniGuard-V34. To gain access to the host port the User must first authenticate himself through the modem, and UniGuard-V34 must enter encryption mode. Once he has authenticated he will be granted access to the host port. A user needs at minimum an ID and password to authenticate in UniGuard-V34's database. Along with the User ID and password, keys must have been loaded in the UniGuard-V34 database for the remote device.

5.3 Services

The services that UniGuard-V34 provides are

1. **Cryptographic operations**
   Encryption – UniGuard-V34 will encrypt the data before sending it out the Modem port to the PTSN. The purpose is to secure the data to protect against unauthorized viewing and/or use.

   Decryption - UniGuard-V34 will decrypt the data that it receives from PTSN through the modem port and deliver the data to the equipment connected to the host port. To be able to use the data that was sent from another UniGuard-V34,

it first has to be decrypted so that it is in usable form for the end user.

Message integrity - UniGuard-V34 uses the MAC function that is part of the X9.17 ANSI standard to protect against attack of the key exchange.

5.4 Key Management

Key and Parameter entry – All keys and parameters with the exception of the Session keys are entered into UniGuard-V34 through the Front Loader Windows package in clear text. The Session keys are entered encrypted by the DES or TDES Encryption keys.

Key output – Only Session keys can be output. These keys are wrapped with the Encryption keys before they are output. The review of the keys that have been entered will not be possible.

Key zeroization – When the Unit is physically opened up, there are tamper switches that will cause a short across SRAM, which in turn will zero out the keys. SRAM is battery backed up to save the keys and Users data in SRAM.

Key generation – The key generation process for creating the Session keys uses the ANSI X9.17 pseudo-random number generator.

5.5 Management functions

Audit – UniGuard-V34 saves up to 150 transactions for review with Front Loader. UniGuard-V34 saves time/date and the User that authenticated, and any attempts from an unauthorized User.

5.6 Cryptographic bypass

If the bypass switch is enabled through programming, the UniGuard-V34 can be placed in bypass mode so that data passes through in clear text. If the UniGuard-V34 is put into bypass; placing the toggle switch to disable, the red bypass LED will flash. When setting the switch back from bypass to secure the Unit will go through a power up sequence. During this time the LEDs go through their power up sequence of flashing DTR, DCD, and BYPASS LEDs.

5.7 Operator Authentication

The UniGuard-V34 by default will not Authenticate and/or operate in the clear text mode until the unit has been programmed with users, IDs, keys and system parameters. If an external user dials into the UniGuard-V34 with a remote UniGuard-V34 it will prompt you for an ID and password. After 3 unsuccessful attempts of entering IDs and passwords, the UniGuard-V34 will disconnect the call.

The default password should be changed after the Crypto-officer gains access and to prevent further access to the UniGuard-V34 programming menu of the Front Loader using this default.

If a user has been authenticated and the Unit is powered down and then powered back up, the Authentication session is terminated. When power is lost the modem will automatically disconnect from the phone line. The User will be required to dial in and Authenticate again after the Unit is powered up.

5.8 Identity Based Authentication

UniGuard-V34 provides Identity based authentication. The user must enter ID and password or some other form of challenge and response. If the user ID and password is valid, the User will cause the UniGuard-V34 to start Encryption Authentication with the remote hardware. Each remote UniGuard-V34 assigned to a User has a unique ID, which prevents other Users having the same ID. The following figure and description shows how operators can be authenticated.

	Authentication Mechanisms		
Identity	Challenge/Response with complete session encryption	Challenge/Response with a token	Challenge/Response without a token (bypass)
User	X	X	X
Crypto-Officer	X	X	X

Figure 11 *Authentication*

Challenge/Response with complete session encryption involves an operator that is prompted (Challenge) for a 6-digit User ID and 8-digit password. The User enters the information (Response) and attempts to log into a remote UniGuard-V34 using a local UniGuard-V34 device. Once the User has sent the User ID in the clear, the UniGuard-V34 generates a unique session key. The module looks up the User's encryption key based on the ID entered. The session key is sent encrypted to the User using that encryption key. If the User has the proper encryption key at the local unit, the session key can be decrypted and the User then sends his/her password to complete the

authentication. If the User ID and password are valid, the rest of the session will be encrypted and the User gains access to the module and the host PC connected to that module.

Challenge/Response with a token involves an operator that has possession of a token device. The token contains a time clock together with a User's encryption key. The key is used to encrypt the time, which is displayed in the LCD of the token. The user is prompted (Challenge) for the User ID and the encrypted displayed information when logging on. After entering this information (Response), the module looks up the user's encryption key and compares the encrypted information to the information generated by the module with the user's encryption key. A session key is generated and sent encrypted to the User using that encryption key. If the User has the proper encryption key at the local unit, the session key can be decrypted and the User then sends his/her password to complete the authentication. If the User ID and password are valid, the rest of the session will be encrypted and the User gains access to the module and the host PC connected to that module.

Challenge/Response without a token involves an operator that is prompted for a User ID and password from the remote module. The operator enters the authentication information and is granted access if it is correct. This occurs when the module is operating in the bypass mode and neither the authentication process nor the session is encrypted.

6 Operating System Security

The UniGuard-V34 does not employ an Operating System. The code that is executed in the UniGuard-V34 is stored in a FLASH chip in binary as executable format.

Use of the cryptographic module is limited to a single user at a time.

The UniGuard-V34 only provides for one user connection at a time, because the User must authenticate through the single modem to gain access to the cryptographic modules. Only the data that flows through UniGuard-V34 between the Modem and Host ports employs the cryptographic modules. Any other user attempting to dial in to the UniGuard-V34 will receive a busy signal.

Use of the cryptographic module is dedicated to the cryptographic process during the time the cryptographic process is in use.

By the statement above it is impossible to have multiple Users connected to the UniGuard-V34 at the same time because the UniGuard-V34 only interfaces to the PTSN with only a dialup modem, and the PTSN only allows for one connection per dialup circuit.

7 Key Management

7.1 Key Storage

The keys (DES or 3DES) are stored in a Pack BCD format in the UniGuard-V34's battery backup RAM. If power is lost to RAM and the batteries are dead the keys will be zeroed out. The battery circuitry includes two tamper switches, one located on the front panel and the other on the rear panel. If one of these switches is tripped by removing the front or rear panel, the keys will be destroyed. Pack BCD allows for 2 plain text characters to be stored in an 8 bit byte so each one of the 16 plain text keys are stored in 8 bytes of RAM. Triple DES requires 3 keys or 24 bytes of RAM.

The keys can't be changed once they are loaded into UniGuard-V34. Keys cannot be viewed. This protects the keys from being reviewed by unauthorized persons.

An ID and key (DES or 3DES) will be assigned to a UniGuard-V34 for a remote User. When this is done, only that key and ID can be used to connect to a Host UniGuard-V34 with encryption. If the key (DES or 3DES) or the ID is incorrect the UniGuard-V34 will drop the connection after 3 unsuccessful attempts. Each User has an ID, a password, and encryption keys to gain access to the Host port of UniGuard-V34.

All keys that are used for a cryptographic session between two UniGuard-V34s are generated by the host UniGuard-V34. The key generation process for creating the keys uses the random number generator to create the 3DES keys. The keys are distributed by using ANSI X9.17 key management with the use of the seed keys.

7.2 Key Destruction

Keys are destroyed when the front or rear cover of UniGuard-V34 is removed. The Crypto-Officer can also delete the keys stored in the module.

7.3 Key Archiving

UniGuard-V34 does not provide a means of retrieving keys in plain text for archiving purpose.

8 Cryptographic Algorithms

The Cryptographic Algorithm used in the UniGuard-V34 is DES or 3DES. 3DES is the preferred encryption algorithm of choice for the UniGuard-V34 and should be used instead of DES whenever possible.

8.1 Key Exchange Validation

Communication Devices Inc. uses ANSI X9.17 that has been NIST validated in 1992.

9 FCC Approval

UniGuard-V34 is FCC approved for Part 15 Class A.

10 Self Test

The self-tests are run every time UniGuard-V34 is powered up and upon certain conditions (bypass, session key generation, X9.17 pseudo random number generation, which is continuously run after power up self test). The self-test does not alter contents of UniGuard-V34. The device performs the following test:

- Cryptographic Algorithm Tests
- Firmware Checksum Test
- Random Number Generator Test
- Bypass Tests

11 Security Policy

UniGuard-V34 is designed and meets FIPS 140-1 Level 2 overall security requirements with hardware and software functionality meeting Level 3 security requirements.
The UniGuard-V34 operates only in a FIPS compliant mode and does not support a non-FIPS mode.

To gain access to the host device that UniGuard-V34 is protecting, the UniGuard-V34 must be in a cryptographic mode such that all data in/out of the modem to the PTSN is encrypted. The User must be programmed in the database and has rights to the host port of UniGuard-V34. Each User first has to be Authenticated before UniGuard-V34 goes into cryptographic mode.

A Host UniGuard-V34 will only authenticate in the cryptographic mode with a Client UniGuard-V34 that has the same X9.17 ID and keys that is in its own database.

The Unit is protected with 2 tamper switches so that opening the unit will zero out keys and User IDs in the database plus other data that is stored in SRAM. Opening the Unit with or without power being applied will zero out the SRAM.

12 NIST X9.17 Certificate

UNITED STATES
DEPARTMENT of COMMERCE

Certificate of Appreciation

Presented to

Communication Devices, Inc.

For a successful automated remote validation utilizing the NIST Key Management Validation System.

October 1992

Director, Computer Systems Laboratory