



National Security Agency

Fort George G. Meade, Maryland

SPECIFICATION NSA NO. 86-32
15 OCTOBER 1986

NATIONAL SECURITY AGENCY SPECIFICATION

WINDSTER

INTERFACE CONTROL DOCUMENT

(ICD)

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

SECTION	TITLE	PAGE NO.
1.	INTRODUCTION.	1
1.1	Scope	1
1.2	Terminology	1
1.3	Comments	1
1.4	NOTICE	1
2.	APPLICABLE DOCUMENTS	2
2.1	Standards	2
2.2	Specifications	2
2.3	Publications	2
3.	SECURITY CONSIDERATIONS	2
3.1	Controlled Cryptographic Items.	2
3.2	NSA Endorsement.	2
3.3	TEMPEST	2
4.	DESCRIPTION	2
4.1	Functional Description	3
4.2	WINDSTER Features	3
4.3	Architectural Description	3
4.3.1	Interface Ports	4
4.3.2	Internal Description.	4
4.4	Operating Modes	7
4.5	Key Processing Modes	7
4.5.1	Manual Key Loading	8
4.5.2	Black Key Processing	8
4.5.3	Over-the-Air Rekeying	8
4.5.4	Crypto Ignition Key (CIK)	8
4.5.5	Key Retention Mode	8
4.5.6	In-Band Rekeying	9
4.6	Power	9
4.7	Zeroize.	9
4.8	Alarm Status Processing	9
4.9	Error Reporting	9
5.	PRINCIPLES OF OPERATION	9
5.1	State Description	9
5.2	Cryptographic Operating Modes.	9
5.3	Cryptographic Synchronization	10
5.3.1	Pre-Synchronization Requirements	10
5.3.2	Initial Synchronization	10
5.3.3	Verification of Cryptographic Synchronization	11
5.3.4	Cryptographic Resynchronization While in Traffic	12
5.4	Backward Compatibility	12
5.5	Key Processing	12
6.	WINDSTER COMMANDS	13
6.1	COMSEC Command Language	13
6.2	Command Protocol	13
6.3	Command Listing	14
6.4	WINDSTER Command Descriptions.	15
6.5	Register Definitions	24
6.6	Service Requests - Error Messages	25

7.	INTERFACE SPECIFICATIONS	26
7.1	Detailed Interface Description	26
7.1.1	Fill Port	29
7.1.2	Housekeeping Port	29
7.1.3	Command/Status Port	30
7.1.4	Command/Status Control Port	30
7.1.5	Transmit Channel Input Port	30
7.1.6	Transmit Channel Output Port	31
7.1.7	Receive Channel Output Port	31
7.1.8	Receive Channel Input Port	31
7.1.9	Power Port	31
7.1.10	CIK Port	32
7.2	Electrical Signal Characteristics	32
7.2.1	Absolute Maximum Ratings	32
7.2.2	Electrical Power Requirements	32
7.2.3	Electrical Characteristics of I/O	32
7.2.3.1	LSTTL Bi-state	32
7.2.3.2	LSTTL Tri-state	33
7.3	Product Timing Relationships	33
7.3.1	Signal Timing Relationships	33
7.3.1.1	Write Cycle	34
7.3.1.2	Read Cycle	35
7.3.1.3	Traffic Data/Clock Input	36
7.3.1.4	Traffic Data/Clock Output	36
7.3.1.5	Zeroize Pulse Specification	37
7.3.1.6	Reset Pulse Specification	37
7.4	Fill Port Interface Requirements	38
8.	MECHANICAL INTERFACE SPEIFICATIONS	38
8.1	Interface Cabling, Connectors	38
8.2	Module Envelope	38
8.3	Detailed Footprint	38
8.4	KRV Requirements	38

LIST OF FIGURES

Fig No.	Title	Page No.
4-1	WINDSTER System Architecture	5
4-2	WINDSTER Block Diagram	6
5-1	Relationship Between INPUT ENABLE and the First Encrypted Bit	10
5-2	Relationship Between OUTPUT ENABLE and the First Decrypted Bit	11
7-1	Interface Signals to the WINDSTER Module	27
7-2	Windster Pinout	28
7-3	Write Cycle Waveform Relationships on Command/Status Port	34
7-4	Read Cycle Waveform Relationships	35
7-5	Traffic Data/Clock Input Relationships	36
7-6	Traffic Data/Clock Output Relationships.	36
7-7	Zeroize Pulse Specification	37
7-8	Reset Pulse Specification	37
8-1	WINDSTER Module Envelope	39
8-2	WINDSTER Detailed Footprint.	40

LIST OF TABLES

Table No.	Title	Page No.
4-1	Key Location and Type	8
6-1	WINDSTER Command Word Listing	14
6-2	Bit Definition of the WINDSTER Status Bytes	24
6-3	Error/Status Codes	25
7-1	Recommended Operating Conditions for LSTTL Bi-state Compatible Module Signals	33
7-2	Recommended Operating Conditions for LSTTL Tri-state Compatible Module Signals	33

INTERFACE CONTROL DOCUMENT (ICD)

1. INTRODUCTION

1.1 Scope

This document defines the functional, electrical and mechanical interface of the WINDSTER COMSEC Module. The WINDSTER COMSEC Module is electronic encryption and decryption circuitry, which can be embedded into a host communication equipment. This CMOS LSI circuitry can be used to secure voice and low speed data communications. This ICD is intended to serve the needs of the host system end item equipment developer. This document contains the detailed interface information that is required to integrate this communications security (COMSEC) module into existing or future telecommunications systems. Specific, system unique, security engineering guidance for the proper use of the WINDSTER COMSEC Module in telecommunication equipment will be provided by the National Security Agency on an individual application basis.

1.2 Terminology

Throughout this document, the embeddable WINDSTER COMSEC Key Generator Module (KGM) will be referred to as the KGM, and the host terminal equipment containing the KGM will be referred to as the host. All signals are referenced to the KGM, that is, inputs are signals to the KGM and output signals are from the KGM. A key generator device provides digital data encryption and decryption based on an internal cryptographic algorithm and a key. A key is a sequence of random binary digits (bits) used to set up the mathematical permutations within the cryptographic algorithm.

1.3. Comments

Comments and questions regarding this ICD or the application of the KGM to any specific program should be forwarded to:

DIRECTOR, NSA
ATTENTION Y24
9800 SAVAGE ROAD
FT. GEORGE G. MEADE, MD 20755-6000

1.4. NOTICE

The information found in the text and graphics contained within this document are the property of the United States Government. This document is intended to be used for official U.S. Government use only. Reproduction or unauthorized use of the information contained herein without written authorization from the originator is expressly prohibited by Federal Law.

2. APPLICABLE DOCUMENTS

2.1 Standards

2.2 Specifications

CSESD-11 - Communications security equipment system document for fill devices KYK-13, KYX-15, KOI-18 (Document is CONFIDENTIAL).

2.3 Publications

Handling and Control Requirements for CCI Equipment and Components During Manufacture and Assembly, dated 1 October 1985.

2.4 DRAWINGS

0N241775 - Fill Connector

3. SECURITY CONSIDERATIONS

3.1 Controlled Cryptographic Items

KGMs are Controlled Cryptographic Items (CCI) which are unclassified. The KGM must be controlled in accordance with the requirements set forth in the document entitled, "Handling and Control Requirements for CCI Equipment and Components During Manufacture and Assembly", dated 1 October 1985. The CCI controls, as a minimum, apply to the KGMs until integration and then to equipments or systems that contain the CCI KGMs.

3.2 NSA Endorsement

The WINDSTER KGM is approved by the National Security Agency for processing classified information at all levels. This approval is not extended automatically to host systems or equipment that contain the WINDSTER KGM. All systems and components of systems that are required to process classified information must be evaluated on a system unique basis prior to endorsement. For further information and a list of those vendors who are authorized to produce and sell the WINDSTER KGM with NSA endorsement, contact the NSA.

3.3 TEMPEST

Good TEMPEST design techniques have been used throughout the development of the WINDSTER KGM. The KGM carries no implied TEMPEST approval. Each integration of this KGM into host end item equipment must be evaluated in light of system specific TEMPEST requirements. Please contact the National Security Agency for further guidance.

4. GENERAL PRODUCT DESCRIPTION

The KGM provides full and half duplex encryption at data rates up to 200 kbps. It processes serial unencrypted (plain text-PT) data and serial encrypted (cipher text-CT) data. The KGM's fill port, as described in paragraph 7.1.1, satisfies the CSESD-11 electrical interface requirements. All other interfaces are LSTTL compatible.

4.1 Functional Description

The purpose of the KGM is to encrypt and decrypt digital communications. Encrypting a signal containing classified information permits the resulting signal to be transmitted over normal communication channels without violating the security of the classified information. Decrypting the encrypted signal "recovers" the classified information in its original plain text form.

The KGM will be designed and analyzed to operate over the full military temperature range even though implementations may encompass environmental restrictions. Several cryptographic modes of operation are available. These modes can be selected by a host equipment via an eight bit command/status bus. The KGM requires two independent data-rate clocks; one for the transmit channel and another for the receive channel.

4.2 WINDSTER Features

- Multiple Configurations
- Flexible key management modes
- DC to 200 kbps data rate
- Microprocessor-style control interface
- NSA standard interface structure
- NSA standard COMSEC Command Language (CCL)
- Independent transmit and receive channels
- LSTTL compatible interface
- Crypto Ignition Key (CIK) option
- Compatible with common fill devices (CSESD-11)
- Backward Compatibility

4.3 Architecture Description

The following sections are provided to functionally describe the architecture of the WINDSTER COMSEC KGM.

4.3.1 Interface Ports

The WINDSTER KGM interface is comprised of major signal groupings or ports. Refer to figure 4-1 "WINDSTER System Architecture".

- * The Command/Status Port is an eight bit wide bi-directional bus used to direct the KGM's mode of operation. The COMSEC Command Language (CCL) is used to control the KGM. Only commands and status are passed via this port, all data intended for encryption/decryption are processed via the traffic ports.

- * The Command/Status Control Port contains the typical microprocessor read, write, addressing, and interrupt signals.

- * The Housekeeping Port contains KGM unique signals such as alarm, zeroize, and tamper loop.

- * Power and key retention voltages are applied to the Power Port.

- * The Fill Port is the access point for manually loading the KGM with keys. This port may be connected to the Key Management Module (KMM) for use in high performance systems.

- * The CIK Port provides the handshaking and data carrying signals to support the use of a CIK function.

- * The Plain Text Ports, transmit in and receive out, are the interfaces for information that is unencrypted.

- * The Cipher Text Ports, transmit out and receive in, are the interfaces for information that is encrypted.

4.3.2 Internal Description

Internal architecture is comprised of 6 major functional sections. Refer to figure 4-2 "WINDSTER Block Diagram".

- * The controller provides all of the command decoding and processing functions. The controller also provides command verification in all modes. This verification is both for content of the command and for the context in which the host has invoked it.

WINDSTER SYSTEM ARCHITECTURE

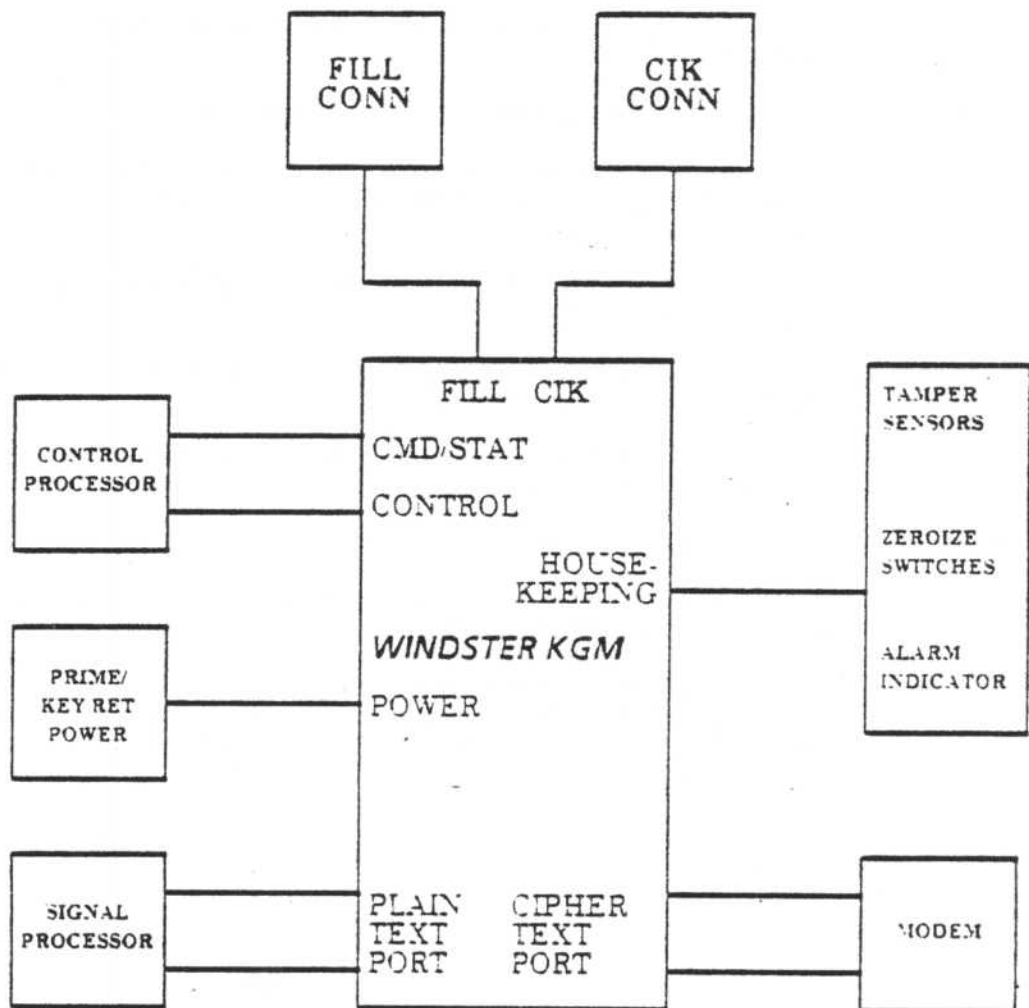


FIGURE 4-1

WINDSTER BLOCK DIAGRAM

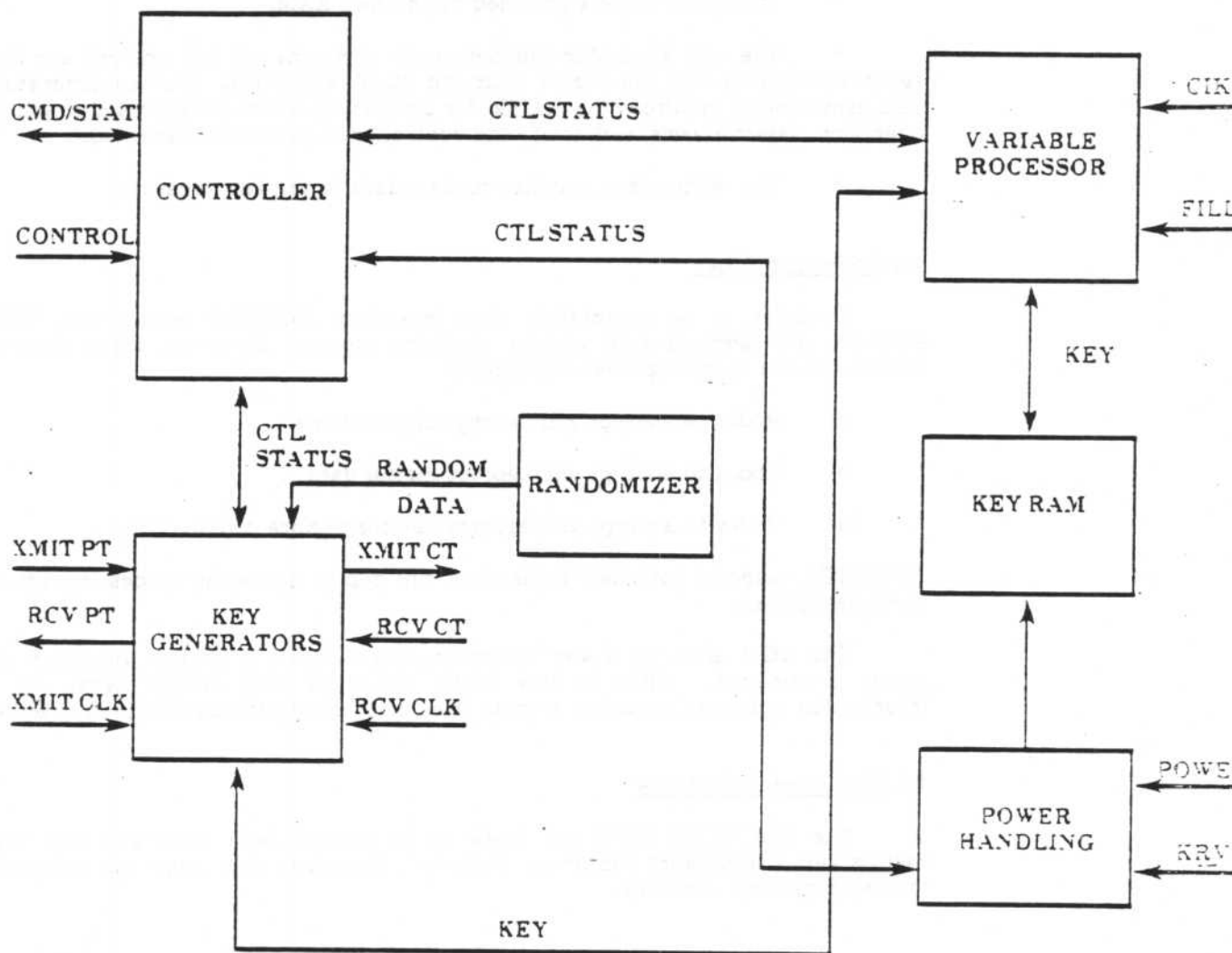


FIGURE 4-2

- * The power handling circuits monitor incoming prime and key retention power. The KGM has been designed to interrupt operation when it detects undervoltage on both the prime and key retention input power lines.
- * The variable processor provides the interface to both the Fill and CIK ports as well as the control for the movement of all keys within WINDSTER.
- * Storage of keys is provided by the Key RAM.
- * The key generator independently performs all I/O control and handshake functions directly with the Cipher Text and Plain Text Ports. The key generator section also continuously monitors the traffic for processing errors or alarms and will interrupt operation, assert alarms, and notify the controller if an error is detected.
- * The randomizer provides random data to the key generator.

4.4 Operating Modes

In order to be compatible with inventory COMSEC equipment, WINDSTER encrypts and decrypts with several operating modes. However, these modes can be sorted into the following three categories:

- o Modes to encrypt and decrypt digital voice
- o Modes to encrypt and decrypt digital data
- o Modes to encrypt and decrypt key for remote distribution.

WINDSTER supports both half duplex and full duplex operating modes in each of these three categories.

The KGM also has a key retention mode, which it enters whenever operating power is removed. While in this mode, the KGM only retains keys, key related information and certain control states. It cannot either process traffic or load keys.

4.5 Key Processing Modes

The WINDSTER KGM can store up to sixteen keys internally and implement various key management features. Table 4-1 illustrates the usage and relationships of the key types and locations.

TABLE 4.1

Key Location and Type

<u>LOCATION</u>	<u>TYPE</u>
0	Z.Variable
1	1 KEK
2	2 KEK
3	3 KEK
4	Traffic Keys or Key Encryption Keys(KEK) (any mix of types)
5	
6	
7	
8	
9	
10	
11	Scratchpad
12	
13	
14	
15	

4.5.1 Manual Key Loading

Keys are loaded thru the fill port. The host interface is the 6-pin connector specified in CSESD-11. The presence of the fill device is sensed by the controller and reported to the host via a status message. The host may then command that key be loaded and stored in a specified location. Only unencrypted (RED) keys can be loaded thru the fill port.

4.5.2 Black Key Processing

The KGM has the capability to encrypt (wrap) red keys upon command by the host for storage in memory external to the KGM. Decrypting black keys upon command of the host can also be accomplished by the KGM and stored in an internal location specified by the host.

4.5.3 Over-the-Air Rekeying (OTAR)

The KGM can be commanded to encrypt or decrypt keys using Key Encryption Keys (KEK) specified by the host. This process is used to support remote electronic distribution of keys.

4.5.4 Crypto Ignition Key (CIK)

The KGM will incorporate an optional CIK function.

4.5.5 Key Retention Mode

A host supplied Key Retention Voltage (KRV) is used to maintain the contents of the Key RAM when prime power is removed. If this KRV is not supplied the KGM will zeroize upon loss of prime power.

4.5.3 In-Band Rekeying

The KGM can be commanded to perform in-band rekeying of selected keys in either a manual or automatic mode.

4.6 Power

The WINDSTER KGM operates from a +5 volt $\pm 5\%$ DC source which is the prime power input. It also has a memory retention capability so that the contents of the key storage and other WINDSTER memories can be retained even though the prime power is removed from the KGM. Both prime power and key retention voltage are supplied by the host.

4.7 Zeroize

The host can command the KGM to zeroize all keys or to zeroize a selected key storage location.

4.8 Alarm Status Output

The KGM outputs an alarm condition to the host on a dedicated pin. Simultaneously, the KGM inhibits all traffic until the alarm condition is corrected. Additionally, the KGM can report the alarm condition via the Command/Status Port.

4.9 Error Reporting

The KGM reports all error conditions to the host, such as an invalid command, key parity error, key update overflow error, etc. The KGM reports the error condition through the Command/Status Port.

5. PRINCIPLES OF OPERATION

The WINDSTER KGM has been designed to provide a cryptographic data processing function for many different types of telecommunication systems. The interface structure and operating modes have been developed to provide efficient data and command processing rates while promoting a simple and secure integration effort. The data processing modes support a variety of cryptographic synchronization acquisition schemes. The selection of the proper mode of operation is system dependent.

5.1 State Descriptions

The WINDSTER KGM will accept commands from its host at any time that the controller is not busy. This can be when the KGM is in an idle state or when the key generators are processing traffic and the controller is no longer occupied in directing operations.

5.2 Cryptographic Operating Modes

WINDSTER is a key on demand system, where the KGM will produce one bit of PT or CT for every data rate clock pulse it receives. The design is to operate at all data rates below 100 kbps.

There is one basic command (set mode) which sets the cryptographic operating mode. This command allows for parameters to be specified such as full or half duplex and data mode type.

5.3 Cryptographic Synchronization

The host is responsible for most of the system synchronization requirements. It must recover the receive clock, perform bit recovery, and perform any word framing associated with redundantly transmitted message indicator bits. The length of the synchronization word is determined by the host. The KGM will achieve cryptographic synchronization from the message indicator bits that are provided by the host.

The host is responsible for detecting the loss of cryptographic synchronization. Both the transmit and receive sections of the WINDSTER KGM output Altered Plain Text pulses (APTs). The host can use these pulses to detect loss of synchronization.

The host must select the applicable method of cryptographic synchronization.

5.3.1 Pre-Synchronization Requirements

The WINDSTER KGM must have key variables transferred into the working storage of the key generators and an encryption and/or decryption mode must have been selected before the KGM can begin cryptographic synchronization.

5.3.2 Initial Synchronization

The WINDSTER KGM requires message indicator (MI) bits to establish an initial setting for the key generator. The random MI bits are generated by the transmitting WINDSTER. At the receiving WINDSTER these same bits are inserted into the KGM by the host.

When the host of the transmitting WINDSTER KGM raises the TRANSMIT input signal, the KGM will begin outputting the MI bits. These bits will appear on the XMIT CT output line and will be coincident with the positive edges of the XMIT CLK input signal. (See paragraph 7.3 for detailed timing relationships.) WINDSTER may encrypt a few additional bits for internal bookkeeping before raising the INPUT ENABLE output signal. The XMIT PT signal is strobed into the KGM with the negative edge of the XMIT CLK signal. The INPUT ENABLE signal indicates when the KGM will begin encrypting the plain text data. INPUT ENABLE is raised with the negative transition of the XMIT CLK signal which precedes the positive edge used to sample the first plain text bit to be encrypted. Figure 5-1 illustrates this relationship.

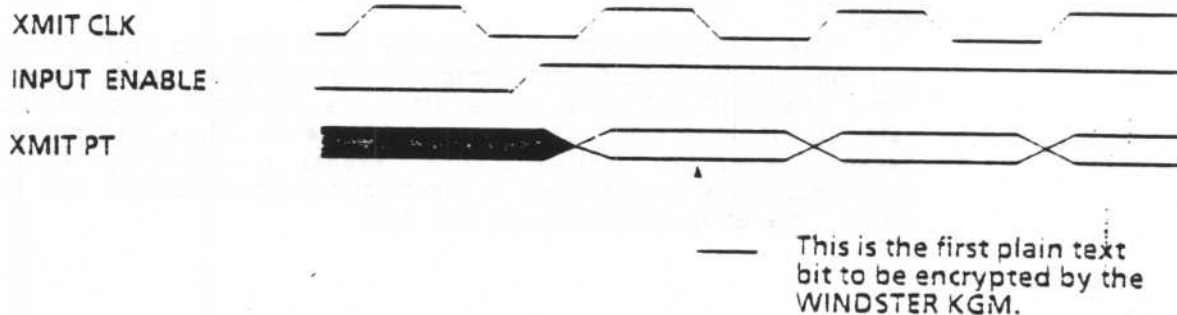


Figure 5-1. Relationship Between INPUT ENABLE and the First Encrypted Bit.

To initialize the receiving WINDSTER with the MI bits, the host must raise the SYNC input signal. The SYNC input signal must remain high for the duration of the received message. Lowering and then raising the SYNC line will cause the KGM to synchronize to a new MI. Once the receiving WINDSTER has been initialized, it will decrypt the few additional bookkeeping bits generated by the transmitting KGM. The receiving KGM will raise the OUTPUT ENABLE output signal to identify the first decrypted bit. WINDSTER outputs the RCV PT bits coincident with the negative edges of RCV CLK signal. (See paragraph 7.3 for detailed timing relationships.) OUTPUT ENABLE will be raised with the negative edge of the RCV CLK that marks the beginning of the first decrypted bit. Figure 5-2 illustrates this relationship.

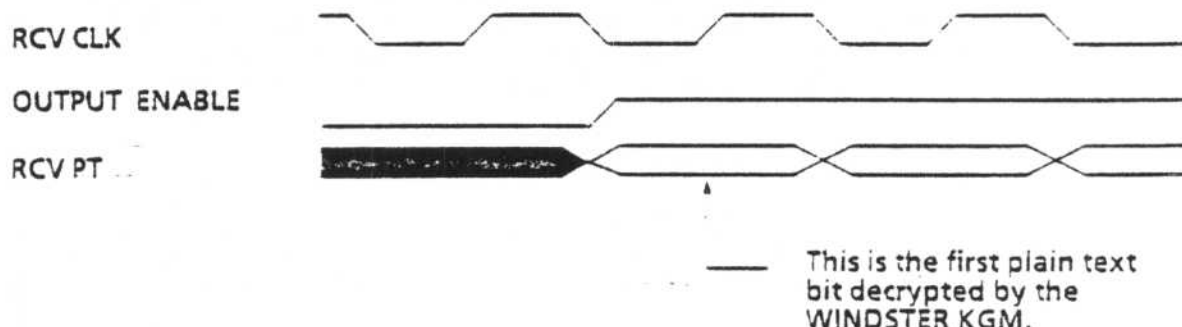


Figure 5-2. Relationship Between OUTPUT ENABLE and the First Decrypted Bit.

5.3.3 Verification of Cryptographic Synchronization

The host, not the WINDSTER KGM, is responsible for continuous verification of cryptographic synchronization. WINDSTER provides signals to assist the host with this responsibility. These signals include the OUTPUT ENABLE, INPUT ENABLE, XMIT APT and RCV APT output signals.

The OUTPUT ENABLE and INPUT ENABLE could be used in conjunction with framing bits inserted by the host to verify synchronization when encrypting synchronous data.

The WINDSTER KGM provides the XMIT APT and RCV APT signals which the host can use to help verify cryptographic synchronization. APT stands for "altered plain text." The XMIT APT signal is most often in a low state. Approximately once every 64 data rate bit times, XMIT APT goes high for one bit. Since the occurrence is result of a deterministic, but pseudo-random, event: a receiving WINDSTER that is cryptographically synchronized to the transmitting WINDSTER will produce the same signal. This latter signal is called RCV APT.

The transmitting equipment can use the XMIT APT signal to randomly place a check bit in the plain text stream. The receiving equipment can then use the RCV APT signal to look for the check bit in the decrypted plain text stream. Whenever the equivalent of XMIT APT goes high in equipment that is using CVSD, a transition is forced in the plain text stream. In other words, if the previous bit out of the voice processor was a zero, the next bit will be a one, regardless of what the processor determines it to be. Conversely, if the previous bit out of the voice processor was a one, the next bit will be forced to a zero. Thus, the forced transition serves as a check bit that can be detected by the receiving equipment. The equivalent of the RCV APT signal determines where the plain text transitions are to occur in the receiving equipment. If the transitions are not there, the receiving equipment declares that it is out of cryptographic synchronization.

5.3.4 Cryptographic Resynchronization While in Traffic

The half duplex implementation enables a receiver to establish cryptographic synchronization from the middle of an encrypted message stream. The WINDSTER KGM assumes that encrypted "1010" patterns exist in the message stream. Therefore, the host can command the KGM to synchronize to this pattern by issuing a resync command. Once the host determines that "1010" patterns are being decrypted, it commands the KGM to return to the normal traffic mode by issuing a return to traffic command. The transmitting host supports this in traffic resynchronization procedure by merely inserting streams of "1010" patterns into the plain text stream.

5.4 Backward Compatibility

The WINDSTER KGM can be used to provide cryptographic compatibility with existing fielded COMSEC gear. The level of compatibility is divided into two groupings. First, the KGM is "traffic compatible" if, in conjunction with the host, it has the ability to communicate in a traffic mode of that equipment. Second, the KGM is "backward compatible" if, in conjunction with the host, it has the capability to perform all functions of that equipment (traffic functions and rekey functions). It is the intent of the WINDSTER KGM to be flexible enough to allow a host integrator to incorporate into his system as much backward compatibility as his requirements call for.

The following equipments are Backwards Compatible:

KY-57/58	KOV-1	KG-82
KY-68/78	KG-84	KYV-2A/B

The following equipments are Traffic Compatible only:

KYV-5	STU-III	KY-71
-------	---------	-------

5.5 Key Processing

The WINDSTER KGM provides 3 major methods of key processing - Wrap, Unwrap, Generate, Transfer, Zeroize, Update, Load, and In-band Rekey. All methods use the internal key storage locations 0 through 15. All keys stored within WINDSTER are comprised of a key packet that contains the following information:

- TYPE
- USE
- ALGORITHM
- UPDATE COUNT
- KEY
- CHECK SEQUENCE

In the case where keys are loaded from a KYK-13 fill device, the additional key packet data is provided by the host as operand bytes with the LOAD RED KEY command on the Command/Status Port. During key processing modes certain fields are checked to insure that the proper key is being used. Error conditions are reported to the host and operations may be denied if an attempt is made to use a key improperly. Refer to the detailed command processing descriptions for more information.

In the case where a KYK-15 (NCD) is attached to the KGM and requesting an operation, the KGM will notify the host by raising BSY, lowering SRQ*, and reporting the requested operation to the host via the Command/Status port. In band rekeying procedures will require host support, while Update, Generate, and Load will be handled directly by the KGM and NCD. Upon completion of any NCD operation, the KGM will lower the BSY line, and thereby return control to the host.

6. WINDSTER COMMANDS

6.1 COMSEC Command Language

The COMSEC Command Language (CCL) has been developed to support NSA's standard product line of embeddable COMSEC modules. This language is used throughout the family where common functionality exists. This method has been selected to enhance the structured nature of the product line. The host system designer does not need to continually become familiar with different command languages in order to efficiently and securely embed the KGMs in various target systems. System level control software will be more easily transportable when it is based on CCL, yielding a significant cost savings.

All commands are comprised of one operator byte followed by 0 to n operand bytes determined by a table lookup of the operator byte. The operator byte is decoded as follows:

bit	7	6	5	4	3	2	1	0	LSB
-----	---	---	---	---	---	---	---	---	-----

FIELD	PARITY	CLASS	TYPE
-------	--------	-------	------

All operator bytes are adjusted for odd parity. Operand bytes have no parity. There are eight possible classes of commands. Each class is assigned as follows:

CLASS	DESCRIPTION
000	"Unused"
001	General Purpose Commands
010	Key Processing Commands
011	Data Processing Commands
100	Special Purpose Commands
101	Special Purpose Commands
110	Special Purpose Commands
111	Special Purpose Commands

Type specifies one of 16 commands for each class.

6.2 Command Protocol

This section explains how the host writes commands to the WINDSTER KGM. The following sequence is used at the beginning of each command. Detailed timing diagrams for transfers over the bidirectional command/status port are provided in figures 7-3 and 7-4.

WINDSTER COMMAND TRANSFER SEQUENCE

1. The host checks the status of BSY and SRQ*. If neither is active then;
2. The host sets CS* and CMD* low, and places the operator on the bus.
3. At this point the WR* signal is pulsed low and the operator will be latched into the KGM on the rising edge of WR*.
4. Also, on the rising edge of WR*, BSY will go high. This indicates that processing of the operator is occurring.
5. If additional operand bytes have to be sent to the KGM, then the host will wait for the KGM to lower its BSY line and repeat steps 2, 3 and 4 with operand data being placed on the bus with CMD* high. This sequence is repeated until all operands have been written to the KGM. If no more operand data is required for a particular command, the KGM will not lower its BSY signal until the command processing has been completed.

6.3 Command Listing

WINDSTER COMMAND LISTING

COMMAND NAME	BYTE	EXECUTION	DESCRIPTION
General Purpose Commands			
Stop	10H	ON	Stops all Traffic
Self Test	91H	E	Checks alarms in WINDSTER
Loop Check-Enable	92H	OFF	Enables Loop around mode
Restart	13H	E	Resets WINDSTER to a known state
Read Status	94H	E	Module outputs status byte
Loop Check-Disable	15H	E	Disables Loop around mode
Activate CIK	1FH	E	Activates CIK
Key Processing Commands			
Zeroize All	20H	E	Zeroizes all keys
Zeroize	A1H	E	Zeroizes selected location
Load Red Key	A2H	OFF	Loads key from fill port
Transfer Enc Key	23H	OFF	Transfers key to encrypt working store
Transfer Dec Key	A4H	OFF	Transfers key to decrypt working store
Unwrap Black OTAR	25H	OFF	Unwrap key
Unwrap Stored Black	26H	OFF	Unwrap local black key
Wrap Black OTAR	A7H	OFF	Wrap key for OTAR
Wrap Red Key	A8H	OFF	Wrap key for local storage
Update Red Key	29H	OFF	Updates the key
Validate Key	2AH	OFF	Check key parity
Copy Red Key	2CH	OFF	Copies keys
Load Red Key	AEH	OFF	Loads key from fill port with host supplied tag
On Line Load	2FH	ON	Special key operation

Data Processing Commands

Set Mode	-B0H	E	Sets mode control registers for various traffic modes.
In Traffic Resync	BCH	ON	Initiate Resync-Operation
Return to Traffic	3DH	ON	Returns to traffic after a Resync

Special Purpose WINDSTER Commands

Encrypt Half Duplex	62H	OFF	Enables half duplex encryption
Decrypt Half Duplex	E3H	OFF	Enables half duplex decryption
Variable Generate	64H	OFF	Generates a key for KYX-15
Change Z	E6H	E	Rewrap old keys with new Z
Go To Full Duplex	67H	E	Enables full duplex traffic
Net Inband Rekey	68H	E	Initiate net rekey
Session Inband Rekey	E9H	E	Initiate per call rekey
Receive Inband Rekey	6AH	E	Receive key and store

Table 6-1 WINDSTER Command Word Listing

NOTE: EXECUTION refers to on-line (host has enabled the traffic ports) or off-line command (host or an alarm have disabled the traffic ports) or E-either.

6.4 WINDSTER Command Description

This section describes the command interface used by the WINDSTER KGM. The commands names are used for identification and description only.

D1	= First byte of a 2 byte Tag header. Shh in hex.
D2	= Second byte of a 2 byte Tag header. Saa in hex.
N,N1,N2	= Key RAM location 0 to 15 in decimal.
S	= Status register 0 to 5. Sss in hex.
K	= Number of wraps/unwraps used in Change Z command.
A	= Set Mode operand.

WINDSTER TRAFFIC PROCESSING MODES

Traffic Mode = Full duplex, both the TX and RX KGs have a valid key and a "GO TO TRAFFIC" command was issued. Encryption and decryption enabled but not begun until the SYNC or TRANSMIT signals are activated.

Idle Mode = Full or half duplex, no precondition on working store. Encryption and decryption are not enabled.

RX Traffic = Half duplex decryption, valid key in RX KG, and the TRANSMIT signal must be low. In this mode decryption is enabled but not begun until the SYNC signal is activated.

TX Traffic = Half duplex encryption, valid key in TX KG, and the SYNC signal must be low. In this mode encryption is enabled but not begun until the TRANSMIT signal is activated.

1. STOP

TYPE: ONLINE

COMMAND FORMAT: \$10

DELAY: TBD

DESCRIPTION: Stops all decryption and encryption while in the full duplex mode, or stops all decryption if in the half duplex mode. Note that encryption is disabled during half duplex on the falling edge of the TRANSMIT signal, after generation of End of Message (EOM).

OPERANDS: None.

ENTRY: Traffic mode full duplex or RX traffic mode in half duplex.

EXIT: Idle mode. If in full duplex the TX and RX KG get over-written, if in half duplex only the RX KG gets overwritten.

STATUS BITS: Resets ENCRYPTION ENABLED and DECRYPTION ENABLED Bits.

2. SELF TEST

TYPE: EITHER

COMMAND FORMAT: \$91

DELAY: TBD

DESCRIPTION: Initiates an alarm check sequence with the last addressed key.

OPERANDS: None.

ENTRY: Any Traffic mode or Idle mode.

EXIT: Idle mode if alarm check passes or the Alarm state (ALARM signal high), if the alarm check fails.

STATUS BITS: Error bytes 1 and 2. (status registers 4 and 5), may be affected.

3. LOOP CHECK ENABLE

TYPE: OFFLINE

COMMAND FORMAT: \$92

DELAY: TBD

DESCRIPTION: Enables the loop around mode where CT out is connected to CT in internally. The XMIT CT and RCV CT signals of the KGM are blocked. Note that it is the host's responsibility to load the same key to both the TX and RX KGs.

OPERANDS: None.

ENTRY: Idle mode, full duplex.

EXIT: Loop mode. Note that the WINDSTER KGM can't enter the Traffic mode until the LOOP CHECK DISABLE command is issued.

STATUS BITS: The Loop Check status bit will be set.

4. RESTART

TYPE: EITHER

COMMAND FORMAT: \$13

DELAY: TBD

DESCRIPTION: Resets the WINDSTER KGM to a known start up state.

OPERANDS: None.

ENTRY: Any Traffic or Idle mode.

EXIT: Idle mode or the Alarm state if an alarm check fails.

STATUS BITS: All status bits set/reset to initial conditions.

5. READ STATUS (S)

TYPE: EITHER

COMMAND FORMAT: \$94 \$ss

DELAY: TBD

DESCRIPTION: Output one of 6 status bytes to be read by the host. The BUSY line stays high until the status is read.

OPERANDS: S= 0 to 5. Object code \$ss = \$00 to \$05.

ENTRY: Any Traffic or Idle mode, or the Alarm state.

EXIT: Remains in the BSY state until a status byte has been read and then returns to its previous state.

STATUS BITS: No change.

6. LOOP CHECK DISABLE

TYPE: OFFLINE

COMMAND FORMAT: \$15

DELAY: TBD

DESCRIPTION: Disables the loop around mode. Disconnects the CT out from CT in which was connected by the LOOP CHECK ENABLE mode.

OPERANDS: None.

ENTRY: Loop mode.

EXIT: Idle mode.

STATUS BITS: The Loop Check status bit will be reset.

7. ACTIVATE CIK

TYPE: OFFLINE

COMMAND FORMAT: \$1F

DELAY: TBD

DESCRIPTION: This command instructs the WINDSTER KGM to look for the presence of a CIK device. Once activated the CIK port always remains enabled until a RESET.

OPERANDS: None.

ENTRY: Idle mode, CIK pin is active

EXIT: Idle mode.

STATUS BITS: No change.

8. ZEROIZE ALL

TYPE: EITHER

COMMAND FORMAT: \$20

DELAY: TBD

DESCRIPTION: Zeroizes RAM memory locations 0 to 15, and will overwrite the TX and RX working store.

OPERANDS: None.

ENTRY: Idle mode or Any Traffic mode.

EXIT: Idle mode if the RAMs zeroized correctly or the Alarm state if an incorrect zeroize occurred.

STATUS BITS: The Parity status bits will be reset along with the Encryption Valid and Decryption Valid status bits.

9. ZEROIZE (N)

TYPE: EITHER

COMMAND FORMAT: SA1 \$nn

DELAY: TBD.

DESCRIPTION: Selectively zeroizes key RAM location N.

OPERANDS: N= 0 to 15. \$nn = \$00 to \$0F.

ENTRY: Idle or Any Traffic modes.

EXIT: Returns to the entry state if zeroized correctly, or the Alarm state if RAM N could not be zeroized.

STATUS BITS: Parity Status bit for Key N will be reset.

10. LOAD RED KEY (N),D1,D2

TYPE: OFFLINE

COMMAND FORMAT: SA2 \$nn \$hh \$aa

DELAY: TBD.

DESCRIPTION: Loads a key from the fill port and compares the host supplied tag with the tag contained in the key. If the tag compare passes and the key has good parity, store the key to RAM location N.

OPERANDS: N = 0 to 15. Object code \$nn= \$00-\$0F. D1 and D2 indicate two bytes of host supplied tag, \$hh and \$aa (header and algorithm).

ENTRY: Idle mode.

EXIT: Idle mode.

STATUS BITS: Parity Status bit for Key N, Configuration or Tag Mismatch status bits, or Parity Error.

11. TRANSFER ENC KEY (N)

TYPE: OFFLINE

COMMAND FORMAT: \$23 \$nn

DELAY: TBD.

DESCRIPTION: Transfers a TEK located at RAM location N to the encrypt key generator for full duplex operation.

OPERANDS: N = 4 to 15, object code \$nn= \$04 to \$0F.

ENTRY: Idle mode, full duplex.

EXIT: Idle mode.

STATUS BITS: Parity error, Configuration or Tag mismatch status bits.

12. TRANSFER DEC KEY (N)

TYPE: OFFLINE

COMMAND FORMAT: SA4 \$nn

DELAY: TBD

DESCRIPTION: Transfers a TEK located at RAM location N to the decrypt key generator for full duplex operation.

OPERANDS: N=4 to 15, object code \$nn= \$04 to \$0F.

ENTRY: Idle mode, full duplex.

EXIT: Idle mode.

STATUS BITS: Parity error, Configuration or Tag mismatch

13. UNWRAP BLACK OTAR (N1,N2),D1,D2 TYPE: OFFLINE

COMMAND FORMAT: \$25 \$n1 \$n2 Shh Saa

DELAY: TBD.

DESCRIPTION: Unwraps a black key from the host using KEK N1. If the TEK tag D1 D2 matches the key tag and parity is passed, the key is stored in RAM location N2.

OPERANDS: N1= 1 to 15, \$n1= \$01-\$0F. Location of KEK.

N2= 4 to 15, \$n2= \$04-\$0F. Location of TEK.

D1 and D2 indicate 2 bytes of host supplied TEK tag, Shh and Saa (header and algorithm).

ENTRY: Idle.

EXIT: Idle.

STATUS BITS: Time out on unwrap, invalid operand, parity error on TEK. tag mismatch.

14. UNWRAP STORED BLACK KEY (N),D1,D2 TYPE: OFFLINE

COMMAND FORMAT: \$26 \$nn Shh Saa

DELAY: TBD.

DESCRIPTION: Unwraps a host black key using the Z variable. The decrypted key's tag will be compared to the host supplied tag D1 D2. If a valid compare occurs then the key is stored in RAM location N.

OPERANDS: N = 1 to 15, \$nn= \$01-\$0F.

D1 and D2 specify 2 bytes of host supplied tag, Shh and Saa (header and algorithm) of the decrypted key.

ENTRY: Idle mode.

EXIT: Idle mode.

STATUS: Key Parity for Key N. Parity error. Configuration or Tag mismatch status bits.

15. WRAP BLACK OTAR (N1,N2),D1,D2 TYPE: OFFLINE

COMMAND FORMAT: \$A7 \$n1 \$n2 Shh Saa

DELAY: TBD

DESCRIPTION: Wraps the TEK located in RAM location N1 using the KEK found in location N2. The tag of the TEK will be compared to the host supplied TEK tag prior to wrapping.

OPERANDS: N1= 1 to 15, \$n1 = \$01-\$0F. Location of KEK.

N2= 4 to 15, \$n2 = \$04-\$0F. Location of TEK.

D1 and D2 specifies 2 bytes of host supplied TEK tag, Shh and Saa (header and algorithm).

ENTRY: Idle.

EXIT: Idle.

STATUS: Parity for Key N. Parity Error. Configuration or Tag mismatch.

16. WRAP RED KEY FOR STORAGE (N),D1,D2 TYPE: OFFLINE

COMMAND FORMAT: \$A8 \$nn Shh Saa

DELAY: TBD.

DESCRIPTION: Wrap the key found in RAM location N using the Z variable found in RAM location 0. Check the tag information of key N using the host supplied tag, D1,D2 prior to wrapping.

OPERANDS: N= 1 to 15, \$nn= \$01 to \$0F. Key to be wrapped.

D1,D2 indicate 2 bytes of host supplied tag, Shh and Saa (header and algorithm), for key N.

ENTRY: Idle mode.

EXIT: Idle mode.

STATUS BITS: Parity for Key N. Parity error. Configuration or Tag mismatch.

17. UPDATE RED KEY (N),D1,D2

TYPE: OFFLINE

COMMAND FORMAT: \$29 \$nn \$hh \$aa

DELAY: TBD.

DESCRIPTION: Update key N and increment the update count. A tag compare using D1 and D2 is performed prior to updating the key.

OPERANDS: N= 1 to 15. \$nn= \$01 to \$0F. Key to update.
D1 and D2 indicate 2 bytes of tag data, \$hh and \$aa (header and algorithm), for key N.

ENTRY: Idle mode.

EXIT: Idle mode.

STATUS BITS: Parity for key N, Parity error, Configuration or Tag mismatch.

18. VALIDATE KEY (N),D1,D2

TYPE: OFFLINE.

COMMAND FORMAT: \$2A \$nn \$hh \$aa

DELAY: TBD.

DESCRIPTION: Validates key N by checking for good parity and comparing its tag to the host supplied tag.

OPERANDS: N= 0 TO 15, \$nn= \$00 to \$0F. Key to validate.

ENTRY: Idle.

EXIT: Idle.

STATUS BITS: Parity for Key N, Parity Error, Configuration or Tag mismatch.

19. COPY RED KEY (N1,N2)

TYPE: OFFLINE

COMMAND FORMAT: \$2C \$n1 \$n2

DELAY: TBD.

DESCRIPTION: Copies key in location N1 into RAM location N2.

OPERANDS: N1= 0 to 15, \$n1= \$00 to \$0F. Source RAM location.
N2= 4 to 15, \$n2= \$04 to \$0F. Destination RAM location.

ENTRY: Idle mode.

EXIT: Idle mode.

STATUS BITS: Bad parity.

20. LOAD RED KEY/W HOST
SUPPLIED TAG (N),D1,D2

TYPE: OFFLINE

COMMAND FORMAT: \$AE \$nn \$hh \$aa

DELAY: TBD.

DESCRIPTION: Loads a key from the fill port and appends the host supplied tag to the key. It then stores the appended key to RAM key location N.

OPERANDS: N = 0 to 15. Object code \$nn= \$00-\$0F.
D1 and D2 specify 2 bytes of host supplied tag, \$hh, and \$aa (header, and algorithm).

ENTRY: Idle mode.

EXIT: Idle mode.

STATUS BITS: Parity for Key N, Parity error.

21. ON LINE LOAD

TYPE: ONLINE

COMMAND FORMAT: \$2F

DELAY: TBD.

DESCRIPTION: This command instructs the WINDSTER KGM to load a key from the fill port, mod 2 add it to the key used in the transmit KG, and use the result of the mod 2 addition as the new key for both the transmit and receive KGs. This command is only valid while in full duplex and will remain in operation until a "STOP" command is issued.

OPERANDS: None.

ENTRY: Traffic mode, full duplex.

EXIT: Traffic with a new working key. The ON LINE load is terminated by the "STOP" command, which zeroizes the receive and transmit work stores.

STATUS BITS: Error status registers 4 and 5 may be affected.

22. SET MODE (A)

TYPE: EITHER

COMMAND FORMAT: \$B0 Saa

DELAY: TBD.

DESCRIPTION: This command will set up the mode control registers for various traffic configurations. The format of operand A is the same as status byte 03, with the exception of bit 7 which is reserved). Note that the half/full duplex mode can not be changed while ONLINE.

OPERANDS: A, Saa indicates the traffic configuration.

ENTRY: Any Traffic or Idle mode.

EXIT: No change in state.

STATUS BITS: Error status registers 4 and 5 may be affected.

23. IN TRAFFIC RESYNC

TYPE: ONLINE

COMMAND FORMAT: \$BC

DELAY: TBD

DESCRIPTION: This command will change the mode of the receive KG to the sync acquisition state if in half duplex.

OPERANDS: None.

ENTRY: RX Traffic mode, half duplex.

EXIT: RX Traffic mode, half duplex, sync acquisition state.

STATUS BITS: No change.

24. RETURN TO TRAFFIC

TYPE: ONLINE

COMMAND FORMAT: \$3D

DELAY: TBD

DESCRIPTION: This command will return the receive KG from sync acquisition to the normal RX traffic mode it was in prior to the "IN TRAFFIC RESYNC" command.

OPERANDS: No operands.

ENTRY: RX Traffic mode, half duplex, sync acquisition.

EXIT: RX Traffic mode, half duplex.

STATUS BITS: No change.

25. ENCRYPT HALF DUPLEX W/KEY (N)

TYPE: OFFLINE

COMMAND FORMAT: \$62 Snn

DELAY: TBD.

DESCRIPTION: This command will transfer a TEK located at RAM location N to the transmit KG and enable traffic encryption in the half duplex mode.

OPERANDS: N= 4 to 15, Snn= \$04-\$0F. Location of TEK.

ENTRY: RX Traffic or Idle mode, half duplex.

EXIT: TX Traffic mode, half duplex. The rising edge of the TRANSMIT signal initiates traffic, and the falling edge of TRANSMIT signal stops traffic, sends an EOM, and returns the Transmit KG to the Idle mode. If a valid key was in the RX KG, the RX traffic mode is entered on the falling edge of TRANSMIT

STATUS BITS: Parity for Key N, Parity error, Configuration or Tag mismatch.

26. DECRYPT HALF DUPLEX W/KEY (N)

TYPE: EITHER

COMMAND FORMAT: \$E3 Snn

DELAY: TBD.

DESCRIPTION: This command will transfer a TEK key from RAM location N to the Receive KG, and enable the decryption of data.

OPERANDS: N= 4 to 15, Snn= \$04-\$0F. Location of TEK.

ENTRY: TRANSMIT signal must be low.

EXIT: RX traffic mode. This mode indicates that the RX KG is ready for decryption.

STATUS BITS: Parity for Key N, Parity Error, Configuration or Tag mismatch.

27. VARIABLE GENERATE

TYPE: OFFLINE

COMMAND FORMAT: \$64

DELAY: TBD

DESCRIPTION: This command will generate a key without a tag for a KYX-15 or KYK-13.

OPERANDS: None.

ENTRY: Idle mode.

EXIT: Idle mode.

STATUS BITS: Error Status registers 4 and 5 may be affected.

28. CHANGE Z (K)

TYPE: OFFLINE

COMMAND FORMAT: \$E6 skk

DELAY: TBD.

DESCRIPTION: This command will copy the old Z variable from location 0 and temporarily store it in location 15. It will then allow the fill device to load in a new Z variable into location 0. The KGM then expects K number of UNWRAP and WRAP commands to be issued from the host. Unwraps will use the old Z wraps will use the new Z.

OPERANDS: $0 < K \leq 255$.

ENTRY: Idle mode.

EXIT: Idle mode.

STATUS BITS: Parity Error.

29. GO TO FULL DUPLEX TRAFFIC

TYPE: OFFLINE.

COMMAND FORMAT: \$67

DELAY: TBD.

DESCRIPTION: Enables decryption and encryption of data while in the full duplex mode.

OPERANDS: None.

ENTRY: Idle mode, full duplex.

EXIT: Traffic mode.

STATUS BITS: Encryption Valid, Decryption Valid status bits.

30. NET INBAND REKEY (N1,N2)

TYPE: ONLINE

COMMAND FORMAT: \$68 \$n1 \$n2

DELAY: TBD

DESCRIPTION: Initiates full duplex rekey to send a new net key without an NCD.

OPERANDS: N1 = KEK to be used. \$n2=02,04-0F

N2 = TEK to be sent. \$n1=\$04-0F

ENTRY: In traffic, Full duplex.

EXIT: In traffic, Full duplex.

STATUS BITS: Bad parity.

31. SESSION INBAND REKEY (N1,N2)

TYPE: ONLINE

COMMAND FORMAT: \$69 \$n1 \$n2

DELAY: TBD

DESCRIPTION: Initiates full duplex rekey, without an NCD, to send a new session per call key.

OPERANDS: N1 = KEK to be used \$n2=02,04-0F

N2 = TEK to be sent \$n1=\$04-0F

ENTRY: In traffic, full duplex, switched net.

EXIT: In traffic, full duplex.

STATUS BITS: Bad parity.

32. RECEIVE INBAND REKEY (N)

TYPE: ONLINE

COMMAND FORMAT: \$6A \$nn

DELAY: TBD

DESCRIPTION: Prepare the KGM to receive an inband rekey message for cooperative rekey operation.

OPERANDS: N = 4 to 15, \$nn = \$04 to \$0F. Location of key RAM to store TEK.

ENTRY: RX traffic, Voice mode, Full or Half duplex.

EXIT: Traffic mode in full duplex, idle mode if in half duplex.

STATUS BITS: Bad parity.

6.5 Register Definitions

The only host readable registers within the WINDSTER KGM are the status registers. These register are each one byte wide. The registers can be read one at a time by issuing a READ STATUS (s) command where s is the number of the byte that the host wishes to read.

WINDSTER STATUS REGISTER DEFINITIONS

Type of Status	Byte #	Bit #	Description
Summary Byte	00	7	Configuration 2 pin
	00	6	Configuration 1 pin
	00	5	Fill Device Attached
	00	4	CIK Device Attached
	00	3	CIK Enable Option Pin
	00	2	Encryption Enabled
	00	1	Decryption Enabled
	00	0	Alarm
Key Parity Byte 1	01	7	Parity of Key 15
	01	6	Parity of Key 14
	01	5	Parity of Key 13
	01	4	Parity of Key 12
	01	3	Parity of Key 11
	01	2	Parity of Key 10
	01	1	Parity of Key 9
	01	0	Parity of Key 8
Key Parity Byte 2	02	7	Parity of Key 7
	02	6	Parity of Key 6
	02	5	Parity of Key 5
	02	4	Parity of Key 4
	02	3	Parity of Key 3
	02	2	Parity of Key 2
	02	1	Parity of Key 1
	02	0	Parity of Key 0
Mode Byte	03	7	Data Mode Configuration Bit 1
	03	6	Data Mode Configuration Bit 2
	03	5	APT Enable
	03	4	Full/ Half Duplex Mode
	03	3	Mode A/B
	03	2	Voice/ Data
	03	1	Switched/ Dedicated
	03	0	Loop Check Mode

Error Byte 1	04	7	Reserved
	04	6	Reserved
	04	5	Reserved
	04	4	Reserved
	04	3	Reserved
	04	2	Configuration Mismatch
	04	1	Tag Mismatch
	04	0	Parity Error
Error Byte 2	05	7-0	Reserved

Table 6-2. Bit Definition of the WINDSTER Status Bytes

6.6 Service Requests/ Error Messages

A few events will cause the WINDSTER KGM to request service from the host. These events are limited to conditions that require the attention of the host. Any time the WINDSTER KGM requests service from the host or is reporting an error message, the SRQ* signal to the host is asserted. An eight bit error/status code will be provided to the host on the Command/ Status control port. This error/status code is defined in Table 6-3.

WINDSTER ERROR/STATUS MESSAGES

I. GENERIC ERROR/STATUS MESSAGES

BYTE	DESCRIPTION
02H	Unrecognizable Command
03H	Invalid Command
04H	No Fill Device Attached (Fill Time Out)
05H	Fill Operation Incomplete
07H	Key Parity Error (Parity Error)
08H	Wrong Key Type (Tag Mismatch)
0FH	CIK Failure
10H	CIK Not Inserted (CIK Time Out)
11H	ERROR, Update Limit Reached (Max Update)
12H	Internal Hardware Time Out
13H	Host Time Out
14H	Tamper/ Zeroize
15H	Fill Device Attached
16H	CIK Device Attached
17H	CIK Device Removed
18H	WARNING, Last Update allowed.

II. WINDSTER SPECIFIC ERROR/STATUS MESSAGES

BYTE	DESCRIPTION
60H	Failed Self Test
61H	EOM Detected
62H	Configuration Change, Read Status Byte 0
63H	Receive In Band Rekey
65H	VG
66H	VU
67H	Non Cooperative In Band Rekey
68H	Cooperative In Band Rekey
69H	Mode Error, Read Status Byte 3

Table 6-3. Error/Status Codes

7. INTERFACE SPECIFICATIONS

7.1 Detailed Interface Description

The interface signals to the WINDSTER COMSEC Module are shown in figure 7-1 and the pinout identification in Figure 7-2. These signals have been partitioned into ten interface ports.

- o The Fill Port provides the standard CSESD-11 interface signals. Keys are inserted here.
- o The Housekeeping Port includes a system clock and other signals necessary to setup the KGM.
- o The Command/Status Port is an eight bit bi-directional data bus.
- o The Command/Status Control Port contains the signals necessary to control the Command/Status Port.
- o The Transmit Channel Input includes the plain text data signal and the control signals necessary for its encryption and transmission.
- o The Transmit Channel Output consists of the cipher text output signal.
- o The Receive Channel Input consists of the cipher text input signal and clock.
- o The Receive Channel Output includes the plain text data signal and the control signals necessary for its decryption and reception.
- o The Crypto Ignition Key (CIK) Port allows the KGM to be rendered unclassified while still maintaining keys.
- o The Power Port contains the prime 5V DC input voltage along with the key retention voltage input

UNCLASSIFIED

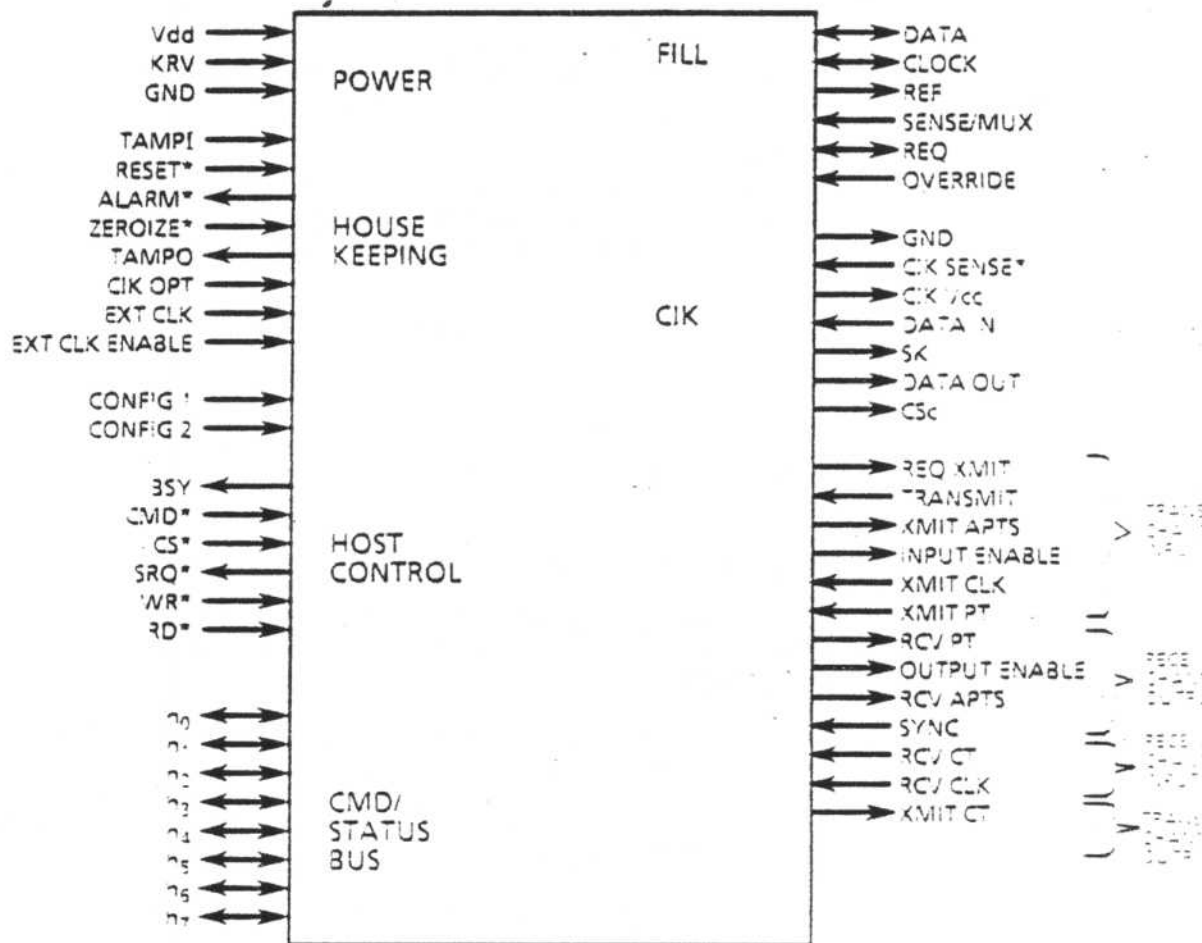


Figure 7-1. Interface Signals to the WINDSTER Module.

POWER	-----Vdd	+ 1	64 + DATA	-----	FILL
	GND	+ 2	63 + CLOCK		
	KRV	+ 3	62 + REF		
	GND	+ 4	61 + SENSE/MUX		
	Vdd	+ 5	60 + REQ		
HOUSE KEEPING	-----GND	+ 6	59 + OVERRIDE		CIK
	TAMPI	+ 7	58 + SPARE	-----	
	RESET*	+ 8	57 + CIK GND	-----	
	ALARM*	+ 9	56 + CIK SENSE*		
	ZEROIZE*	+ 10	55 + CIK Vcc		
	TAMPO	+ 11	54 + DATA IN		
	CIK OPT	+ 12	53 + SK		
HOST CONTROL	EXT CLK	+ 13	52 + DATA OUT		DATA CONTROL
	EXT CLK ENABLE	+ 14	51 + CS _c	-----	
	CONFIG 1	+ 15	50 + REQ XMIT	-----	
	-----CONFIG 2	+ 16	49 + TRANSMIT		
	BSY	+ 17	48 + XMIT APTS		
	CMD*	+ 18	47 + INPUT ENABLE		
	CS*	+ 19	46 + XMIT CLK		
	SRQ*	+ 20	45 + XMIT PT		
	WR*	+ 21	44 + RCV PT		
	RD*	+ 22	43 + SPARE		
CMD/ STATUS BUS	-----n0	+ 23	42 + SPARE		
	n1	+ 24	41 + SPARE		
	n2	+ 25	40 + OUTPUT ENABLE		
	n3	+ 26	39 + RCV APTS		
	n4	+ 27	38 + SYNC		
	n5	+ 28	37 + RCV CT		
	n6	+ 29	36 + RCV CLK		
	-----n7	+ 30	35 + XMIT CT	-----	
	SPARE	+ 31	34 + SPARE		
	SPARE	+ 32	33 + SPARE		

Figure 7-2. WINDSTER Pinout

7.1.1 Fill Port

The KGM is compatible with the CSESD-11 fill devices, including the KYX-15 (NCD), the KOI-18, and the KYK-13. The KGM will be compatible with the Data Transfer Device (DTD) when the DTD is operated in the common fill device emulation mode. This port also provides the key interface between the WINDSTER KGM and the future Key Management Module (KMM).

DATA - (bi-directional) Fill data line which transfers key information between the fill device and the KGM.

CLOCK - (bi-directional) Clock used to transfer key between the fill device and the KGM. The source of the key generates this clock.

REFERENCE - (output) WINDSTER ties this signal to an internal positive voltage. This provides a reference level to the CSESD-11 family of fill devices. This voltage is not to be used as a power supply to power most circuits.

SENSE/MUX - (input) A sense signal which indicates whether or not a fill device is attached. In NCD operations, this signal frames the MUX words.

REQUEST - (bi-directional) This signal initiates the transfer of the key; it is generated by the equipment that will receive the key.

OVERRIDE - (input) The NCD, or other remote control device, can control the WINDSTER KGM via this multiplexed serial input. A serial word is used for this control.

7.1.2 Housekeeping Port

CONFIG 1 and CONFIG 2 - (inputs) Selects WINDSTER Configuration.

ALARM* - (output) This is a latched output signal that results from an internal cryptographic alarm condition. It indicates that a failure occurred in the KGM and no further operation is possible. During the alarm test, this signal will toggle briefly to test the circuit, but this momentary alarm does not indicate a real alarm. An alarm is present when this signal is in the low state.

ZEROIZE* - (input) This asynchronous signal causes the KGM to immediately destroy all internally stored keys. The low state on this signal causes the zeroization to occur.

EXT CLK - (input) An externally supplied, though optional, (TBD) MHz squarewave clock signal which is used by the KGM's microcontroller.

EXT CLK ENABLE - (input) This signal instructs the KGM to use the externally supplied housekeeping clock. A high level selects the external clock.

RESET* - (input) This asynchronous signal causes the KGM to perform an initialization routine that sets the KGM to a known condition. Within the KGM this signal is pulled to Vdd through a (TBD) ohm resistor. A low level causes the reset to occur.

TAMPI - (input) This is one of the two tamper loop signals; if this loop is broken, then the KGM will be zeroized and further operation will be inhibited. The host can connect this loop through passive switches and sensors to the TAMPO signal. Thus, the KGM is warned if an attempt is made to tamper with the unit.

TAMPO - (output) This is second of the two tamper loop signals; the TAMPI signal description provides additional explanation.

CIK OPT - (input) This signal must be strapped high when the CIK function is desired.

7.1.3 Command/Status Port

h0-h7 - (bi-directional) This bi-directional and tri-stated I/O bus transfers the command and status bytes between the host and the KGM. h7 is the most significant bit (MSB).

7.1.4 Command/Status Control Port

CS* - (input) This input is used to select the KGM from other devices that may be connected to the Command/Status Port. It is used in conjunction with the RD* and WR* signals. CS* is pulled up to Vdd through a (TBD) ohm resistor. The signal is normally high, and serves to select the KGM when low.

BSY - (output) This output notifies the host that the KGM is momentarily unavailable for additional commands. A high level indicates that the KGM is busy.

SRQ* - (output) This signal is an asynchronous latched output to the host equipment. It informs the host that the KGM status register has valid information that is available to be read. An SRQ* is asserted any time the status of the KGM has changed. SRQ* is cleared when the status has been read. To request service, this signal is low.

RD* - (input) This host generated signal establishes that data is to be read from the KGM. This signal is only significant while the CS* signal is active. A low level indicates that the data will be read from the KGM.

WR* - (input) This host generated signal establishes that data is to be written to the KGM. This signal is only significant while the CS* signal is active. A low level indicates that the data will be written to the KGM.

CMD* - (input) This signal, when low, is used to notify the KGM that data on the COMMAND/STATUS BUS is an operator byte.

7.1.5 Transmit Channel Input Port

REQ XMIT - (output) This signal requests that the host activate its TRANSMIT signal. It is used when the KYX-15 is attached to the KGM to perform the transmit in-band rekey function. The KYX-15 commands the KGM to transmit, however, the KGM does not control the push-to-talk (PTT) switch. Thus the KGM can only request a transmission from its host equipment. A high level requests the transmission.

TRANSMIT - (input) This is a command from the host that tells the KGM to begin encrypting and outputting data from the XMIT CT line. A high level indicates that the data is ready.

XMIT APT - (output) This pseudo-random output pulse has a mean occurrence of once in 64 data rate bits. It can be used by the host to establish when cryptographic synchronization check bits can be put into the plain text stream. This signal is normally low, the pulse is high.

INPUT ENABLE - (output) This signal becomes true approximately 37 bits after the TRANSMIT input signal goes true. It marks the first bit of plain text input data to be encrypted. A high level indicates that the input is enabled.

XMIT CLK - (input) This squarewave will clock data out of the serial XMIT CT port and into the XMIT PT port.

XMIT PT - (input) This is the serial input data port for plain text to be encrypted by the KGM.

7.1.6 Transmit Channel Output Port

XMIT CT - (output) This is the serial output port for the data which was encrypted by the KGM.

7.1.7 Receive Channel Output Port

OUTPUT ENABLE - (output) This read request signal indicates that the KGM has decrypted the RCV CT data and the RCV PT signal is ready to be read. A high level on this signal indicates that the data is ready to be read.

SYNC - (input) This signal indicates that the next 37 bits to appear on the RCV CT line of the KGM are synchronization bits. The KGM will use these bits to place the receive key generator into a known cryptographic state. A high level causes the KGM to synchronize.

RCV APTS - (output) This signal alerts the host to look for a check bit in the receive plain text stream (see the XMIT APTS for a corresponding description). This signal enables the host to be compatible with various inventory COMSEC equipment. This signal is normally low, the alert high.

RCV PT - (output) This is the serial output port for data which was decrypted by the KGM.

7.1.8 Receive Channel Input Port

RCV CT - (input) This is the received cipher text data input line. It is a serial data input.

RCV CLK - (input) This squarewave signal clocks data into the RCV CT port and out of the RCV PT port.

7.1.9 Power Port

KRV - (input) This input provides a positive up voltage for the key storage RAM. The host should apply an uninterrupted voltage to this input to maintain the keys and other critical information when the main power is off.

Vdd - (input) This is the main switched power to the KGM.

GND - (input) Ground reference.

7.1.10 CIK Port

CSc - (output) Chip Select for the CIK. A high on this signal selects the CIK.

DATA OUT - (output) Serial output data to the CIK.

DATA IN - (input) Serial input data from the CIK.

SK - (output) Squarewave clock signal used to read and write data from the CIK.

CIK Vcc - (output) +5V power to the CIK.

CIK SENSE* - (input) Sense line used to determine if a CIK is attached. A low indicates the presence of a CIK.

GROUND - (output) Reference voltage for the CIK.

7.2 Electrical Signal Characteristics

7.2.1 Absolute Maximum Ratings

Absolute maximum ratings over which the KGM may be damaged:

Supply Voltage, Vcc -0.3 to +7.0 V
Input Voltage, GND - 0.3 <= Vin <= Vdd + 0.3 VDC

7.2.2 Electrical Power Requirements

1. Prime operating input voltage	Will have a value of -5 V +/- 5% Supplied by the host
----------------------------------	--

2. Key Retention Voltage Characteristics

- Voltage Range	Value of -5 V +/- 5%. KRV shall be supplied by the host.
-----------------	---

Current Drain	1 ma.
---------------	-------

7.2.3 Electrical Characteristics of I/O

7.2.3.1 LSTTL Bi-state

The Command/Status Bus Control Port, Receive Port, Transmit Port, and Housekeeping Port are LSTTL bi-state compatible signals. All outputs are capable of driving 4 LSTTL loads. Recommended operating conditions for these signals are shown in Table 7-1.

Table 7-1
Recommended Operating Conditions for LSTTL
Bi-state Compatible Module Signals

	MIN	TYP	MAX	
VOH - HIGH LEVEL OUTPUT VOLTAGE (I _{out} = 6.5 mA)	2.7	3.4		VOLTS
VOL - LOW LEVEL OUTPUT VOLTAGE (I _{out} = -1.6 mA)		.25	.4	VOLTS
t _{OR} - OUTPUT RISE TIME (CL = 20 pF)			20	nSEC
t _{OF} - OUTPUT FALL TIME (CL = 20 pF)			20	nSEC
VIH - HIGH LEVEL INPUT VOLTAGE	2.4			VOLTS
VIL - LOW LEVEL INPUT VOLTAGE			0.3	VOLTS
t _{IRD} - INPUT RISE TIME, DATA	10		100	nSEC
t _{IFD} - INPUT FALL TIME, DATA	10		100	nSEC
t _{IRC} - INPUT RISE TIME, CLOCK	10		100	nSEC
t _{IFC} - INPUT FALL TIME, CLOCK	10		100	nSEC
I _{IH} - HIGH LEVEL INPUT CURRENT			1	uA
I _{IL} - LOW LEVEL INPUT CURRENT			1	uA
INPUT CAPACITANCE			30	pF

7.2.3.2 LSTTL Tri-state

The Command/Status Bus is an LSTTL tri-state compatible bus. Recommended Operating Conditions for Tri-state LSTTL Module Signals are shown below in Table 7-2.

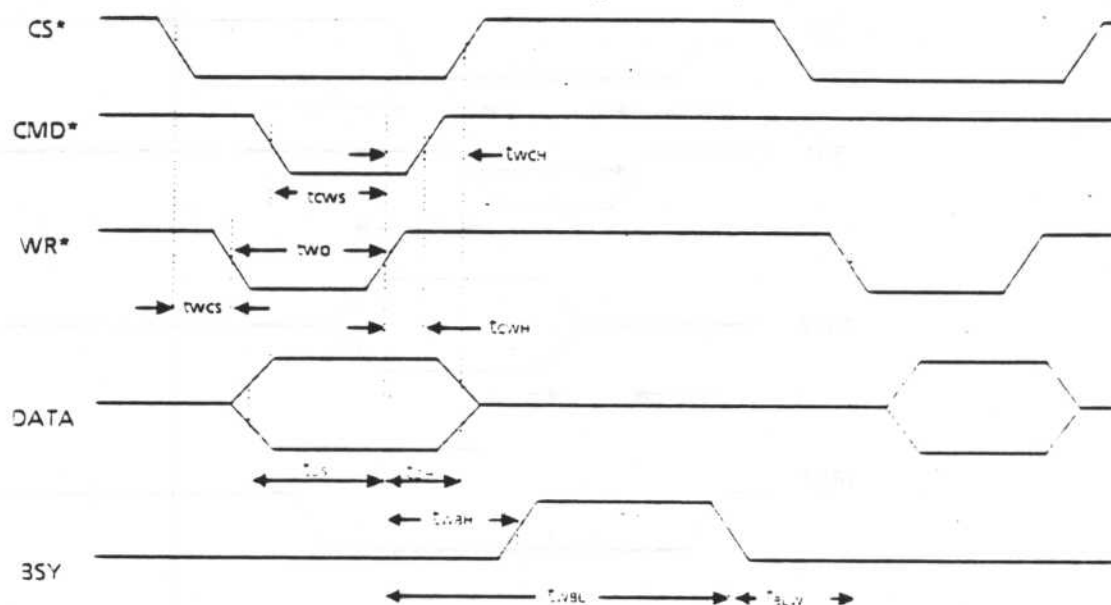
TABLE 7-2
Recommended Operating Conditions for LSTTL
Tri-state Compatible Module Signals

	MIN	TYP	MAX	UNITS
VOH - HIGH LEVEL OUTPUT VOLTAGE (I _{out} = 7.13 mA)	2.4			VOLTS
VOL - LOW LEVEL OUTPUT VOLTAGE (I _{out} = -1.93 mA)			0.5	VOLTS
t _{OR} - OUTPUT RISE TIME (CL = 20 pF)			20	nSEC
t _{OF} - OUTPUT FALL TIME (CL = 20 pF)			20	nSEC
VIH - HIGH LEVEL INPUT VOLTAGE	2.4			VOLTS
VIL - LOW LEVEL INPUT VOLTAGE			0.3	VOLTS
t _{IRD} - INPUT RISE TIME, DATA	10		100	nSEC
t _{IFD} - INPUT FALL TIME, DATA	10		100	nSEC
I _{IH} - HIGH LEVEL INPUT CURRENT			1	uA
I _{IL} - LOW LEVEL INPUT CURRENT			1	uA
INPUT CAPACITANCE			30	pF

7.3 Product Timing Relationships

7.3.1 Signal Timing Relationships

7.3.1.1 Write Cycle



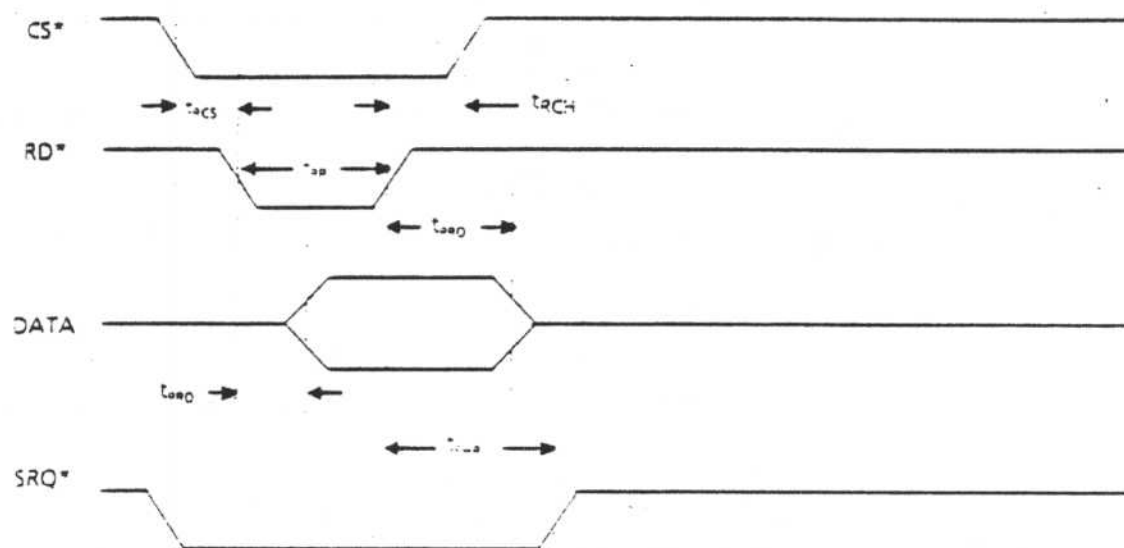
	MIN	TYP	MAX	UNITS
tWCS - SET-UP TIME, CS* TO WR* (TIME CS* MUST BE LOW BEFORE WR* GOES LOW)	0			nSEC
tWCH - HOLD TIME, WR* TO CS* (TIME CS* MUST REMAIN LOW AFTER WR* GOES HIGH)	0			nSEC
tWP - WRITE PULSE WIDTH	110			nSEC
tCWS - SET-UP TIME, CMD* TO WR* (TIME CMD* MUST BE LOW BEFORE WR* GOES HIGH)	25			nSEC
tCWH - HOLD TIME, CMD* TO WR* (TIME CMD* MUST REMAIN LOW AFTER WR* GOES HIGH)	0			nSEC
tDS - DATA SET-UP TIME	45			nSEC
tDH - DATA HOLD TIME	45			nSEC
tWBH - DATA RECOGNITION TIME (TIME BETWEEN WR* GOING HIGH AND BUSY GOING HIGH)	140			nSEC
tWBL - OPERATION COMPLETE TIME (TIME BETWEEN WR* GOING HIGH AND BSY GOING LOW)	WILL VARY WITH TYPE OF OPERATION			
tBLW - NEXT WRITE CYCLE (TIME BETWEEN BSY GOING LOW AND WR* GOING LOW)	0			nSEC

Write Cycle Waveform Relationships

FIGURE 7-3

NOTE: CMD* is only required when an operator byte is placed on the data bus.

7.3.1.2 Read Cycle

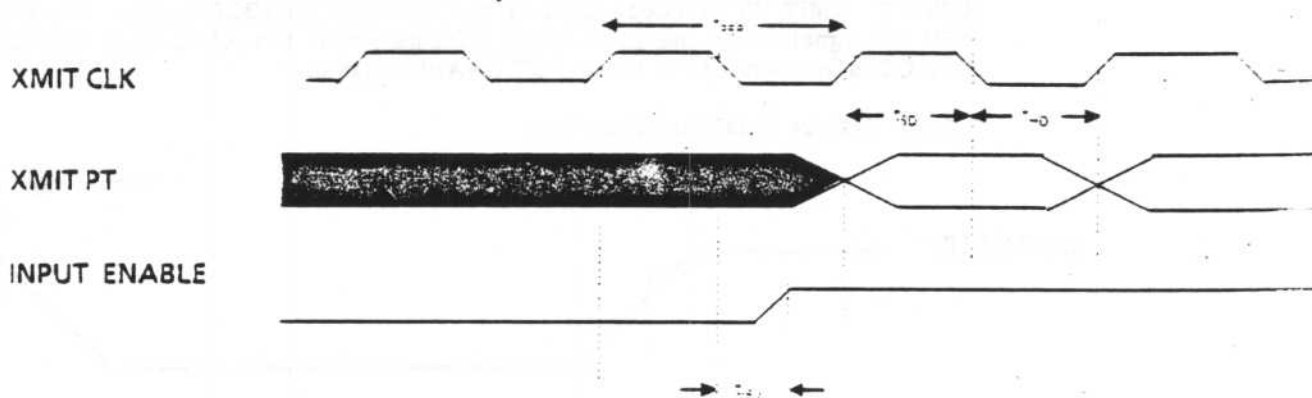


	MIN	TYP	MAX	UNITS
t_{RCS} - SET-UP TIME, CS* TO RD* (TIME CS* MUST BE LOW BEFORE RD* GOES LOW)	0			nSEC
t_{RCH} - HOLD TIME, RD* TO CS* (TIME CS* MUST REMAIN LOW AFTER RD* GOES HIGH)	0			nSEC
t_{RP} - READ PULSE WIDTH	150			nSEC
t_{PRD} - PROPAGATION DELAY	110			nSEC
t_{SHR} - STATUS READ FROM KGM* (TIME BETWEEN RD* GOING HIGH AND SRQ* GOING HIGH)			160	nSEC

Read Cycle Waveform Relationships
FIGURE 7-4

NOTE: The SRQ* and BSY signals are not required from the KGM in order for the host to execute a read. (See section 7.1.4).

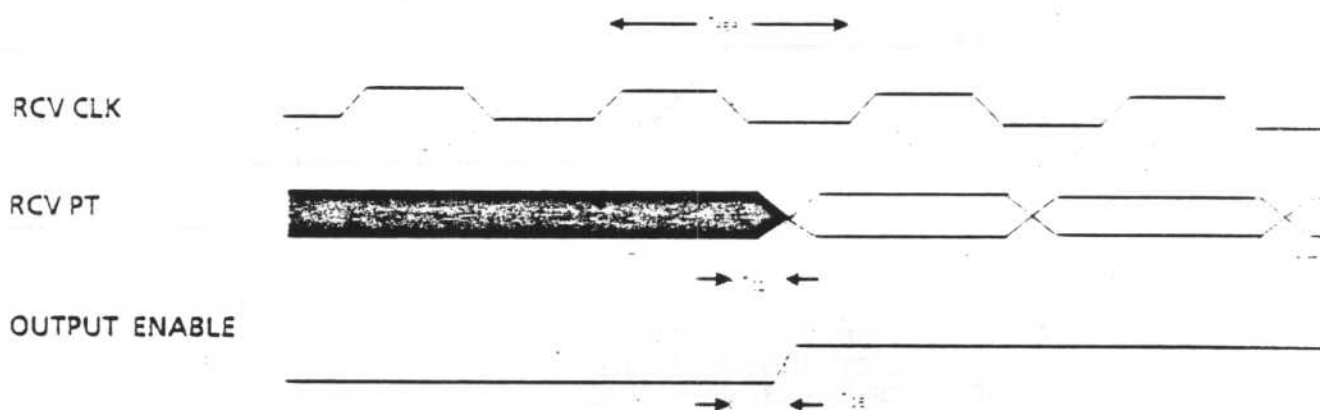
7.3.1.3 Traffic Data/Clock Input



	MIN	TYP	MAX	UNITS
t_{PER} - PERIOD	5			nSEC
t_{SD} - DATA SET-UP TIME	30			nSEC
t_{HD} - DATA HOLD TIME	30			nSEC
t_{IEV} - INPUT ENABLE VALID (TIME BETWEEN CLOCK GOING HIGH AND INPUT ENABLE GOING HIGH)			300	nSEC

Traffic Data/Clock Input Waveform Relationships
FIGURE 7-5

7.3.1.4 Traffic Data/Clock Output

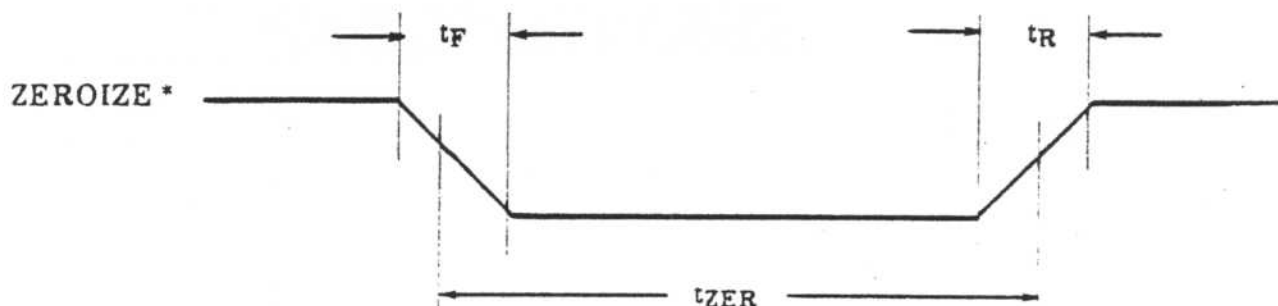


	MIN	TYP	MAX	UNITS
t_{PER} - Period (WILL TRACK TRAFFIC INPUT CLOCK)		5		nSEC
t_{CD} - CLOCK TO DATA DELAY			130	nSEC
t_{OEV} - OUTPUT ENABLE VALID (TIME BETWEEN CLOCK GOING LOW AND OUTPUT ENABLE GOING HIGH)			300	nSEC

Traffic Data/Clock Output Waveform Relationships
FIGURE 7-6

NOTE: Delay information for XMIT CLK and XMIT CT is the same as RCV CLK and RCV PT. XMIT CT is independent of the OUTPUT ENABLE signal. The RCV CLK and RCV CT signals have the same delay information as the XMIT CLK and the XMIT PT. RCV CT is independent of the INPUT ENABLE signal.

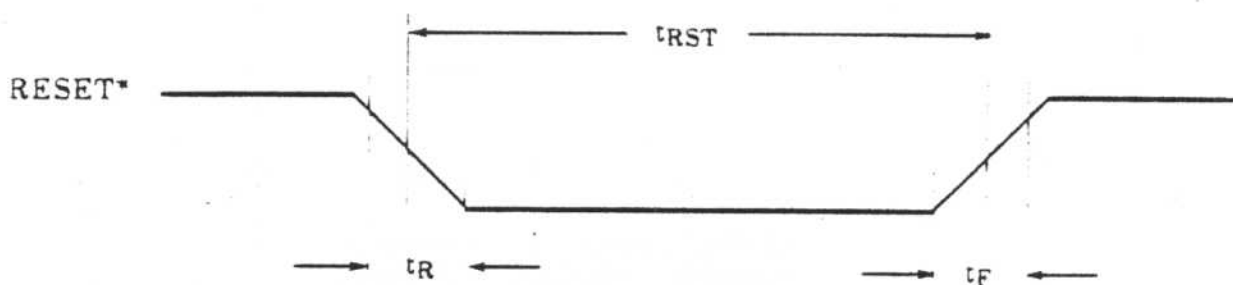
7.3.1.5 Zeroize Pulse Specifications



	MIN	TYP	MAX	UNITS
t_{ZER} - ZEROIZE PULSE WIDTH	20			nSEC
t_R - ZEROIZE PULSE RISE TIME	10		100	nSEC
t_F - ZEROIZE PULSE FALL TIME	10		100	nSEC

Zeroize Pulse Waveform Specifications
FIGURE 7-7

7.3.1.6 Reset Pulse Specifications



	MIN	TYP	MAX	UNITS
t_{RST} - RESET PULSE WIDTH	5			nSEC
t_R - RESET PULSE RISE TIME	10		100	nSEC
t_F - RESET PULSE FALL TIME	10		100	nSEC

Reset Pulse Waveform Specifications
FIGURE 7-8

7.4 Fill Port Interface Requirements

The Fill Port interface signals are compatible with the interface requirements of CSESD-11 (COMMUNICATIONS SECURITY EQUIPMENT SYSTEM DOCUMENT FOR FILL DEVICES). The Fill Port clock, data, and request lines are bi-directional to support in-band rekey operations as well as future Key Management Module interface requirements. Each input line is electronically protected to prevent damage from the high negative voltages which the fill devices may possibly generate.

8. MECHANICAL INTERFACE SPECIFICATIONS

8.1 Interface Cabling, Connectors

The host shall provide an interface board for mounting the KGM. The board shall be connected to the host equipment with cables and/or connectors consistent with the host configuration.

The host shall provide a direct connection between a fill connector located on its external surface and the fill port of the KGM. The fill connector is specified by the Government drawing 0N241775. The direct connection between the fill port and fill connector shall be achieved through a shielded, or equivalently protected, cable.

8.2 Module Envelope

Refer to figure 8-1 WINDSTER Module Envelope

8.3 Detailed Footprint

Refer to figure 8-2 WINDSTER Detailed Footprint

8.4 KRV Requirements

The KRV is an option. The addition of a key retention voltage will enable the KGM to retain all keys when main power is removed. If this option is not selected, the preferred approach is to wire this pin in common with prime power. If KRV is not present when prime power is removed, the contents of all storage registers and RAM is lost.

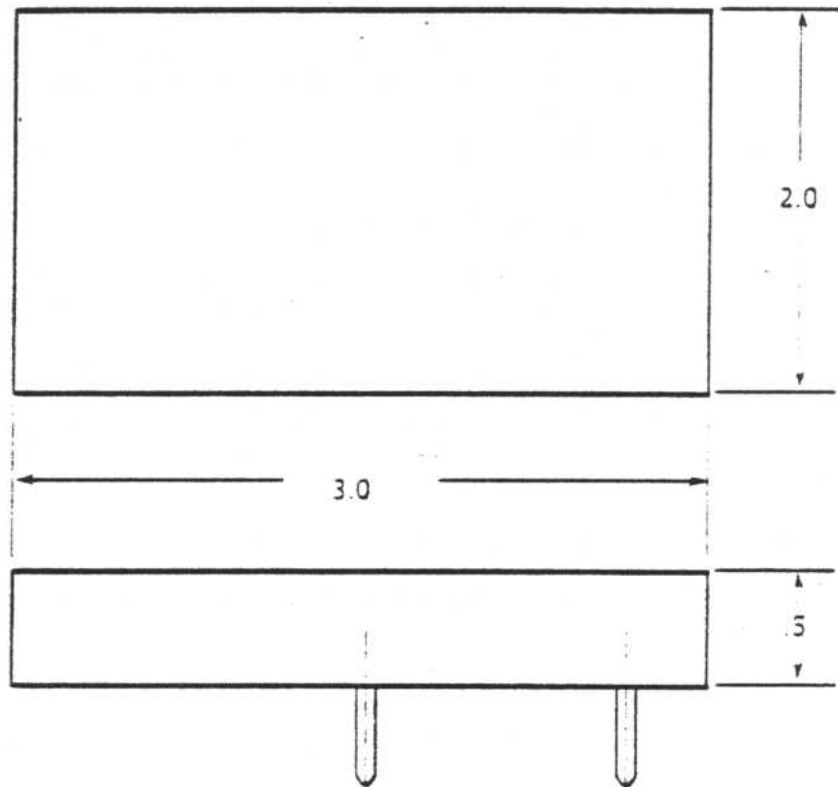


Figure 8-1 Windster KGM Envelope

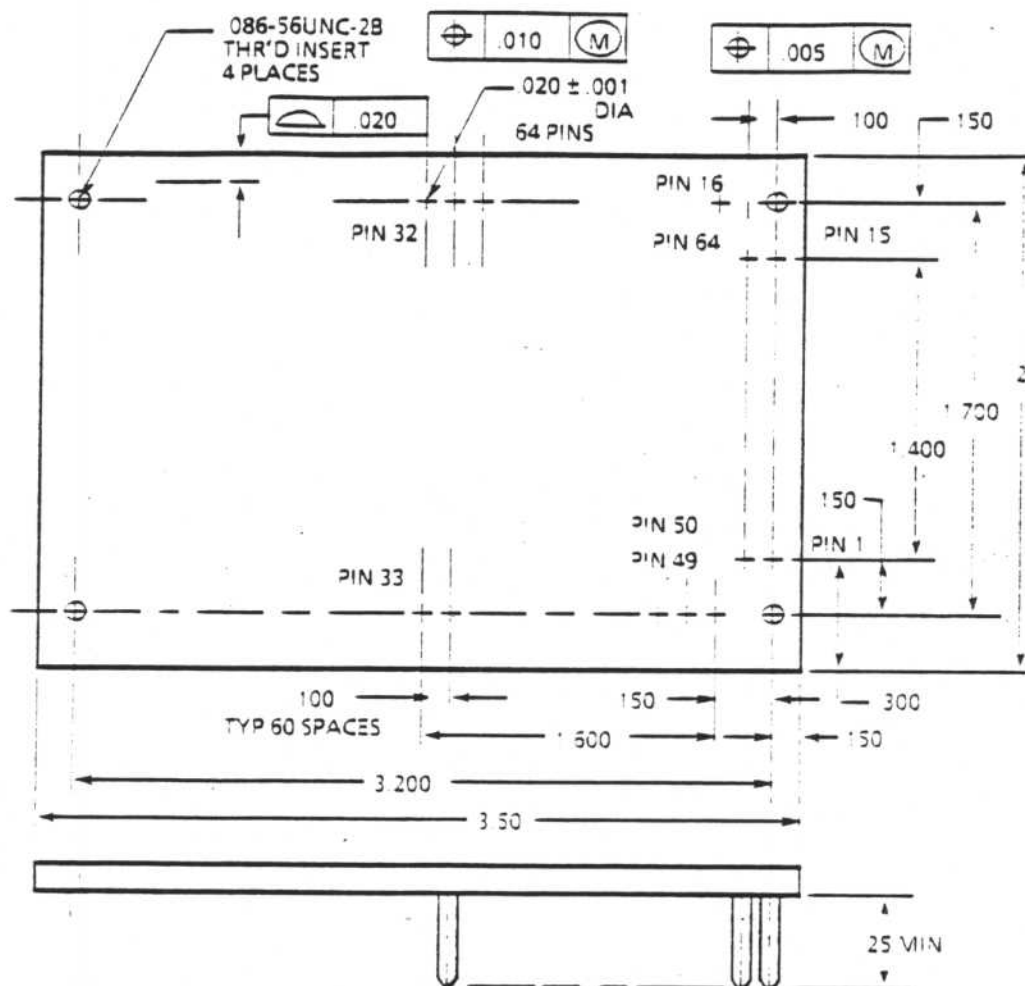


FIGURE 8-2 WINDSTER KGM DETAILED FOOTPRINT

FOR OFFICIAL USE ONLY