

iKGM-100 Advanced Key Generation Module

- Designed Under NSA's Project Overtake
- Minimized Time to Market
- Asynchronous 7Mbit/sec, Half Duplex Operation in Selected Modes
- 16 Bit Parallel LSTTL Interface
- Controlled and Auditable Bypass
- 8 or 16 Bit Host Support
- Self Test
- Message Authentication Code Mode
- Compatible with KOI 18 Common Fill Device and DTD (CSESD-II Configuration)
- Storage for 255 Keys
- Key Unwrapping/Wrapping Capability
- OTAR Capability
- Support for CIK
- 5 Volt, Low Power Operation
- Operates on 8, 64, and 128 bit Block Boundries

The iKGM-100 is a member of the National Security Agency's family of standard embeddable COMSEC products. The iKGM-100 advanced key generation module is the result of an NSA sponsored design effort to provide the COMSEC community with a security module for medium to high bandwidth data communications.

Included in the iKGM-100 are several security features and cryptographic operational modes. The security features in the iKGM-100 are intended to reduce the amount of time required to design COMSEC equipment by providing an NSA endorsed set of security features. Proper implementation of the security features found in the iKGM-100 should result in greatly reduced NSA evaluation and endorsement time, thus improving time to market.

The iKGM-100 is a general purpose half duplex cryptographic device capable of providing COMSEC protection of digital data at all classification levels. The iKGM-100 is designed to support a wide variety of system architectures by acting as an intelligent slave to the host terminal equipment. The microprocessor compatible interface and control structure is highly flexible, and the powerful command set will permit the host equipment developer to select the most efficient modes of operation to satisfy unique system requirements.

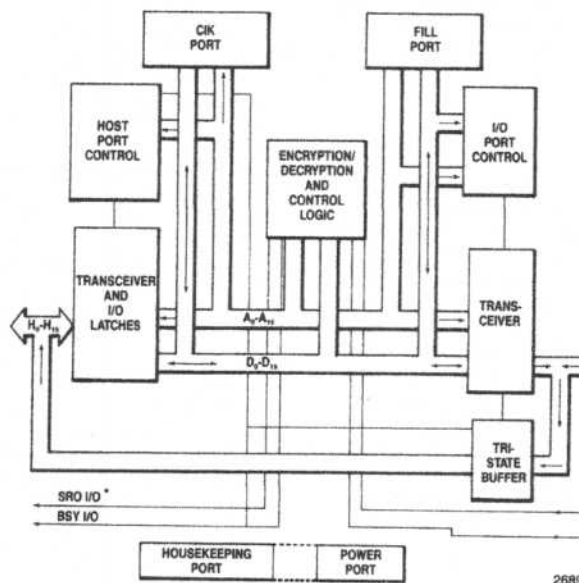


Figure 1. iKGM-100 Block Diagram

Intel Corporation assumes no responsibility for the use of any circuitry other than circuitry embodied in an Intel product. No other circuit patent licenses are implied. Information contained herein supersedes previously published specifications on these devices from Intel.

© Intel Corporation, 1987

OCTOBER 1987
Order Number: 280713-001

ARCHITECTURAL DESCRIPTION

A block diagram of the iKGM-100 is shown in Figure 1. The iKGM-100 is designed to work in either 8-bit or 16-bit bus systems. All commands and responses from the iKGM-100 are 8 bits, independent of mode. For data, the 16 bit configuration is the default.

The iKGM-100 has 6 ports — Host port, I/O port, Fill port, CIK port, Housekeeping port, and Power port — which are described in detail below. Throughout this data sheet, an * in conjunction with a signal name indicates an active low signal.

In this data sheet, the term "Host" refers to the vendor designed equipment which supports the iKGM-100. Examples of a "Host" might be LAN controller, rotating magnetic media controller or a link communications controller.

Host Port

The host port circuitry includes a 16-bit transceiver latch, and port control logic. Eight or sixteen-bit data words or 8-bit command words pass from the host into the iKGM-100. Data and status words may also pass from the iKGM-100 back to the host. All data, commands and status which are transferred between the iKGM-100 and the host, pass over the host port lines. This includes words read from the I/O port, words read from the host port latch, and also commands and data written to the iKGM-100 by the host. The port control circuitry provides handshaking and timing signals for the host port. The proper operation of the host port is checked during the SELF TEST command process.

I/O Port

The I/O circuitry includes port control logic, a 16-bit transceiver and a 16-bit tri-state buffer. Data and commands pass from the iKGM-100 to the I/O through the transceiver. A tri-state buffer permits 16 bits of data coming from the I/O to bypass through the iKGM-100 to the host. This bypass circuit was included in the iKGM-100 to prevent the iKGM-100 from slowing down the I/O, and so that the host builder will not be required to provide security analysis for the circuit. The service request (SRQⁱ) and the busy (BSYⁱ) are used by the iKGM-100 and sent to the host to synchronize data flow from the I/O port. The host port control circuitry provides handshaking and timing signals for the I/O port. The proper operation of the I/O port is checked during the self test.

Fill Port

The fill port is used to load RED key into the iKGM-100. These keys can be stored for use inter-

nally while power is on, or encrypted and stored in the host if a CIK (crypto ignition key) is connected. The fill port is designed according to the specifications of CSESD-11 (see Note 1). The KOI-18 is the only fill device which is capable of loading a 256-bit key packet. The KOI-18 does not use the OVER-RIDE and REQ* fill port pins. These additional fill port pins have been included so that future key fill devices can be interfaced to the iKGM-100. The fill port on the iKGM-100 is intended to be attached to the external fill connector by a shielded fill cable, which is a host responsibility. This circuit is checked during the self test.

Note 1: The CSESD-11 Edition I is the abbreviation for the Communication Security Equipment System document. This document is classified confidential and can be acquired from the NSA.

CIK Port

The Crypto Ignition Key (CIK) port has been designed to interface directly to a CIK. The iKGM-100 drives the CIK directly. Use of the CIK in conjunction with the iKGM-100 is optional. The iKGM-100 can be configured for CIK option by tying the CIK OPT pin high, in which case a CIK is required for operation of the iKGM-100. Tying CIK OPT low indicates to the iKGM-100 that a CIK will not be employed. This circuit is checked during the self test.

Housekeeping Port

The housekeeping port provides a means of implementing various security features. These features are summarized below:

ZEROIZE — This feature provides the ability to zeroize all volatile storage within the iKGM-100 and causes the iKGM-100 to reset. No red information will be retained after the zeroize function is complete. The "zeroize" function is invoked by grounding the "zeroize pin".

RESET — The RESET is used by the host to return the iKGM-100 to a known initial state. Grounding and releasing this pin has the same affect on the iKGM-100 as turning the power off and back on again. All RED information will be purged from the iKGM-100. Once reset, the iKGM-100 will respond with a "Ready for Self Test" status message and await a SELF TEST command from the host. Self test must be completed before any other command processes will be executed.

TAMPER — The tamper feature provides support for a current loop which is serviced by the host for tamper protection. If this current loop is broken, the

iKGM-100 "zeroizes" and "resets" as described above. The current loop pins are identified as "Tamper 1" and "Tamper 0".

ALARM — When the iKGM-100 detects an internal failure, it will ground the ALARM pin. The alarm output can be used by the host to activate an audible or visual alarm. When in an alarm condition, the iKGM-100 stops all internal processing, sets the ports to high impedance and will not output any data or accept any commands. An alarm can be cleared by performing a hardware reset (grounding the RESET* pin), zeroizing (grounding the ZEROIZE* pin), or cycling power off/on.

SYSTEM MGR* — The System Manager pin is used to select either System Manager (ground) or Node (+5V) operating configurations.

CIK OPT — The CIK Option is used to configure the iKGM-100 to function with a CIK (CIK Option pin tied to +5V) or to function without a CIK (CIK Option pin tied to ground). This CIK opt function is sampled during iKGM-100 initialization and should not be changed during operation.

Power Port

This port provides a means of accepting prime power input for the iKGM-100. The host provides +5V DC power to the iKGM-100. Internally, the iKGM-100 has low power detection circuitry. If power is interrupted, the low power detector will reset the iKGM-100. The host reset and zeroize signals can also be used to reset the iKGM-100 when the host detects low power.

CRYPTOGRAPHIC OPERATING MODES

The iKGM-100 has 6 cryptographic modes of operation. They are referred to as modes A, B, C, D, E, and F for both encryption and decryption. The selection of which mode of operation for data processing is based on system requirements. Each data processing mode offers unique synchronization and error

extension features. A Message Authentication Code (MAC) function is also available. Both data and commands may be bypassed through the iKGM-100 from the host to the I/O. A Bypass Control Word within the iKGM-100 determines the allowable amount of bypass.

KEY PROCESSING METHODS

Secure communication systems rely heavily on the secure, timely and relatively transparent distribution of keys. This process is referred to as the key management system. The iKGM-100 provides the means for communication system developers to custom design a key management architecture that "fits" the application. Internal active storage of multiple keys, local (within the host equipment) storage of encrypted keys, crypto ignition key, remote electronic rekeying, and key updating are all available for use in the iKGM-100.

COMSEC COMMAND LANGUAGE (CCL)

The COMSEC command language (CCL) has been developed to support NSA's standard line of key generation modules. The CCL forms the software interface standard for the iKGM-100. Future evolutions of the iKGM-100 will be compatible with the CCL.

Table 1 lists the commands available on the iKGM-100.

MODULE ELECTRICAL INTERFACE

Figure 2 and Table 2 show the iKGM-100 connector electrical connections and pin descriptions, respectively. The module is mechanically attached to the host via the electrical connector mounting holes and 4 additional mounting holes in the corners of the module. Figure 3 depicts a typical mounting arrangement.

Table 1. COMSEC Command Language

SELF TEST	STOP
LOAD RED KEY	ABORT
LOAD RANDOM SEED KEY	LOAD BYPASS CONTROL WORD
ACTIVATE CIK	READ BYPASS AUDIT
TRANSFER KEY	SET 8-BIT MODE
VALIDATE KEY	SET 16-BIT MODE
WRAP RED KEY FOR STORAGE	SET DECRYPT DIRECT
UNWRAP STORED BLACK KEY	SET DECRYPT VIA HOST
UNWRAP RANDOM SEED KEY	SET ENCRYPT PATH AS COPROCESSOR
DECRYPT REMOTE KEY	SET ENCRYPT PATH TO OUTPUT
UNWRAP BLACK OTAR KEY	RESET RANDOM SEED KEY FLAG
ZEROIZE	COMMAND BYPASS
ZEROIZE ALL	PREPARE REMOTE REKEY MESSAGE CONTAINING TRAFFIC KEYS BEGINNING AT AND NEW KEY ENCRYPTION KEY, ENCRYPTED USING KEY ENCRYPTION KEY
COPY RED KEY	
UPDATE RED KEY	ENCRYPT BYPASS CONTROL WORD USING KEY ENCRYPTION KEY
ENCRYPT WITH RESYNC	
ENCRYPT WITHOUT RESYNC	DECRYPT BYPASS AUDIT WORD USING KEY ENCRYPTION KEY
DECRYPT WITH RESYNC	
DECRYPT WITHOUT RESYNC	
MESSAGE AUTHENTICATION CODE MODE (MAC)	
END OF MESSAGE	
END OF MESSAGE MIDDLE OF WORD	
SET MODE	
RESTART	

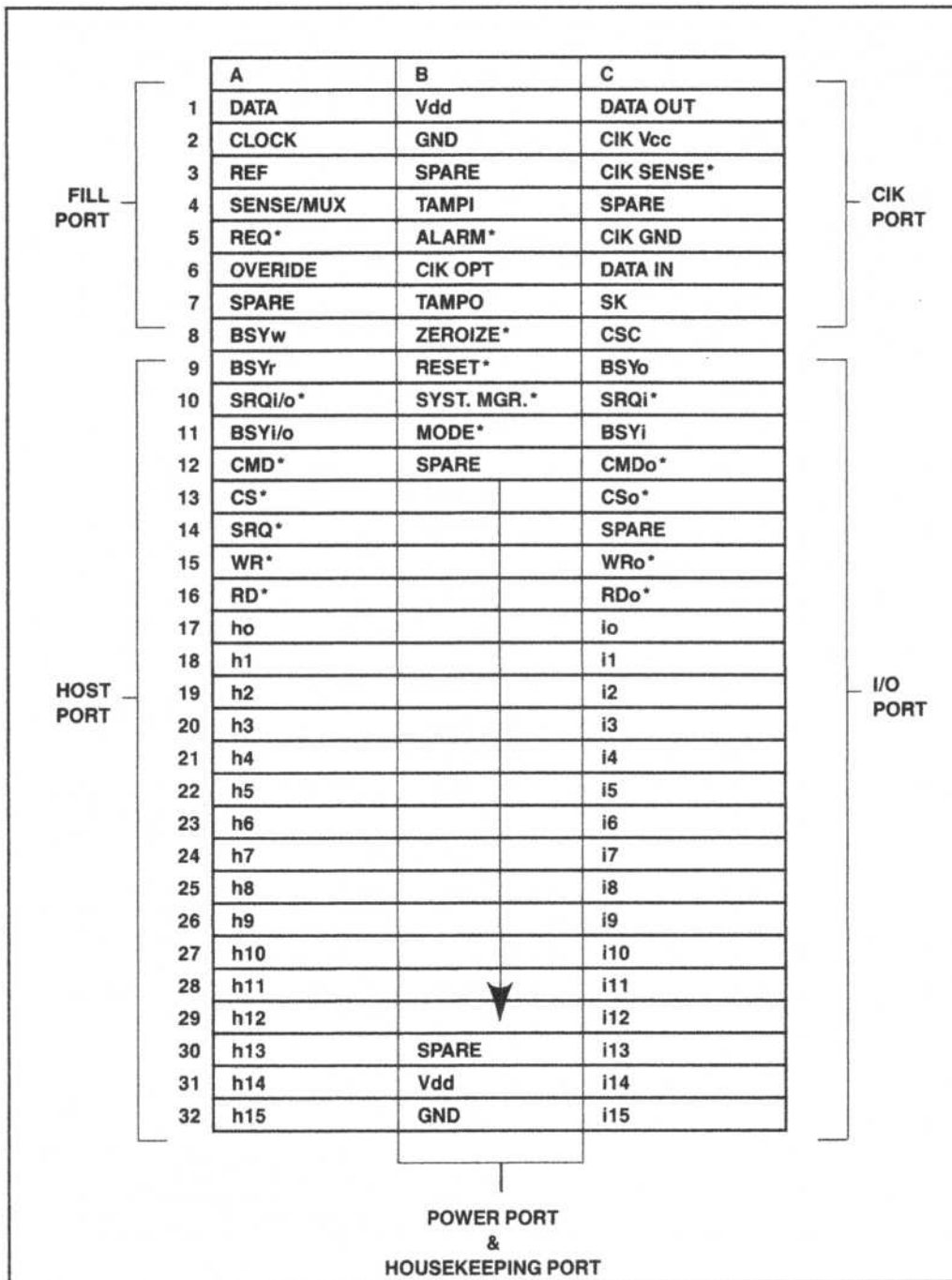


Figure 2. TEPACHE Pinout

Table 2. Pin Description

Pin	Name	Type	Description
B1&B31	Vdd	I	POWER SUPPLY + These pins contain the input power for the iKGM-100, regulated 5V DC.
B2&B32	GND	O	POWER SUPPLY GROUND These pins are also the reference for all signals.
A7,B3,C4	SPARE		Spare pins
B12-B30,C14	SPARE		Spare pins
B4	TAMPI	I	TAMPER IN This line senses current flow in a tamper loop using TAMPER OUT as a source. If TAMPER IN voltage is low (<.7V), then tamper will be detected. Tamper detection will cause an automatic zeroize and subsequent iKGM-100 reset.
B9	RESET*	I	RESET When RESET* = 0 it causes the iKGM-100 to zeroize; and when RESET* = 1, to begin its initialization.
B5	ALARM*	O	ALARM Under normal conditions, ALARM* = 1. When an alarm is present in the iKGM-100, ALARM* = 0.
B8	ZEROIZE*	I	ZEROIZE When this pin is grounded, all RED keys within the iKGM-100 are erased. It will also result in a iKGM-100 reset.
B7	TAMPO	O	TAMPER OUT The tamper out line is +5V, current limited to 10mA. This line is used as a source for TAMPER IN.
B6	CIK OPT	I	CIK OPTION When this pin is high, the iKGM-100 is configured to utilize a CIK. This pin is sampled during iKGM-100 initialization and should not be changed while the iKGM-100 is in operation.
B10	SYSTEM MGR*	I	SYSTEM MANAGER When this pin is connected to ground, the iKGM-100 is configured as a System Manager. When it is connected to 5V, the iKGM-100 is configured as a Node.
A8	BSYw	O	BUSY WRITE When BSYw = 1 the iKGM-100 is notifying the host that the iKGM-100 input buffer is full or that the iKGM-100 is performing a task and not ready for new data or a command.
A9	BSYr	O	BUSY READ When BSYr = 0, the iKGM-100 is notifying the host that new data is in the host port output buffer and that the host can do a read of the iKGM-100.
A10	SRQi/o*	O	I/O SERVICE REQUEST SRQi/o* is a direct feed-through from the SRQi* signal from the I/O port.
A11	BSYi/o	O	I/O BUSY When BSYi/o = 1, the iKGM-100 is notifying the host that the I/O is not ready to be read by the host or that the iKGM-100 is addressing the I/O. The iKGM-100 sets BSYi/o = 1 when encrypting data or decrypting data received directly from the I/O port.

Table 2. Pin Description (continued)

Pin	Name	Type	Description
B11	MODE*	I	MODE When this pin is connected to 5V, continued state operation of modes A, B, and C is not allowed and mode F cannot be used.
A12	CMD*	I	This signal is used by the host to specify whether command or data is being written to the iKGM-100 or read from the iKGM-100 or from the I/O.
A13	CS*	I	CHIP SELECT Signal from host. Alerts iKGM-100 that the host will perform a Read or Write.
A14	SRQ*	O	SERVICE REQUEST The iKGM-100 will bring SRQ* = 0 (latched output) when a status word is available in the host port output buffer. When the host performs a read of the iKGM-100, the SRQ* latch is released (SRQ* = 1).
A15	WR*	I	WRITE STROBE When WR* is strobed low, the host reads a word into the iKGM-100.
A16	RD*	I	READ STROBE When RD* is strobed low, the host reads a word from the iKGM-100 or the I/O.
A17-A32	h0-h15	I/O	HOST BUS h0-h15 are bidirectional data lines used to communicate between the host and iKGM-100.
C17-C32	i0-i15	I/O	I/O LINES i0-i15 are bidirectional data lines used to communicate between the iKGM-100 and I/O.
C16	RDo*	O	I/O READ STROBE When RDo* is strobed low by the iKGM-100, it reads a word from the I/O or sends it to the host.
C15	WRo*	O	I/O WRITE STROBE When WRo* is strobed low by the iKGM-100, it writes a word into the I/O.
C13	CSo*	O	I/O CHIP SELECT The iKGM-100 uses this signal CSo* = 0 to notify the I/O that is is being addressed.
C12	CMDo*	O	This signal is used by the iKGM-100 to specify whether command or data is being written to the I/O or a read is being performed by the iKGM-100 or host.
C11	BSYi	I	INPUT BUSY When BSYi = 1, the I/O is notifying the iKGM-100 that it is not ready to be written to.
C10	SRQi*	I	I/O INTERRUPT This signal is fed through to the SRQi/o* pin on the host port and also used by the iKGM-100 for control.
C9	BSYo	I	I/O BUSY When BSYo = 1, the I/O is notifying the iKGM-100 that it is not ready to be read.
C8	CSC	O	CIK CHIP SELECT Chip Select for CIK. The iKGM-100 uses this signal CSc = 1 to notify the CIK that it is being addressed.
C1	DATA OUT	O	Data output to CIK.
C7	SK	O	CIK CLOCK Clock for CIK.
C6	DATA IN	I	Data input from CIK.
C2	CIK VCC	O	CIK Power +5V power to CIK.

Table 2. Pin Description (continued)

Pin	Name	Type	Description
C3	CIK SENSE*	I	CIK Sense Sense line for CIK, 0V when CIK attached.
C5	CIK GND	I	CIK Ground Ground for CIK.
A6	OVERRIDE	I	OVERRIDE FILL (Not Used)
A5	REQ*	O	FILL REQUEST The iKGM-100 pulls this signal low to initiate a fill process if required by the fill device.
A4	SENSE/MUX	I	FILL SENSE/MUX When SENSE/MUX = +5V, it signifies to the iKGM-100 that a fill device is attached.
A3	REF	O	FILL LOGIC LEVEL REFERENCE This pin is used as a logic reference for the fill device. It is not intended to be used as a power supply to power circuits. It is nominally +5V DC.
A2	CLOCK	I	FILL CLOCK This pin carries the clock signal for clocking data into the iKGM-100 over the fill port.
A1	DATA	I	FILL DATA This pin carries data synchronized by the FILL CLOCK.

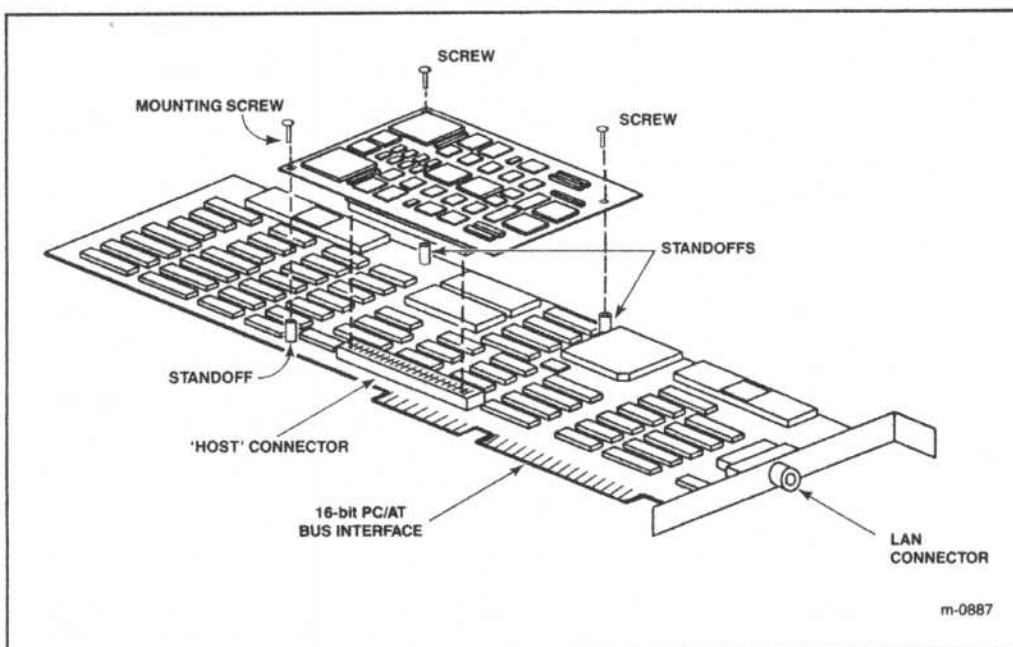


Figure 3. Typical Mounting Arrangement

SPECIFICATIONS**Environmental Characteristics**

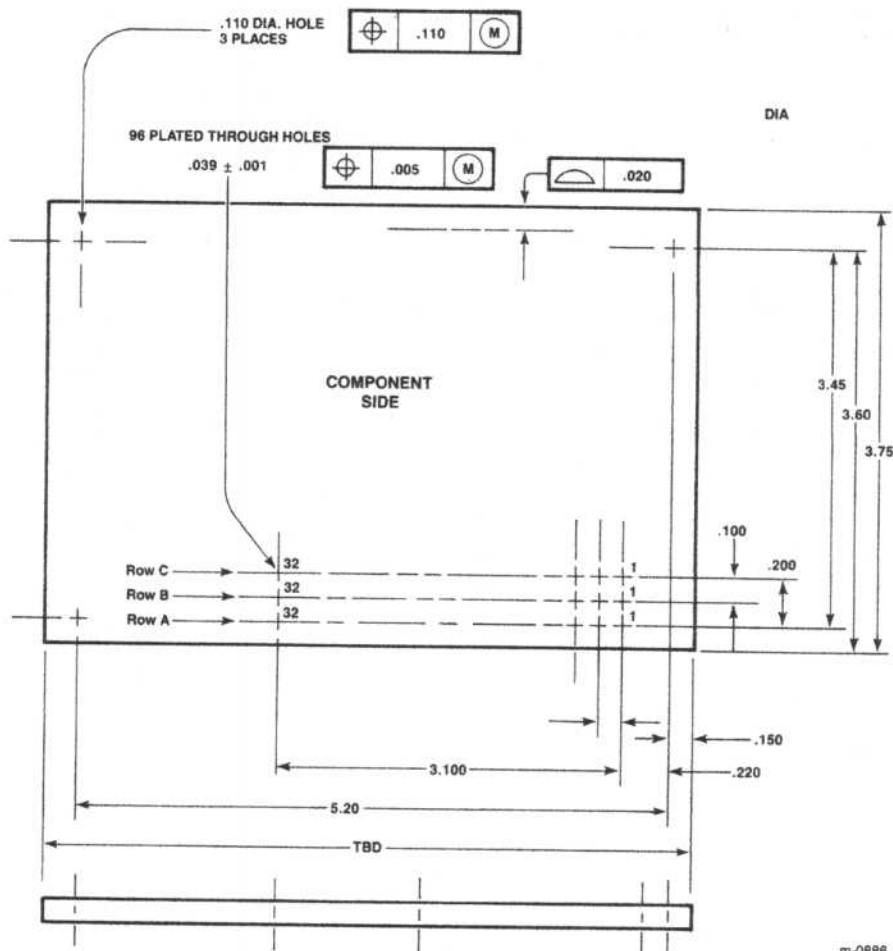
Temperature: 0 to 55 C ambient temperature with surface temperature not to exceed 70° C or be lower than 0° C
 Humidity: to 90% noncondensing (25 C to 70 C)

DC Electrical Characteristics

$V_{CC} = 5V \pm 5\%$
 $ICL = 5 \text{ watts} \pm 5\%$
 $PD = 5 \text{ watts} \pm 5\%$
 Absolute maximum voltages on any pin with respect to ground: $-0.3V$ to $7.0V$

Physical Characteristics

Width: 3.75"
 Length: TBD
 Height (with connector): 0.368"
 Weight: 4.5 ounces



m-0886

Figure 4. Mechanical Configuration