WESTERN DIGITAL
CORPORATION

WD2001/WD2002 Data Encryption Devices

FEATURES

- CERTIFIED BY NATIONAL BUREAU OF STANDARDS.
- TRANSFER RATE: 1.3M BITS/SEC (2 MHz CLOCK) (HIGHER SPEEDS AVAILABLE)
- ENCRYPTS/DECRYPTS 64 BIT DATA WORDS USING 56 BIT KEY WORD
- SINGLE PORT 28 PIN PACKAGE WD2001 OR DUAL PORT 40 PIN PACKAGE WD2002
- COMMAND BIT PROGRAMMING VIA DAL BUS OR INPUT PINS
- DMA COMPATIBLE (SEE WESTERN DIGITAL DM1883)
- PARITY CHECK ON KEY WORD LOADING
- STANDARD 8 BIT MICROPROCESSOR INTERFACE
- INPUTS AND OUTPUTS TTL COMPATIBLE
- KEY STORED ON CHIP IS NOT EXTERNALLY ACCESSIBLE
- SEPARATE CLEAR AND CIPHER BUS STRUCTURE ON WD2002

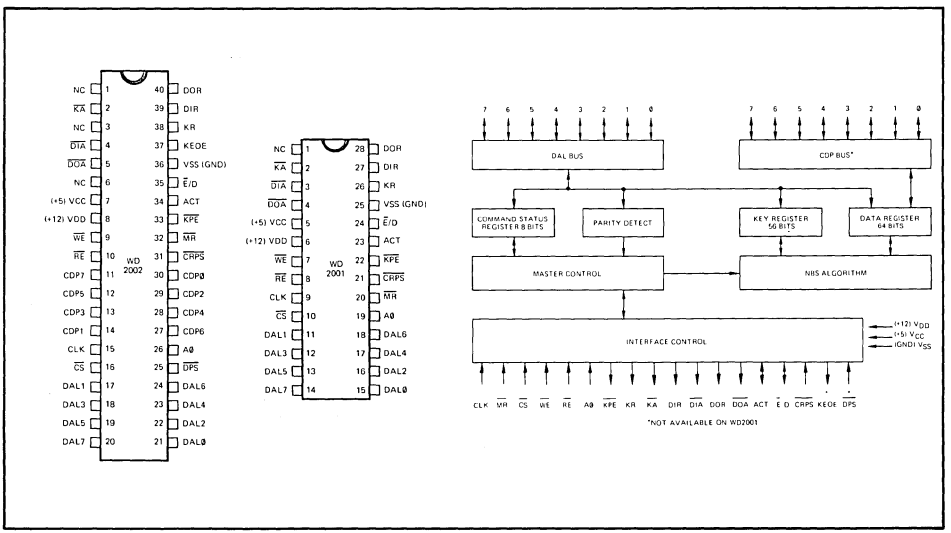
APPLICATIONS

- SECURE BROKERAGE TRANSACTIONS
- ELECTRONIC FUNDS TRANSFERS
- SECURE BANKING/BUSINESS ACCOUNTING
- MAINFRAME COMMUNICATIONS
- REMOTE AND HOST COMPUTER COMMUNICATIONS
- SECURE A/D
- SECURE DISK OR MAG TAPE DATA STORAGE
- SECURE PACKET SWITCHING TRANSMISSION

GENERAL DESCRIPTION

The Western Digital WD2001 and WD2002 Data Encryption/Decryption devices are designed to encrypt and decrypt 64-bit blocks of data using the algorithm specified in the Federal Information Processing Data Encryption Standard (#46). These devices encrypt a 64-Bit clear text word using a 56-Bit user-specified key to produce a 64-Bit cipher text word. When reversed, the cipher text word is decrypted to produce the original clear text word.

The DE2001/2 are fabricated in N-channel silicon gate MOS technology and are TTL compatible on all inputs and outputs.



WD2001/WD2002 BLOCK DIAGRAM

PIN OUTS

PIN NO. WD2001	PIN NO. WD 2002	PIN NAME	SYMBOL	FUNCTION
11-18	17-24	DATA LINES	DAL Ø → DAL 7	Eight active true three-state bi-directional I/O lines used for information transfer to and from the DES chip's registers. During single port operation, all COMMAND/STATUS, KEY WORD and DATA WORD transfers are via this bus. During dual port operation, all COMMAND/STATUS, KEY WORD and clear DATA WORD transfers are via this bus. (Cipher DATA WORD transfers are via the CIPHER DATA PORT (CDP) bus.)
N/A	11-14 27-30	CIPHER DATA PORT	CDP Ø → CDP 7	Eight active true three-state bi-directional I/O lines used only in dual port operation. Cipher DATA WORD transfers are via this bus. These pins are available on the WD2002 40 pin package version only.
6	8	POWER SUPPLY	V_{DD}	+ 12v
5	7	POWER SUPPLY	V_{CC}	+ 5v
25	36	GROUND	V_{SS}	GROUND
9	15	CLOCK	CLK	System clock input.
21	32	$\overline{\text{MASTER RESET}}$	$\overline{\text{MR}}$	$\overline{\text{MR}}$ active low resets the COMMAND/STATUS REGISTER and resets internal circuitry. (Requires active clock for reset operation.)
10	16	$\overline{\text{CHIP SELECT}}$	$\overline{\text{CS}}$	$\overline{\text{CS}}$ is made low to access registers within the device.
8	10	$\overline{\text{READ ENABLE}}$	$\overline{\text{RE}}$	The contents of the selected register are placed on the DAL (or CDP) bus lines when $\overline{\text{CS}}$ and $\overline{\text{RE}}$ are made low.
7	9	$\overline{\text{WRITE ENABLE}}$	$\overline{\text{WE}}$	Information on the DAL (or CDP) bus lines is written into the selected DES register when $\overline{\text{CS}}$ and $\overline{\text{WE}}$ are made low.
19	26	AØ	AØ	When this input is active high (during $\overline{\text{CS}}$ active) the COMMAND/STATUS REGISTER is addressed. (AØ active high will override internally generated addressing of the KEY and DATA REGISTERS as described on page 6.) This input is ignored when $\overline{\text{CRPS}}$ is active.
26	38	KEY REQUEST	KR	This output is active high when the DES chip is requesting that a byte of the KEY WORD be written into the KEY REGISTER. (The KEY REGISTER is automatically addressed when KR is active, unless overriden by AØ.)
2	2	$\overline{\text{KEY ACKNOWLEDGE}}$	$\overline{\text{KA}}$	This output is active low when $\overline{\text{WE}}$ is made low while the KEY REGISTER is addressed. (Can be used for handshake.)
27	39	DATA-IN REQUEST	DIR	This output is active high when the DES chip is requesting that a byte of the DATA WORD be written into the DATA REGISTER. (The DATA REGISTER is automatically addressed when DIR is active, unless overriden by AØ.)
3	4	$\overline{\text{DATA-IN ACKNOWLEDGE}}$	$\overline{\text{DIA}}$	This output is active low when $\overline{\text{WE}}$ is made low while the DATA REGISTER is addressed. (Can be used for handshake.)

PIN NO.		PIN NAME	SYMBOL	FUNCTION
WD2001	WD2002			
28	40	DATA-OUT REQUEST	DOR	This output is active high when the DES chip is requesting that a byte of the DATA WORD be read from the DATA REGISTER. (The DATA REGISTER is automatically addressed when the DOR is active, unless overridden by AØ.)
4	5	$\overline{\text{DATA-OUT ACKNOWLEDGE}}$	$\overline{\text{DOA}}$	This output is active low when $\overline{\text{RE}}$ is made low while the DATA REGISTER is addressed. (Can be used for handshake.)
22	33	$\overline{\text{KEY PARITY ERROR}}$	$\overline{\text{KPE}}$	This output is active low when enabled via the COMMAND/STATUS REGISTER BIT 2 (KEOE) and a parity error has been detected during loading of the KEY REGISTER.
21	31	$\overline{\text{COMMAND REGISTER PIN SELECT}}$	$\overline{\text{CRPS}}$	This input selects DAL bus or input pin programming of the COMMAND/STATUS REGISTER. $\overline{\text{CRPS}}$ high or open selects DAL bus programming. $\overline{\text{CRPS}}$ low selects input pin programming.
23	34	ACTIVATE	ACT	When $\overline{\text{CRPS}}$ is high or open, this pin is an output reflecting the status of the ACTIVATE bit (bit 1) of the COMMAND/STATUS REGISTER. When $\overline{\text{CRPS}}$ is low, this pin is an input that overrides the ACTIVATE bit of the COMMAND/STATUS REGISTER.
N/A	37	KEY ERROR OUTPUT ENABLE	KEOE	This output indicates the status of the KEY ERROR OUTPUT ENABLE bit (bit 2) of the COMMAND/STATUS REGISTER. This output is active when input pin programming is selected ($\overline{\text{CRPS}}$ low). This pin is available on the WD2002 40 pin package version only.
24	35	$\overline{\text{ENCRYPT}}$/DECRYPT	$\overline{\text{E}}$/D	When $\overline{\text{CRPS}}$ is high or open, this pin is an output reflecting the status of the $\overline{\text{ENCRYPT}}$/DECRYPT bit (bit 3) of the COMMAND/STATUS REGISTER. When $\overline{\text{CRPS}}$ is low, this pin is an input pin that overrides the $\overline{\text{ENCRYPT}}$/DECRYPT bit of the COMMAND/STATUS REGISTER.
N/A	25	$\overline{\text{DUAL PORT SELECT}}$	$\overline{\text{DPS}}$	When this input is high or open, single port operation is selected and all DES chip transfers are via the DAL bus. When $\overline{\text{DPS}}$ is low, dual port operation is selected and both the DAL bus and the CDP bus are used [separate busses for clear data (DAL bus) and cipher data (CDP bus)]. This pin is available on the WD2002 40 pin package version only.

NOTE: The WD2001 28 pin package version does not have the following pins: The 8 CDP pins, the KEOE pin, and the $\overline{\text{DPS}}$ pin.

SECTION 1

ORGANIZATION

The Data Encryption Standard chip consists of a 56-bit KEY REGISTER, a 64-bit DATA REGISTER, an 8-bit COMMAND/STATUS REGISTER, plus the necessary logic to check KEY parity and implement the NBS algorithm. A typical system implementation is shown on page 10 and the block diagram is shown on page 1. Although the DES chip interfaces to a wide variety of processors including mini-computers, the interface is tailored to the 8080A class microprocessor.

GENERAL OPERATING DESCRIPTION

The user programs the DES chip for encryption or decryption, and single or dual port operation.* Data is encrypted/decrypted with a 64-bit user defined KEY WORD. Data encrytped with a given KEY WORD can be decrypted only using that KEY WORD. The KEY REGISTER is loaded by the computer with eight successive 8-bit bytes. Parity is checked on each byte of the KEY WORD as it is loaded into the KEY REGISTER (The 8th bit (DALØ) of each 8-bit byte is reserved for odd parity for that byte and is not used in the algorithm calculation.) Similarily the DATA REGISTER is loaded with eight successive 8-bit bytes. The DATA REGISTER is read by reading eight successive 8-bit bytes.

When the DES chip is programmed for encryption, the DATA REGISTER is loaded with eight bytes of plain or clear text. The DES chip encrypts the data, then the encrypted data may be read from the DATA REGISTER (64-bits of encrypted text). When the DES chip is programmed for decryption, the DATA REGISTER is loaded with eight bytes of encrypted or cipher text. The DES chip decrypts the data, then the plain text may be read from the DATA REGISTER (64-bits of plain text). Note that all transfers to and from the KEY REGISTER and/or DATA REGISTER must occur in eight successive 8-bit bytes.

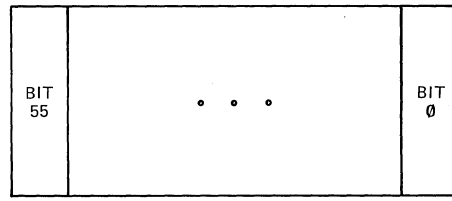
*Note: Dual port operation available with WD2002 40 pin package version only. (Single and dual port operation is described in detail under PART V. OPERATION.)

REGISTER DESCRIPTION

The following describes the KEY, DATA, and COMMAND/STATUS REGISTERS of the DES chip.

Key Register

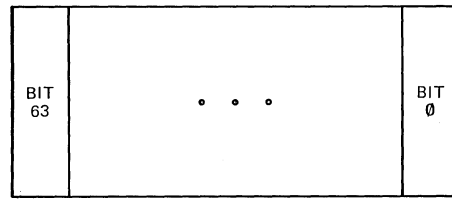
This 56-bit register contains the KEY by which the Data Encryption Algorithm operates. Eight successive bytes are needed to load the KEY REGISTER. The KEY REGISTER can be loaded only when there is a KEY REQUEST (Status bit and output). THIS REGISTER IS LOAD ONLY AND CANNOT BE READ.



KEY REGISTER
(LOAD ONLY)

Data Register

This 64-bit register contains plain or cipher text. When in the encrypt mode, the DATA REGISTER is loaded with plain text, and when read contains cipher text. When in the decrypt mode, the DATA REGISTER is loaded with cipher text, and when read contains plain text. The DATA REGISTER is always read or loaded with eight successive byte transfers. The DATA REGISTER can be loaded only when there is a DATA-IN REQUEST (status bit and output); similarily the DATA REGISTER can be read only when there is a DATA-OUT REQUEST (status bit and output).



DATA REGISTER

Command/Status Register (C/S R)

This 8-bit register controls the operation of the DES chip and monitors its status. Bits 7, 6, 5 and 4 are status-only bits (read only). Bits 3, 2 and 1 are COMMAND/STATUS bits (read/write). Bit Ø is not used. The COMMAND/STATUS bits (bits 3, 2, and 1) are normally loaded only once for an entire encrypt or decrypt process.

7	6	5	4	3	2	1	Ø
DOR	DIR	KPE	KR	$\overline{E}$/D	KEOE	ACT	N/U
STATUS BITS (READ ONLY)				COMMAND/STATUS BITS [READ / WRITE]			

COMMAND/STATUS REGISTER

COMMAND/STATUS REGISTER (C/S R)

Bit	Name	Function
C/S R0	NOT USED	
C/S R1	ACTIVATE	This bit must be set from '0' to '1' to initiate loading the KEY REGISTER. This bit must be '1' for encrypt/decrypt operation. This is a read/write bit.
C/S R2	KEY ERROR OUTPUT ENABLE (KEOE)	When '0', the $\overline{\text{KEY PARITY ERROR}}$ output pin ($\overline{\text{KPE}}$) remains inactive regardless of the status of the $\overline{\text{KEY PARITY ERROR}}$ bit (bit 5). When '1', the $\overline{\text{KEY PARITY ERROR}}$ output pin is active when the KPE bit (bit 5) is '1'. This bit is set to '1' upon a MASTER RESET. This is a read/write bit.
C/S R3	$\overline{\text{ENCRYPT}}$/DECRYPT ($\overline{\text{E}}$/D)	When '0' data is to be encrypted. When '1' data is to be decrypted. This is a read/write bit.
C/S R4	KEY REQUEST (KR)	This bit is set one clock period after the ACTIVATE bit is set (from '0' to '1'). It is reset upon loading of the 8th and final byte of the KEY REGISTER. This is a read only bit.
C/S R5	KEY PARITY ERROR (KPE)	This bit is set internally upon detection of a parity error during loading of the KEY REGISTER. It is reset when the ACTIVATE bit is programmed from '1' to '0' (i.e., chip is deactivated). This is a read only bit.
C/S R6	DATA-IN REQUEST (DIR)	This bit is set upon either: a) Completion of KEY REGISTER loading - or - b) Completion of DATA REGISTER reading, (ie, the last DATA-OUT REQUEST has been serviced by an 8-byte read and the DATA REGISTER is now empty and ready to be loaded with the next DATA WORD). It is reset upon loading of the 8th and final byte of the DATA REGISTER. This is a read only bit.
C/S R7	DATA-OUT REQUEST (DOR)	This bit is set upon completion of the internal encrypt/decrypt calculation of a DATA WORD. It is reset upon reading of the 8th and final byte of the DATA REGISTER. This is a read only bit.

Note: All bits of the COMMAND/STATUS REGISTER are reset to '0' upon MASTER RESET, except bit 2 (KEOE) which is set to '1' and bit Ø(not used) which will read '1' by default during a COMMAND/STATUS REGISTER read.

DETAILED OPERATING DESCRIPTION

The DES chip is initiated by programming a '1' in the ACTIVATE bit of the COMMAND/STATUS REGISTER. The DES chip will respond by activating the KEY REQUEST (KR) bit (bit 4) of the STATUS REGISTER and the KEY REQUEST output.

The user must deactivate AØ (allowing the chip to internally address the KEY REGISTER), and load the KEY REGISTER with the 64-bit KEY WORD. The KEY REGISTER is loaded with 8 consecutive 8-bit bytes by activating $\overline{WE}$ 8 times (with $\overline{CS}$ active).

When $\overline{WE}$ is made active, the DES chip deactivates the KR output. When $\overline{WE}$ is deactivated, the KR output is again activated. The DES chip will activate 8 KEY REQUESTs in this fashion until the KEY REGISTER is full.

Also, when $\overline{WE}$ is made active, the DES chip responds by activating the $\overline{KEY\ ACKNOWLEDGE}$ ($\overline{KA}$) output. Thus, 8 $\overline{KA}$ activations will be made.

The KR and $\overline{KA}$ outputs can be used for asynchronous handshaking (as in DMA control) or further activations following the first KR can be ignored and the KEY REGISTER can be loaded in a synchronous (programmed I/O) manner via 8 successive activations of $\overline{WE}$.

Each byte of the KEY WORD is checked for odd parity as it is loaded. If a parity error is found, the chip will set the KEY PARITY ERROR (KPE) bit (bit 5) of the COMMAND/STATUS REGISTER. If the KEY ERROR OUTPUT ENABLE bit (bit 2) of the COMMAND/STATUS REGISTER has been set, the DES chip will also activiate the $\overline{KPE}$ output. The KPE bit will be reset when the ACTIVATE bit is re-programmed to a '0'.

After loading the last (8th) byte of the KEY WORD into the KEY REGISTER, the DES chip will set the DATA-IN REQUEST bit (bit 6) of the STATUS REGISTER and activate the DATA-IN REQUEST (DIR) output. The 64-bit DATA WORD must then be loaded into the DATA REGISTER. The DATA REGISTER is loaded in the same manner as the KEY REGISTER via 8 successive activations of DATA-IN REQUEST (DES output), $\overline{WE}$ (DES input, and DATA-IN ACKNOWLEDGE (DES output).

After the last (8th) byte of the DATA WORD has been loaded, the chip begins the internal calculation of the NBS algorithm. Upon completion of the calculation, the new data is internally loaded into the DATA REGISTER, and the DES chip sets the DATA-OUT REQUEST bit (bit 7) of the STATUS REGISTER and activates the DATA-OUT REQUEST (DOR) output. The DATA WORD must then be read from the DATA REGISTER. The DATA REGISTER is read in the same manner as it was loaded via 8 successive activations of DATA-OUT REQUEST (DES output), $\overline{RE}$ (DES input), and $\overline{DATA\text{-}OUT\ ACKNOWLEDGE}$ (DES output).

Again, for both data-in and data-out, further activations of the DIR, DOR and $\overline{DIA}$, $\overline{DOA}$ outputs, after the first request, can be ignored and the DATA REGISTER loaded (read) by 8 successive activations of $\overline{WE}$ ($\overline{RE}$).

After the last (8th) byte of the DATA REGISTER has been read, the DES chip will reactivate the DATA-IN REQUEST. This cycle of loading the DATA REGISTER, internal algorithm calculation, and reading the new data from the DATA REGISTER can continue indefinitely until all desired data has been encrypted or decrypted with the current KEY WORD.

After all desired data has been encrypted/decrypted with the current KEY WORD, the ACTIVATE bit of the COMMAND/STATUS REGISTER should be programmed to '0'. When the ACTIVATE bit has been reset to '0', an unauthorized user will not have access to the last KEY loaded into the DES chip since to resume operation, the ACTIVATE bit must be programmed to '1' which activates KEY REQUEST and a new KEY must be loaded before access to the DATA REGISTER is possible.

To encrypt plain data, plain data is loaded into the DATA REGISTER, and encrypted data is read from the DATA REGISTER. (The $\overline{ENCRYPT}$/DECRYPT bit (bit 3 of the COMMAND/STATUS REGISTER) must have been previously programmed to '0'.)

To decrypt encrypted data, encrypted data is loaded into the DATA REGISTER, and plain data is read from the DATA REGISTER. (The $\overline{ENCRYPT}$/DECRYPT bit must have been previously programmed to '1'.)

Note: If it is desired to switch from encrypt to decrypt (or vice versa) under the same KEY WORD, this can be accomplished before a DATA WORD transfer is initiated. By making AØ high, the DES chip will override the internal addressing of the DATA REGISTER, and address the COMMAND/STATUS REGISTER. The COMMAND/STATUS REGISTER can be re-programmed. When AØ is returned to a low state, the DES chip will internally address the DATA REGISTER awaiting loading of the next DATA WORD.

DUAL PORT OPTION

(Available on WD2002 40 Pin Version Only)

When the $\overline{DUAL\ PORT\ SELECT}$ ($\overline{DPS}$) input is high or left open (ie., single port operation is selected), all transfers to/from the DES chip are via the DAL bus. The CDP bus is not used and remains three-stated.

When $\overline{DPS}$ is made low (ie., dual port operation is selected), all transfers to/from the COMMAND/STATUS REGISTER, and transfers to the KEY REGISTER are still via the DAL bus. Clear DATA WORDS are also transferred via the DAL bus. However, cipher DATA WORDS are now transferred via the CDP bus. This provides separate busses for clear and ciphered text.

Encryption during dual port operation requires loading clear data via the DAL bus, and reading cipher data via the CDP bus.

Decryption during dual port operation requires loading cipher data via the CDP bus, and reading clear data via the DAL bus.

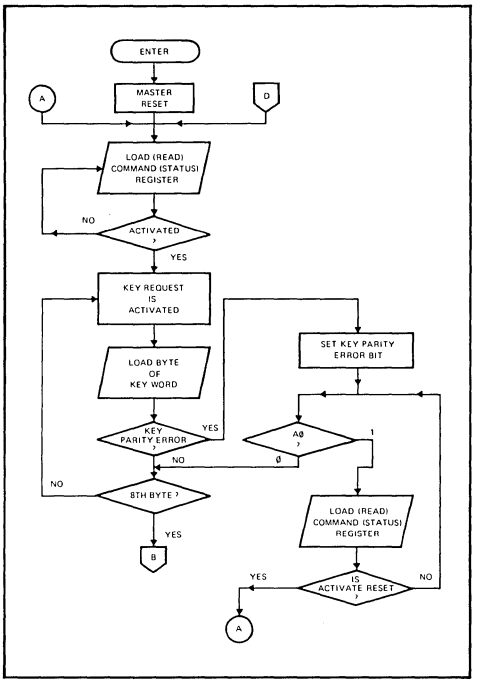
COMMAND SELECT OPTION

When the COMMAND REGISTER PIN SELECT (CRPS) input is made low, the ACT and $\overline{E}$/D pins are enabled as inputs. These inputs override bits 1 and 3 (respectively) of the COMMAND/STATUS REGISTER. This allows input pin control of the DES chip. The KEOE bit (bit 2) of the COMMAND/STATUS REGISTER will be held to '1'.

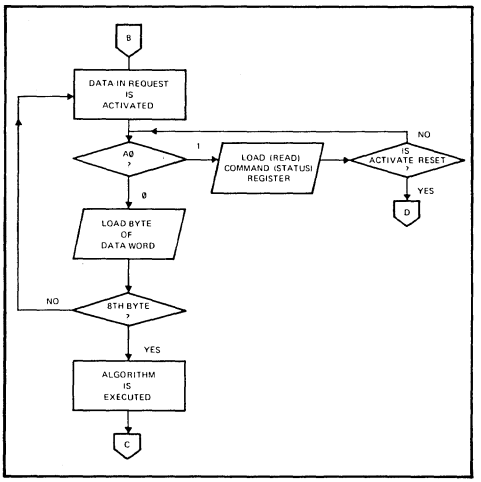
Input AØ will be disregarded in this mode of operation, and the COMMAND/STATUS REGISTER cannot be accessed via the DAL lines.

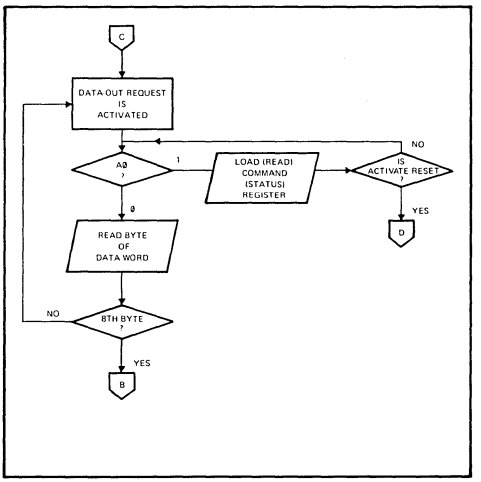
Note that the ACT pin must be toggled from '1' to a '0' to clear a parity error detection in this mode of operation.

All other operation remains as described previously.



WD2001/WD2002 FLOW CHARTS





MAXIMUM RATINGS

V_{DD} with Respect to V_{SS} (Ground) +15 to - 0.3V
Max. Voltage to any Input with Respect to V_{SS} +15 to - 0.3V
Operating Temperature 0°C to 70°C
Power Dissipation 1 W

Storage Temp. Ceramic -65°C to +150°C
Plastic -55°C to +125°C

OPERATING CHARACTERISTICS

T_A = 0°C to 70°C, V_{DD} = +12.0V ± .6V, V_{CC} = + 5.0V ± .25V, V_{SS} = OV

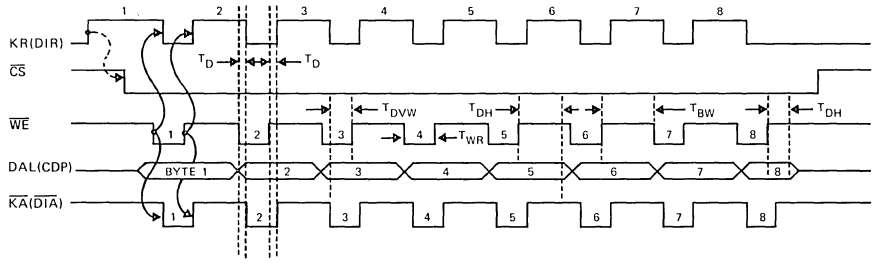
SYMBOL	CHARACTERISTIC	MIN.	TYP.	MAX.	UNITS	CONDITIONS
I_{LI}	Input Leakage			10	uA	V_{IN} = V_{DD}
I_{LO}	Output Leakage			10	uA	V_{OUT} = V_{CC}
I_{CCAVE}	V_{CC} Supply Current		68	100	mA	
I_{DDAVE}	V_{DD} Supply Current		17	25	mA	
V_{IH}	Input High Voltage	2.4			V	
V_{IL}	Input Low Voltage (All Inputs)			.8	V	
V_{OH}	Output High Voltage	2.8			V	I_O = -100uA
V_{OL}	Output Low Voltage			.4	V	I_O = 1.6 mA

AC CHARACTERISTICS

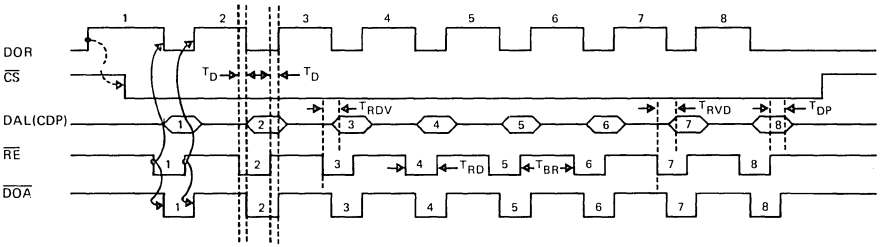
T_A = 0°C to 70°C, V_{DD} = +12.0V ± 0.6V, V_{SS} = OV, V_{CC} = +5.0 ± .25V

SYMBOL	CHARACTERISTIC	MIN.	TYP.	MAX.	UNITS	CONDITIONS
READ						
T_{ACS}	AØ, $\overline{CS}$ Set up to $\overline{RE}\downarrow$	60			ns	
T_{RDV}	$\overline{RE}\downarrow$ to DAL (CDP) Valid			330	ns	C_{LOAD} = 50PF
T_{RD}	$\overline{RE}$ Pulse Width	330			ns	
T_{DF}	$\overline{RE}\uparrow$ to DAL Float	30		200	ns	
T_{ACH}	AØ, $\overline{CS}$ Hold From $\overline{RE}\uparrow$	0			ns	
WRITE						
T_{ACS}	AØ, $\overline{CS}$ Set up to $\overline{WE}\downarrow$	60			ns	
T_{DVW}	DAL (CDP) Set up to $\overline{WE}\uparrow$	200			ns	
T_{WR}	$\overline{WE}$ Pulse Width	200			ns	
T_{DH}	DAL (CDP) Hold From $\overline{WE}\uparrow$	60			ns	
T_{ACH}	AØ, $\overline{CS}$ Hold From $\overline{WE}\uparrow$	0				
HAND-SHAKE						
T_D	KR (DIR) $\downarrow$, KA ($\overline{DIA}$) $\downarrow$ From $\overline{WE}\downarrow$ KR (DIR) $\uparrow$, KA ($\overline{DIA}$) $\uparrow$ From $\overline{WE}\uparrow$ DOR $\downarrow$, $\overline{DOA}\downarrow$ From $\overline{RE}\downarrow$ DOR $\uparrow$, $\overline{DOA}\uparrow$ From $\overline{RE}\uparrow$		300	450	ns	C_{LOAD} = 50PF

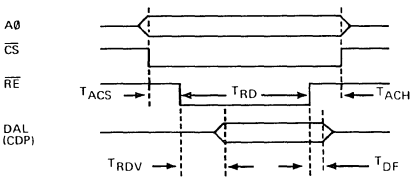
NOTE: All output timing specifications reflect the following: High Output 2.0V
Low Output 0.8V



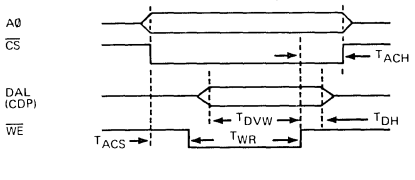
TYPICAL KEY OR DATA REGISTER LOAD



TYPICAL DATA REGISTER READ & TIMING



READ TIMING



WRITE TIMING

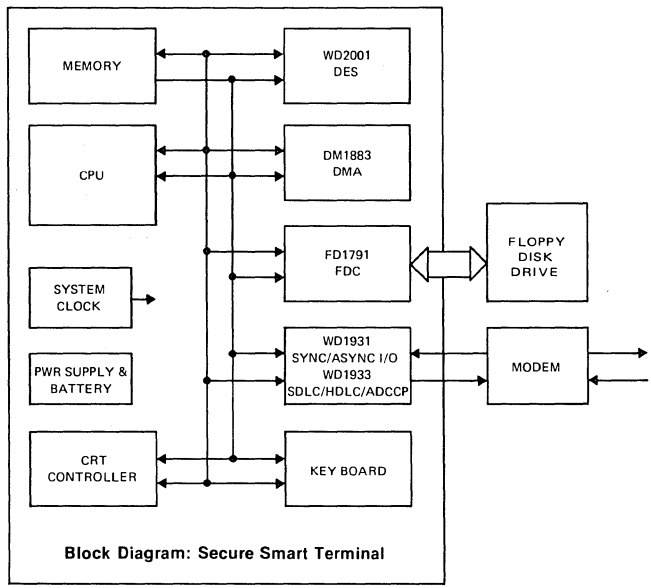
MISCELLANEOUS TIMING

1. CLOCK INPUT
   FREQUENCY: 2 MHZ (MAX); 100 KHZ (MIN).
   PULSE WIDTH: 250 nsec MIN.
2. MASTER RESET PULSE WIDTH: 10 Clock Periods
3. Time between consecutive $\overline{RE}$ or $\overline{WE}$ pulses:
   $T_{BR} = T_{BW}$ = 2 CLOCK PERIODS MINIMUM
4. ACT, $\overline{E}$/D, KEOE OUTPUTS
   These pins will be valid within 2 CLK ↓ + 450 nsec from $\overline{WE}$ ↑ of a COMMAND REGISTER write operation.
5. $\overline{KPE}$ OUTPUT
   This pin will be active within 2 CLK ↓ + 450 nsec from $\overline{WE}$ ↑ of a write of a KEY WORD byte that results in a parity error.
6. $\overline{CRPS}$, $\overline{DPS}$, $\overline{E}$/D INPUTS require a 300 ns set-up time.
7. The initial KR activation will be valid within 3 CLK ↓ + 450 nsec from $\overline{WE}$ ↑ of a write operation that programs a '1' into the COMMAND REGISTER ACTIVATE bit (or 2 CLK ↓ + 450 nsec from ACT input ↑, if $\overline{CRPS}$ = 0).
8. The initial DIR activation will be valid within 2 CLK ↓ + 450 nsec from $\overline{WE}$ ↑ of the 8th write into the KEY REGISTER.
9. The initial DOR activation will be valid within 49 CLK ↓ + 450 nsec from $\overline{WE}$ ↑ of the 8th write into the DATA REGISTER.
10. When reading the DATA REGISTER (in response to DOR), subsequent data bytes are made available internally to the DAL (CDP) output buffers within 2 CLK ↓ + 450 nsec from $\overline{RE}$ ↑

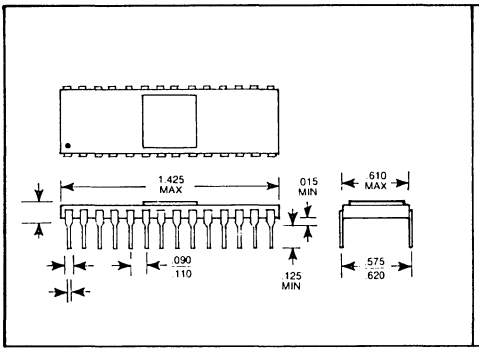
NOTE: All output timings assume C_{LOAD} = 50 PF

TYPICAL APPLICATION

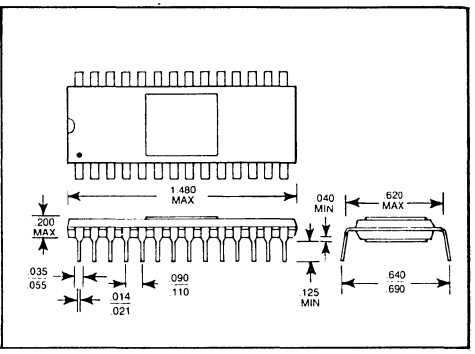
Shown below is a block diagram for a floppy disk based DES secure smart terminal. The Direct Memory Access (DMA) controller optimizes data transfer operations for not only the floppy but also for file encryption and decryption operations. Secure features for the terminal include: secure file storage on floppy disks, optical clear/ secure transmission via the communications I/O and battery backup of the Terminal ID key.
Tampering with the Terminal by unauthorized persons either through the key board power supply interrupt interlock or attempting to open the service panel results in memory scrambling and terminal ID key destruction. Finally, a hardware option was also included to allow the use of the pin compatible WD1933 device in place of the WD1931 for bit oriented SDLC, HDLC, or ADCCP protocols.



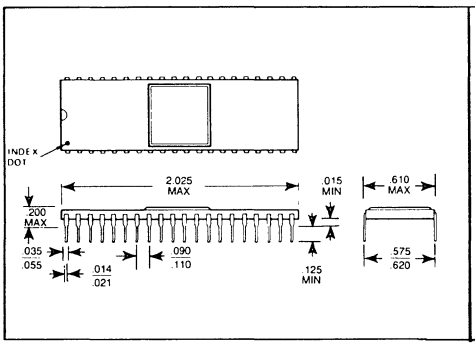
Block Diagram: Secure Smart Terminal



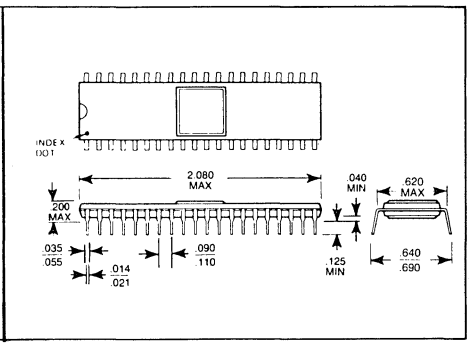
WD2001E CERAMIC PACKAGE



WD2001F PLASTIC PACKAGE



WD2002A CERAMIC PACKAGE



WD2002B PLASTIC PACKAGE

EXPORT CONTROL: Cryptographic devices and technical data regarding them are subject to Federal Government export controls as specified in Title 22, Code of Federal Regulations. Parts 121 through 128.

WESTERN DIGITAL
CORPORATION

3128 REDHILL AVENUE, BOX 2180
NEWPORT BEACH, CA 92663 (714) 557-3550,TWX 910-595-1139