- **The CA20C03A is an improved version of the DES encryption processor designed by Tundra Semiconductor Corporation.**
- **Data transfer rates up to 3.85 Mbytes per second**
- **Encrypt and decrypt using Data Encryption Standard (DES) adopted by the U.S. Department of Commerce, National Bureau of Standards (NBS) - publication FIPS PUB 46 (1-15-1977)**
- **Validated by the National Institute for Standards and Technology (NIST) in accordance with the procedures specified in NBS publication 500-20**
- **Electronic Code Book (ECB) and Cipher Block Chaining (CBC)**
- **Encrypt and decrypt 64-bit data words using 56-bit key words**
- **Parity check on key word loading**
- **Key stored in device is not externally accessible**
- **Standard 8-bit microprocessor interface**
- **Battery Back-up capability of internal key register**
- **Low power CMOS with TTL I/O compatibility**
- **Available in PLCC, PDIP, and TQFP packages**

The Tundra Semiconductor Corporation CA20C03A *DES Encryption Processor* is designed to encrypt and decrypt 64-bit blocks of data using the algorithm specified in the Federal Information Processing Data Encryption Standard - publication FIPS PUB 46 (1-15-1977). DES is the standard data encryption algorithm used for file and communications encryption, and as such is widely established in the security, finance and banking industries. The CA20C03A encrypt 64-bit clear text words using 56-bit, user-specified keys to produce 64-bit cipher text words. When reversed, the cipher text words are decrypted to produce the original clear text words.

If your application requires strictly WD2001 mode then please contact the factory for documentation.

The CA20C03A is implemented in low power CMOS technologies with TTL compatible I/O. It is offered in 28-pin PDIP, 28-lead PLCC, and 44-pin TQFP packaging.

Application areas for the CA20C03A DES chip spans a diverse industrial base of financial, information processing, telecommunications and data communications companies.

- Secure Brokerage transactions
- Electronic fund transfers
- Secure banking/business accounting
- Mainframe communications
- Remote and host computer communications
- Secure disk or magnetic tape data storage
- Secure packet-switching transmission

Table 3-1 : CA20C03A Transfer Rates

Product Code	Data Transfer Rates - ECB Mode (Mbytes per Second)	System Clock
CA20C03A-5	0.77	5 MHz
CA20C03A-10	1.54	10 MHz
CA20C03A-16	2.46	16 MHz
CA20C03A-20	3.08	20 MHz
CA20C03A-25	3.85	25 MHz

Warning: These devices cannot be shipped outside North America without written authorization from Canadian External Affairs and Department of National Defence or the US State Department and Department of Defence.

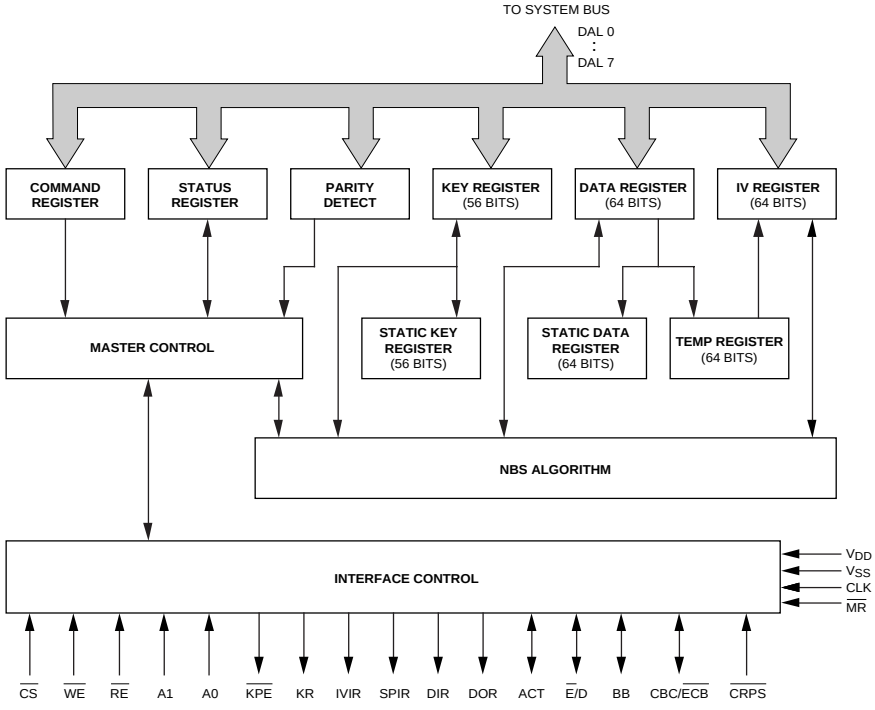
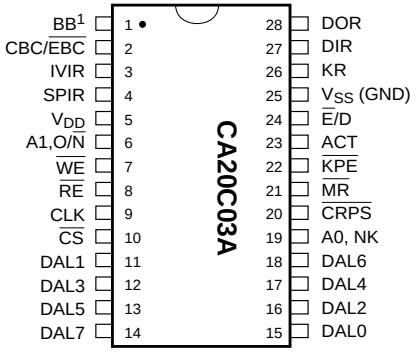
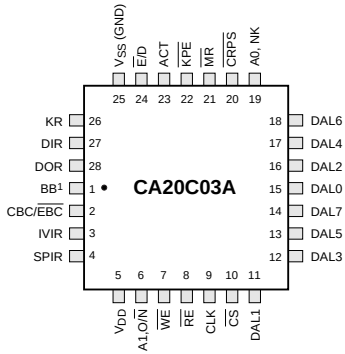


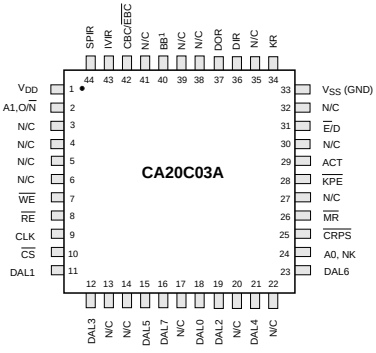
Figure 3-1 : CA20C03A Block Diagram



a) 28-pin PDIP



b) 28-pin PLCC



c) 44-pin TQFP

Figure 3-2 : CA20C03A Pin Configuration

Table 3-2 : Pin Description

Symbol	Pin			Type	Name and Function
	PLCC	PDIP	TQFP		
A0, NK	19	19	24	I	**Address 0, New Key:** When $\overline{CRPS}$ is logic 1 or open, a high on this input addresses the Command or Status Register (see Table 3-18). When $\overline{CRPS}$ and A1, O/$\overline{N}$ are logic 0, a high on this input requests that a new key be loaded in the Key Register. Device responds by activating the KR pin.
A1, O/$\overline{N}$	6	6	2	I	**Address 1, Old/New:** When $\overline{CRPS}$ is logic 1 or open, and this input is logic 1, the Status Register is addressed ($\overline{CS}$ = 0, A0 = 1). When this input is logic 0, the Command Register is addressed ($\overline{CS}$ = 0, A0 = 1). This input is ignored when A0 = 0. Note that this input has an internal pull-up resistor. When $\overline{CRPS}$ is logic 0 (low) and this input is logic 0, the device is in CA20C03A mode. When this input is logic 1, the device is in WD2001 mode. The only way to return to CA20C03A mode from WD2001 mode is to reset the device. *Caution: In WD2001 mode, pin 6 of the CA20CO3A device must not be connected to +12V as it will irreparably damage the device.*
ACT	23	23	29	I/O	**Activate:** When $\overline{CRPS}$ is logic 1 or open, this pin is an output reflecting the status of the *Activate* bit (bit 1) of the Command Register. When $\overline{CRPS}$ is logic 0, this pin is an input that overrides the Activate bit of the Command Register.
BB	1	1	40	I/O	**Battery Back-up Key:** When $\overline{CRPS}$ is logic 1 (open), this pin is an output reflecting the status of the *battery back-up key* bit (bit 5) of the Command Register. When $\overline{CRPS}$ is logic 0 or low, this pin is an input that overrides the *battery back-up key* bit.
CBC/$\overline{ECB}$	2	2	42	I/O	**Cipher Block Chaining/Electronic Code Book:** When $\overline{CRPS}$ is logic 1 or open, this pin is an output pin reflecting the status of CBC/$\overline{ECB}$ bit (bit 7) of the Command Register. When $\overline{CRPS}$ is logic 0, this pin is an input pin and overrides the CBC/$\overline{ECB}$ bit of the Command Register.
CLK	9	9	9	I	**Clock:** System clock input.
$\overline{CRPS}$	20	20	25	I	**Command Register Pin Select:** This input selects DAL bus or input pin programming of the Command Register. $\overline{CRPS}$ high or open selects DAL bus programming. $\overline{CRPS}$ low selects input pin programming.This input incorporates an internal pull-up resistor.
$\overline{CS}$	10	10	10	I	**Chip Select:** $\overline{CS}$ is made low to access registers within the device.
DAL 7 - 0	11-18	11-18	11,12,15, 16,18,19,2 1,23	I/O	**Data Lines:** Eight active true, tri-state, bi-directional I/O lines used for information transfer to and from the DES device. All *Command Register, Status Register, Key Word* and *Data Word* transfers are via this bus.
DIR	27	27	36	O	**Data-In Request:** This output is active high when the DES device is requesting that byte of the *Data Word* be written into the Data Register (The Data Register is automatically addressed when DIR is active, unless overridden by A0).
DOR	28	28	37	O	**Data-Out Request:** This output is active high when the DES device 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 A0).
$\overline{E}$ /D	24	24	31	I/O	**Encrypt/Decrypt:** When $\overline{CRPS}$ is high or open, this pin is an output reflecting the status of the *Encrypt/Decrypt* bit (bit 3) of the Command Register. When $\overline{CRPS}$ is low, this pin is an input pin that overrides the *Encrypt/Decrypt* bit of the Command Register.

Table 3-2 : Pin Description Cont'd

Symbol	Pin			Type	Name and Function
	PLCC	PDIP	TQFP		
IVIR	3	3	43	O	**Initial Vector-In Request:** This output is active high when the device is requesting that a byte of the *IV Word* be written into the IV register (The IV register is automatically addressed when IVIR is active, unless overridden A0).
$\overline{KPE}$	22	22	28	O	**Key Parity Error:** This output is active low when enabled via the Command Register bit 2 (KEOE) and a parity error has been detected during loading of the Key Register.
KR	26	26	34	O	**Key Request:** This output is active high when the DES device 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 overridden by A0.)
$\overline{MR}$	21	21	26	I	**Master Reset:** $\overline{MR}$ active low resets the Command and Status Registers and resets internal circuitry. (Requires active clock for reset operation.)
$\overline{RE}$	8	8	8	I	**Read Enable:** The contents of the selected register are placed on the DAL bus lines when $\overline{CS}$ and $\overline{RE}$ are made low.
SPIR	4	4	44	O	**Special Pattern-In:** This output is active high during battery back-up mode, when the device is requesting that a byte of the *Special Pattern Word* be written into the Data Register (The Data Register is automatically addressed when SPIR is active, unless overridden by A0).
V_{DD}	5	5	1	-	**Power Supply:** +5 V ±10%
V_{SS}	25	25	33	-	**Ground:** Ground
$\overline{WE}$	7	7	7	I	**Write Enable:** Information on the DAL bus lines is written into the selected register when $\overline{CS}$ and $\overline{WE}$ are made low.

Table 3-3a : AC Characteristics For CA20C03A (5, 10, 16 MHz)
T_A = 0 to 70 °C, V_{DD} = +5.0V ± 10%, V_{SS} = 0V

Symbol	Parameter	Test Condition	Limits 5MHz		Limits 10MHz		Limits 16MHz		Unit
			MIn	Max	MIn	Max	Min	Max	
t_{BR}	$\overline{RE}\uparrow$ to next $\overline{RE}\downarrow$		2CLK		2CLK		2CLK		ns
t_{BW}	$\overline{WE}\uparrow$ to next $\overline{WE}\downarrow$		2CLK		2CLK		2CLK		ns
t_{CY}	Clock cycle time			200		100		62.5	ns
t_{DAR}	DOR$\uparrow$ from $\overline{RE}\uparrow$			2CLK+30		2CLK+30		2CLK+30	ns
t_{DAW}	KR$\uparrow$, DIR$\uparrow$, IVIR$\uparrow$, and SPIR$\uparrow$ from $\overline{WE}\uparrow$			2CLK+30		2CLK+30		2CLK+30	ns
t_{DDR}	DOR$\downarrow$ from $\overline{RE}\downarrow$			150		80		50	ns
t_{DDW}	KR$\downarrow$, DIR$\downarrow$, IVIR$\downarrow$, SPIR$\downarrow$ from $\overline{WE}\downarrow$	CLOAD = 50 pF		150		80		50	ns
t_{DF}	$\overline{RE}\uparrow$ to DAL float		10	100	10	50	5	35	ns
t_{DH}	DAL hold from $\overline{WE}\uparrow$		20		15		10		ns
t_{DVW}	DAL setup WE$\uparrow$		80		40		30		ns
t_{MR}	Master reset pulse width		2CLK		2CLK		2CLK		µs
t_{RACH}	A0, A1, CS hold from $\overline{RE}\uparrow$		0		0		0		ns
t_{RACS}	A0, A1, CS setup to $\overline{RE}\downarrow$		25		15		5		ns
t_{RD}	$\overline{RE}$ pulse width		200		100		60		ns
t_{RDV}	$\overline{RE}\downarrow$ to DAL valid	CLOAD = 50pF		150		90		50	ns
t_{WACH}	A0, A1, CS hold from $\overline{WE}\uparrow$		0		0		0		ns
t_{WACS}	A0, A1,CS setup to $\overline{WE}\downarrow$		25		15		5		ns
t_{WR}	$\overline{WE}$ Pulse Width		125		95		60		ns

Notes for Tables 3a, 3b, and 3c:

1. All output timing specifications reflect the following:
   High Output 2.0V, Low Output 0.8V
2. Clock Input: Clock signal duty cycle is 50% ±10%. There is no minimum frequency.
3. t_{MR} is 2 CLKS in all cases for the CA20C03A device.
4. Time between consecutive $\overline{RE}$ or $\overline{WE}$ pulses: $t_{BR} = t_{BW}$ = 2 Clock periods *minimum*.
5. ACT, $\overline{E}$ /D, and CBC/$\overline{ECB}$ are valid 2CLK$\downarrow$ + 450 ns from $\overline{WE}\uparrow$ of a Command Register write operation.
6. $\overline{KPE}$ output is valid within 2CLK$\downarrow$ + 450 ns from $\overline{WE}\uparrow$ of a write of a *Key Word* byte that results in a parity error.
7. ACT, $\overline{E}$ /D, BB and CBC/$\overline{ECB}$ are valid 2CLK$\downarrow$ + 30 ns from $\overline{WE}\uparrow$ of a Command Register write operation (for CA20C03A).
8. $\overline{KPE}$ output is valid within 1CLK$\downarrow$ + 30 ns from $\overline{WE}\uparrow$ of a write of a *Key Word* byte that results in a parity error (for CA20C03A).

Table 3-3b : AC Characteristics For CA20C03A (20, 25 MHz)
T_A = 0 to 70 °C, V_{DD} = +5.0V ± 10%, V_{SS} = 0V

Symbol	Parameter	Test Condition	Limits 20MHz		Limits 25MHz		Unit
			Min	Max	Min	Max	
t_{BR}	$\overline{RE}\uparrow$ to next $\overline{RE}\downarrow$		2CLK		2CLK		ns
t_{BW}	$\overline{WE}\uparrow$ to next $\overline{WE}\downarrow$		2CLK		2CLK		ns
t_{CY}	Clock cycle time			50		40	ns
t_{DAR}	DOR$\uparrow$ from $\overline{RE}\uparrow$			2CLK+30		2CLK+30	ns
t_{DAW}	KR$\uparrow$, DIR$\uparrow$, IVIR$\uparrow$ and SPIR$\uparrow$ from $\overline{WE}\uparrow$			2CLK+30		2CLK+30	ns
t_{DDR}	DOR$\downarrow$ from $\overline{RE}\downarrow$			40		35	ns
t_{DDW}	KR$\downarrow$, DIR$\downarrow$, IVIR$\downarrow$, SPIR$\downarrow$ from $\overline{WE}\downarrow$	CLOAD = 50 pF		40		35	ns
t_{DF}	$\overline{RE}\uparrow$ to DAL float		5	25	5	20	ns
t_{DH}	DAL hold from $\overline{WE}\uparrow$		5		5		ns
t_{DVW}	DAL setup WE$\uparrow$		20		20		ns
t_{MR}	Master reset pulse width		2CLK		2CLK		µs
t_{RACH}	A0, A1, CS hold from $\overline{RE}\uparrow$		0		0		ns
t_{RACS}	A0, A1, CS setup to $\overline{RE}\downarrow$		5		5		ns
t_{RD}	$\overline{RE}$ pulse width		50		40		ns
t_{RDV}	$\overline{RE}\downarrow$ to DAL valid	CLOAD = 50pF		45		35	ns
t_{WACH}	A0, A1, CS hold from $\overline{WE}\uparrow$		0		0		ns
t_{WACS}	A0, A1,CS setup to $\overline{WE}\downarrow$		5		5		ns
t_{WR}	$\overline{WE}$ Pulse Width		45		35		ns

Notes for Tables 3a, 3b, and 3c continued:

9. KR activation is valid within 2CLK$\downarrow$ + 30 ns from $\overline{WE}\uparrow$ (for CA20C03A) and 3CLK$\downarrow$ + 450 ns from $\overline{WE}\uparrow$ of a write operation that programs a 1 into the COMMAND REGISTER ACTIVATE bit (or from a ACT input$\uparrow$, if $\overline{CRPS}$ = 0).
10. Initial DIR activation is valid within 20CLK$\downarrow$ + 30 ns from $\overline{WE}\uparrow$ of the 8th write into the Key Register.
11. Initial DOR activation is valid within 20CLK$\downarrow$ + 30 ns from $\overline{WE}\uparrow$ of the 8th write into the Data Register.
12. When reading the Data Register (in response to DOR), subsequent data bytes are made available internally to the DAL output buffers within 2CLK$\downarrow$ + 30 ns from $\overline{RE}\uparrow$.
13. After reading the Data Register in response to DORs, DIR is activated and valid within 2CLK$\downarrow$ + 30 ns from $\overline{RE}\uparrow$ of the 8th read from the Data Register.
14. All output timings assume CLOAD = 50pF.

Figure 3-3 : Typical Key or Data Register Load Timing

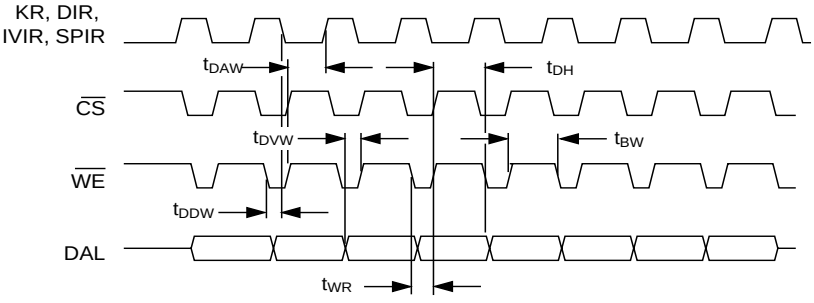


Figure 3-4 : Typical Register Read Timing

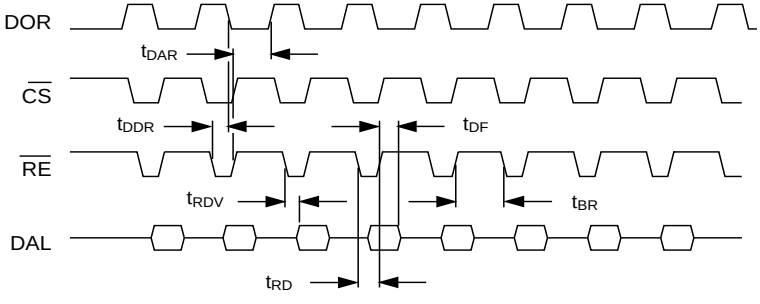


Figure 3-5 : Read Timing

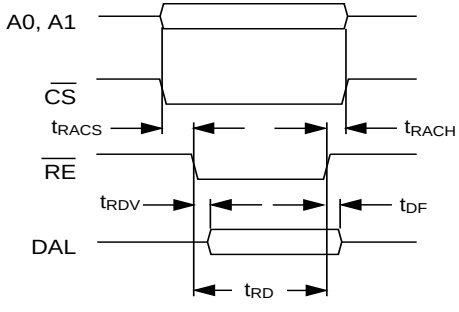
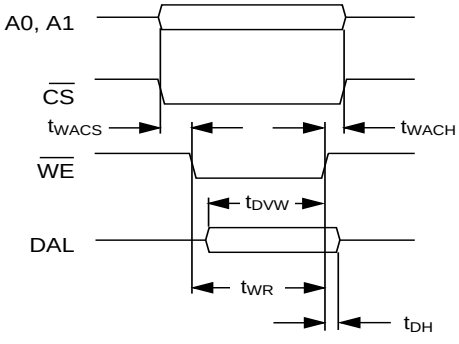


Figure 3-6 : Write Timing



USING THE CA20C03A TO ATTAIN MAXIMUM THROUGHPUT

In order to obtain maximum throughput from the CA20C03A, the number of cycles used to perform I/O operations is minimized. The throughput is dictated by eight bytes written to the device plus 20 cycles for processing, plus eight bytes read from the device for each 64-bit block. If the data sheet is followed explicitly, it would take 24 cycles per I/O operation for a total of 48 cycles (i.e. three cycles for each byte written to or read from the device as dictated by t_{BW} timing parameters). So for each 64-bit block, 48 plus 20, or 68 cycles are required, giving a maximum throughput of:
8bytes/(68 cycles x (40ns/cycle) = 2.95 MBytes/s.

The number of cycles per byte can be reduced to two by following a few simple timing rules. The timing parameters t_{BW} and t_{BR} specify two cycles between the rising edge of a read or write and the falling edge of the next read or write. Figure 3-7 shows this timing and hence the three clock cycles per byte. In actual fact, two falling edges of the clock are required between the rising edge of a read or write and the falling edge of the next read or write. Figure 3-8 shows how two cycles are achieved in this case. So for each 64-bit block, 32 plus 20, or 52 cycles are required, giving a maximum throughput of:
8bytes/(52 cycles x (40ns/cycle) = 3.85 MBytes/s

Two new timing parameters, t_1 and t_2, are introduced (see Figure 3-8), and modifications are made to $\overline{WR}$ and $\overline{RD}$ (see Table 3-5 below).

Table 3-4 : Maximum Throughput I/0 Timing For The CA20C03A Device

Symbol	5 MHz		10 MHz		16 MHz		20 MHz		25 MHz		Unit
	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	
t_{WR}	125	185	65	85	30	45	25	35	20	25	ns
t_{RD}	125	185	65	85	30	45	25	35	20	25	ns
t_{RDV}	125		65		30		25		25		ns
t_1	2		2		2		2		2		ns
t_2	13		13		13		13		13		ns

Note: The following timing parameters only apply when the timing of Figure 8 is used.

Figure 3-7 : Typical I/O Timing

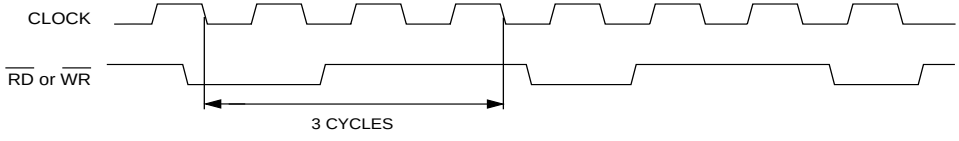


Figure 3-8 : Maximum Throughput Timing For The CA20C03A Device

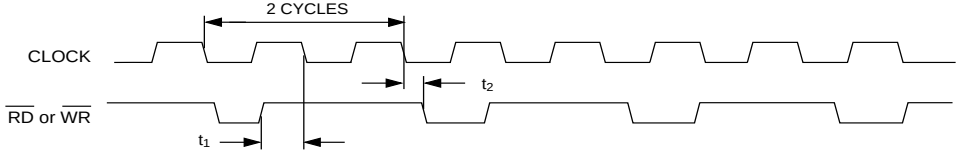


Table 3-5 : DC Characteristics (T_A = 0 to 70 °C, V_{DD} = +5.0V ± 10%, V_{SS} = 0V)

Symbol	Parameter	Test Conditions	Limits		Unit
			Min	Max	
I_{IL}	Input leakage current	V_{IH} = 5.5 V	-10	+10	µA
		V_{IL} = 0 V	-10	+10	µA
I_{LL}	Input low current on CA20C03A $\overline{CRPS}$, A1, O/$\overline{N}$ pins.	V_{IL} = 0 V		1	mA
I_{OL}	Output leakage current	0 V ≤ V_{IN} ≤ V_{DD}	-10	10	µA
I_{DDOP}	Operating current	V_{IN} = V_{DD} or V_{SS}		2	mA/MHz
I_{DDSB}	Standby current	V_{IN} = V_{DD} or V_{SS} V_{DD} = 5.5 V, Outputs open		1.0 (0.1 Typ)	µA
V_{IH}	Voltage input high		2.4		V
V_{IL}	Voltage input low (all inputs)			0.8	V
V_{OH}	Voltage output high	I_{OH} = -100 µA	2.8		V
V_{OL}	Voltage output low	I_{OL} = +1.6 mA		0.4	V
V_{BB}	Min. battery back-up voltage		2.0		V
I_{DR}	Data retention current in battery back-up mode	V_{BB} = 2.0 V		15.0	µA

Notes:
1. I_{IL} applies only to inputs without pull-up resistors.
2. I_{LL} applies only to inputs with pull-up resistors.

Table 3-6 : Recommended Operating Conditions

DC Supply Voltage (V_{DD})	+4.5 V to +5.5 V
Power Dissipation (P_{DD})	0.5 W
Ambient Operating Temperature (T_A Commercial)	0° to +70°C

The power dissipation figure is based on typical internal logic dissipation plus the worst case set of outputs simultaneously active with maximum rated loads.

Table 3-7 : Absolute Maximum Ratings

DC Supply Voltage (V_{DD})	-0.3 to +7.0 V
Input Voltage (V_{IN})	-0.3 to VDD +0.3 V
DC Input Current (I_{IN})	-10 to +10 mA
Storage Temperature, plastic (T_{STG})	-40° to +125°C

Stresses beyond those listed above may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to maximum rating conditions for extended periods may affect device reliability.

FUNCTIONAL DESCRIPTION

The CA20C03A Data Encryption Standard (DES) device consists of eight registers, two ciphering options, the DES algorithm and key parity checking. The CA20C03A also contains the necessary logic to implement a Battery Back-up Key option.

The eight registers include a 56-bit Key Register, a 64-bit Data Register, a 64-bit Initial Vector Register, a 64-bit Temp Register, two 8-bit registers for both command and status, a 56-bit Static Key Register, and a 64-bit Static Data Register. A block diagram of the CA20C03A is shown in Figure 1.

The CA20C03A devices can be programmed for encryption or decryption using either the *Electronic Code Book* (ECB) or *Cipher Block Chaining* (CBC) modes with or without a *Battery Back-up Key.* Data is encrypted or decrypted with a 64-bit, user-defined *Key Word*. Data encrypted with a given *Key Word* can be decrypted only using the same *Key Word*.

The Key Register is loaded by the system with eight successive bytes beginning with the most significant byte of the key. Parity is checked on each byte of the *Key Word* as it is loaded into the Key Register. The least significant bit (DAL0) of each 8-bit byte is reserved for odd parity for that byte and is not used in the algorithm calculation (see Table 3-8 and Table 3-9 below for Key Word loads and Data loads and reads).

Table 3-8 : Format for *Key Word* Loads

7	6	5	4	3	2	1	Parity
DAL7	DAL6	DAL5	DAL4	DAL3	DAL2	DAL1	DAL0

Table 3-9 : Format for Data Loads and Reads

7	6	5	4	3	2	1	0
DAL7	DAL6	DAL5	DAL4	DAL3	DAL2	DAL1	DAL0

In a mode without a *Battery Back-up Key*, the *Key Word* is requested after each activation and should be loaded into the Key Register. The Static Key Register and Static Data Register are not used in this mode.

In a mode with a *Battery Back-up Key*, the *Key Word* is requested only when the user requests a new key by programming the Command Register, or when the *Key Word* stored in the Static Key Register is found no longer valid after power-up key verification. In this mode, the *Key Word* is loaded into the Static Key Register, and a special 64-bit pattern is requested and encrypted by the CA20C03A. The encrypted pattern is loaded in the Static Data Register.

During power-down or power failure, the contents of these two Static Registers are retained by the battery back-up power. As soon as the power is up again, the contents in the Static Data Register are used to verify and validate the contents in the Static Key Register during the key verification process.

When the CA20C03A is programmed for the Cipher Block Chaining (CBC) mode, the *Initial Vector* (IV) is requested by the device after the *Key Word* is loaded into the Key Register and is ready to be used for encryption or decryption. The Initial Vector Register is loaded with eight successive bytes (most significant byte first) of *Initial Vector* data at the start of each encryption or decryption process.

To encrypt plain data, the Data Register is loaded with eight successive bytes (most significant byte first) of the first plain text block. The contents of the Data Register are then added (modulo 2) to the contents of the Initial Vector Register one bit at a time. The modified text is then encrypted to the DES algorithm and the resulting encrypted (cipher) text is loaded into the Initial Vector Register for the next block of plain text to be modified, as well as being ready to be read out. This cycle is repeated until all required data is encrypted. To decrypt encrypted data, the Data Register is loaded with eight successive bytes (8-bit) of the first cipher text block. The contents of the Data Register are loaded into the Temp Register and at the same time they are decrypted to the DES algorithm. The resulting text in the Data Register is added (modulo 2) with the contents of the Initial Vector Register. The contents of the Initial Vector Register becomes plain text and are loaded into the Data Register, ready to be read out. The contents of the Temp Register are then loaded into the Initial Vector Register to allow for the next block of cipher text to be decrypted. This cycle is repeated until all required data is decrypted.

When the CA20C03A is programmed for Electronic Code Book (ECB) mode, neither the Initial Vector Register nor the Temp Register are used. The *Data Word* is requested by the device after the *Key Word* is loaded in the Key Register and ready to be used for encryption or decryption. In both encryption and decryption, the Data Register is loaded with eight successive bytes (8-bit) of text, then the contents of the Data Register go through the DES algorithm calculation. The resulting text in the Data Register is ready to be read out. It is read by reading eight successive bytes (8-bit).

The data transfer into or out of the device's registers (Key Register, Data Register, IV Register) through the DAL bus is accomplished by loading or reading out eight successive bytes (8-bit). The first byte written to or read from these registers is always the most significant byte. The data transfer between registers (Key Register, Static Key Register, Data Register, Static Data Register, IV Register and Temp Register) is performed internally and automatically by this device.

REGISTER DESCRIPTIONS

Table 3-10 : Command Register

This 8-bit read/write register controls the operation of the CA20C03A. It is normally loaded only once for an entire encryption or decryption process.

Bits	Function							
7-0	CBC/$\overline{ECB}$	NK	BB	n/u	$\overline{E}$/D	KEOE	ACT	N/O

Name	Description
NEW/OLD (N/O)	When logic 0, the DES device is backward compatible with the WD2001 device in both hardware & software. When logic 1, the DES device is in CA20C03A mode.
ACTIVATE (ACT)	This bit must be logic 1 for encrypt/decrypt operation. When this bit is set from logic 0 to logic 1, one of the following events happen: • Initiates loading the Key Register in non-battery back-up key mode. • Initiates loading the Key Register in Battery Back-up Key mode while NK (command bit) is logic 1 • Initiates *Special Pattern-in Request* in Battery Back-up Key mode while NK = 0 and KV (status bit) is logic 1. • Initiates a *Data-in Request* in *Battery Back-up Key* mode while NK = 0, KV = 0, and CBC/$\overline{ECB}$ (command bit) is logic 0. • Initiates an *Initial Vector-in Request* in *Battery Back-up Key* mode while NK = 0, KV = 0 and CBC/$\overline{ECB}$ = 1.
KEY ERROR OUTPUT	When logic 0, the KEY PARITY ERROR output pin ($\overline{KPE}$) remains inactive regardless of the status of the KEY PARITY ERROR bit (status bit 5). When logic 1, the KEY PARITY ERROR output pin is active when the KPE bit (status bit 5) is logic 1. This bit set to logic 1 upon a $\overline{MASTER\ RESET}$.
ENCRYPT/DECRYPT ($\overline{E}$/D)	When logic 0, data is to be encrypted. When logic 1, data is to be decrypted.
n/u	Not used.
BATTERY BACK-UP KEY (BB)	When logic 0, the DES device is in non-battery back-up key mode. When logic 1, the DES device is in *Battery Back-up Key* mode. This bit is only used in the CA20C03A device.
NEW KEY REQUEST (NK)	This bit is ignored in non-battery back-up key mode. While in *Battery Back-up Key* mode, a *key request* is initiated when NK = 1, or the device skips the key loading process and does either the Cipher Block Chaining process or the Electronic Code process when NK = 0. This bit is only used in the CA20C03A device.
CIPHER BLOCK CHAINING/ $\overline{ELECTRONIC\ CODE\ BOOK}$ (CBC/$\overline{EBC}$)	When logic 0, the DES device encrypts/decrypts data using the Electronic Code Book method. When logic 1, the DES device encrypts/decrypts data using the Cipher Block Chaining method.

Note: All bits of the Command Register are reset to logic 0 upon $\overline{MASTER\ RESET}$ when $\overline{CRPS}$ = 1, except bit 2 (KEOE) which is set to 1. When $\overline{CRPS}$ = 0, this register is disregarded after $\overline{MASTER\ RESET}$.

Table 3-11 : Status Register

This 8-bit read-only register monitors the status of the device.

Bits	Function							
7-0	DOR	DIR	KPE	KR	IVIR	SPIR	RLK	KV

Name	Description
KEY VERIFICATION REQUEST (KV)	If the $\overline{\text{CRPS}}$ pin is logic 1, this bit is set each time the N/O bit of the Command request (KV) Register is set from logic 0 to logic 1. If the $\overline{\text{CRPS}}$ pin is logic 0 and N/O is logic 0, this bit is set upon each $\overline{\text{MASTER RESET}}$. It is reset at the end of the *Key Verification* process while the *Key* is valid, or at the end of the *Key Reloading* process. This bit is only used in the CA20C03A device.
RELOAD KEY REQUEST (RLK)	This bit is set when the user requests a new Key (NK = 1) in *Battery Back-up Key* mode (BB = 1) or at the end of the *Key Verification* process when the Key is found not valid. When this bit is set, the *Key Reloading* process starts. This bit is reset at the end of the *Key Reloading* process. The reset occurs when the encrypted *Special Pattern* (encrypted by the new loaded *Key*) is loaded into the Static Data Register from the Data Register. If this bit becomes set, it can only be cleared through the *Key Reloading* process or by performing a Master Reset (i.e. deactivating the device by writing to the command registers will not reset this bit). This bit is only used in the CA20C03A device.
SPECIAL PATTERN-IN REQUEST (SPIR)	This bit is set to logic 1 when the ACT bit is programmed from logic 0 to logic 1, BB = 1, NK = 0, and KV = 1, or when KR is reset from logic 1 to logic 0 and RLK = 1. It is reset upon loading of the last (8th) byte of the *Special Pattern* into the Data Register. This bit is only used in the CA20C03A device.
INITIAL VECTOR-IN REQUEST (IVIR)	This bit is set to logic 1 upon one of the following conditions: • Completion of Key Register loading while BB = 0 and CBC/$\overline{\text{ECB}}$ = 1. • Completion of *Key Reloading* process while BB = 1 and CBC/$\overline{\text{ECB}}$ = 1 (CA20C03A device only). • Completion of *Key Verification* process and the *Key* being found valid while BB = 1 and CBC/$\overline{\text{ECB}}$ = 1 (CA20C03A device only). • The ACT bit is set from logic 0 to logic 1 while BB = 1, NK = 0, KV = 0 and CBC/$\overline{\text{ECB}}$ = 1 (CA20C03A device only). This bit is reset upon loading of the last (8th) byte of the *Initial Vector*.
KEY REQUEST (KR)	This bit is set to logic 1 when ACT is programmed from logic 0 to logic 1 and BB = 0 or, when RLK is set internally from logic 0 to logic 1 (CA20C03A device only). It is reset upon loading of the last (8th) byte of the Key Register.
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 ACT is programmed from logic 1 to logic 0 (i.e., the device is deactivated).
DATA-IN REQUEST (DIR)	This bit is set to logic 1 upon one of the following conditions: • Completion of Key Register loading while BB = 0 and CBC/$\overline{\text{ECB}}$ = 0. • Completion of the *Key Reloading* process while BB = 1 and CBC/$\overline{\text{ECB}}$ = 0 (CA20C03A device only). • Completion of the *Key Verification* process and the *Key* being found valid while BB = 1 and CBC/$\overline{\text{ECB}}$ = 0 (CA20C03A device only). • The ACT bit is set from logic 0 to logic 1 while BB = 1, NK = 0, KV = 0 and CBC/$\overline{\text{ECB}}$ = 0 (CA20C03A device only). • Completion of IV Register loading while BB = 1 and CBC/$\overline{\text{ECB}}$ = 1 (CA20C03A device only). • Completion of Data Register reading (i.e.: the last *Data-out Request* has been serviced by an 8-byte read and the Data Register is now emptied and ready to be loaded with the next Data Word). This bit is reset upon loading of the last (8th) byte of the Data Register.
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 the last (8th) byte of the Data Register.

Note: Upon $\overline{\text{MASTER RESET}}$ and $\overline{\text{CPRS}}$ is logic 1, the Status Register is not addressable because the device comes up in the WD2001 mode. Once the Command Register is programmed into the new mode (write 1 to the N/O bit) the Status Register is addressable and will have all bits reset to 0, except the KV bit which is set to a logic 1. When $\overline{\text{CPRS}}$ = 0 and A1, O/$\overline{\text{N}}$ = 0, all bits are reset to 0 except KV (bit 0) which is set to logic 1.

Table 3-12 : KEY Register (Load Only)

This 56-bit register contains the *Key* which is used to encrypt or decrypt the data with the DES algorithm. The Key Register can be loaded with eight successive bytes only when there is a *Key Request* (status bit and output). The Key Register can also be parallel loaded from Static Key Register in Battery Back-up Key mode. This is a *write-only* register.

DATA Reg. Bits	55..49	48..42	• • •	15..07	06..00
DAL Bits	7..1	7..1	• • •	7..1	7..1
Byte Loaded	1st	2nd	• • •	7th	8th

Table 3-13 : STATIC KEY Register

This 56-bit register contains the current *Key* for data encryption and decryption using the DES algorithm. The Static Key Register is updated when a new *Key* is loaded into the Key Register and when the device is programmed for *Battery Back-up* mode. The contents of this register are retained by battery power during power-down or power failure. If the device is programmed for a mode without a Battery Back-up Key, this register is not used. The register is not accessible to the user.

DATA Reg. Bits	55..49	48..42	• • •	15..07	06..00
DAL Bits	7..1	7..1	• • •	7..1	7..1
Byte Loaded	1st	2nd	• • •	7th	8th

Table 3-14 : DATA Register

This 64-bit register contains the plain or cipher text either to be read out or that has been loaded in. During encryption, the Data Register is loaded with plain text and contains cipher text to be read out. During decryption, the Data Register is loaded with cipher text and contains plain text to be read out. The Data Register is always read or loaded with eight successive bytes (8-bit).

The Data Register can only be loaded when there is a *Data-in Request* or *Special Pattern-in Request* (Status bit and Output). Similarly, the Data Register can only be read when there is a *Data-out Request* (Status bit and Output). However, when the device is programmed for a mode with Battery Back-up, the contents of this register can be parallel loaded into the Static Data Register when the special pattern for key verification is encrypted.

DATA Reg. Bits	63..56	55..48	• • •	15..8	07..00
DAL Bits	7..0	7..0	• • •	7..0	7..0
Byte Loaded	1st	2nd	• • •	7th	8th

Table 3-15 : STATIC DATA Register

This 64-bit register contains the encrypted special pattern for key verification. When the device is programmed for a mode with a Battery Back-up, the Static Data Register is updated whenever a new key is loaded in. The special pattern is loaded in the Data Register and encrypted by the new key, then the new encrypted special pattern is loaded into the Static Data Register. The contents of this register are retained by battery power during power-down or power failure. If the device is programmed for a mode without a Battery Back-up Key, the Register is not used. This register is not accessible to the user.

DATA Reg. Bits	63..56	55..48	• • •	15..8	07..00
DAL Bits	7..0	7..0	• • •	7..0	7..0
Byte Loaded	1st	2nd	• • •	7th	8th

Table 3-16 : INITIAL VECTOR (IV) Register

This 64-bit register contains the initial vector or cipher text for the *Cipher Block Chaining* mode. This register is first loaded with the eight successive bytes (8-bit) of the Initial Vector Register for the first block of plain or cipher text. After the current text in the Data Register (plain or cipher) has been processed (encrypted or decrypted), this register is loaded with the current cipher text from the Data Register (encrypt) or the next block of text from the Temp Register (decrypt). This register is not used in the *Electronic Code Book* mode.

DATA Reg. Bits	63..56	55..48	• • •	15..8	07..00
DAL Bits	7..0	7..0	• • •	7..0	7..0
Byte Loaded	1st	2nd	• • •	7th	8th

Table 3-17 : TEMP Register

This 64-bit register is a temporary storage place used in the *Cipher Block Chaining* mode. This register temporarily stores the current cipher text, before this text is loaded into the IV Register during the decryption process. This register is loaded with the eight bytes of cipher text from the Data Register. It is not used in the *Electronic Code Book* mode and is not accessible to the user.

DATA Reg. Bits	63..56	55..48	• • •	15..8	07..00
DAL Bits	7..0	7..0	• • •	7..0	7..0
Byte Loaded	1st	2nd	• • •	7th	8th

DES ENCRYPTION MODES

Electronic Code Book (ECB) Mode Overview

The Electronic Code Book is a direct implementation of the DES algorithm in which the same plain text always generates the same ciphered text for a given cryptographic key. The CA20C03A determines the codebook entries each time. A single bit error or change, in either the input text block or the key, causes an average bit error rate of 50% for its output block. However, an error in one text block does not affect any other block. In other words, there is no error extension between blocks generated using the ECB mode.

The input and output block size is fixed at 64 bits. Since data blocks are independently ciphered, this mode is suitable for disk applications (see Figure 9).

The ECB mode has the weakness that identical block of plain text generate identical blocks of ciphered text. This violates one of the basic laws of encryption security, namely: never encrypt a given piece of information the same way twice as it makes it easier for an attacker to break the code. This shortcoming in the ECB mode is resolved by the Cipher Block Chaining mode.

Cipher Block Chaining (CBC) Mode Overview

The Cipher Block Chaining mode also operates on 64 bit data blocks, but preprocesses the information before passing it to the DES algorithm. An input data block is first EXORed with a 64 bit *Initial Vector* (IV), then processed by the DES algorithm. The resulting ciphered-output block is loaded into the IV Register, to be EXORed with the next input block. This chaining of cipher text blocks provides different outputs for identical input blocks. It also gives an error extension characteristic which protects against fraudulent data insertion, deletion or alteration in a block sequence (see Figure10). A one-bit error in the input text block, the key or the *Initial Vector* causes an average error rate of 50% in all subsequent output blocks. Thus, the CBC mode is far better suited to high-speed data communications applications.

Cipher Feedback (CFB) and Output Feedback (OFB)

These two DES modes can be implemented with the CA20C03A using the ECB mode with additional software overhead. For more information refer to the publication: *Cryptography and Data Security*, by D. Denning, Addison-Wesley Publishing Company, Inc., 1982.

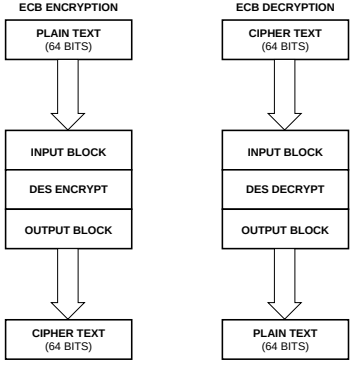


Figure 3-9 : Electronic Codebook (ECB) Mode

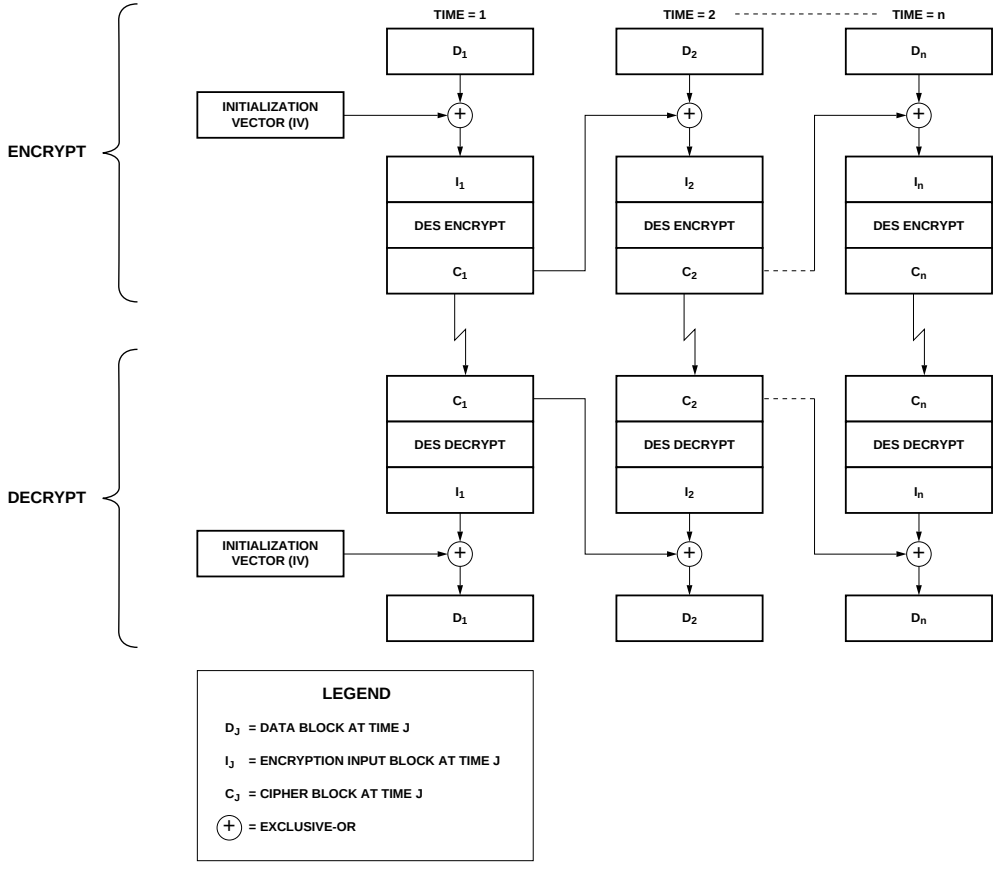


Figure 3-10 : Cipher Block Chaining (CBC) Mode

CA20C03A MODES of OPERATION

The CA20C03A can operate in two major encryption modes: Electronic Code Book (ECB) mode and Cipher Block Chaining (CBC) mode (each an implementation of the DES algorithm). Each of these two modes can be selected with or without Battery Back-up, giving a total of four operational modes (for the CA20C03A):

- Electronic Code Book without a Battery Back-up Key
- Cipher Block Chaining without a Battery Back-up Key
- Electronic Code Book with a Battery Back-up Key
- Cipher Block Chaining with a Battery Back-up Key

The CA20C03A can also be programmed to operate in a WD2001 mode, which offers ECB type encryption only. When the N/O bit is programmed to logic 1, the device is in the CA20C03A mode, and either ECB or CBC type encryption modes can be selected. When the N/O bit is logic 0, the device is in WD2001 mode. All modes are described in more detail below.

WD2001 Compatibility Mode

To ensure backward compatibility with the WD2001 device, the CA20C03A can also be programmed to emulate functions in the WD2001 (ECB mode only). This is determined by the setting of bit 0 (N/O) in the Command Register, which indicates whether the CA20C03A is in WD2001 mode (ECB) or in CA20C03A mode (ECB or CBC). When the N/O bit is programmed to logic 0, the device is in the WD2001 mode (ECB) and only the Command/Status, Data, and Key Registers are then available. The pinouts and the operation of the device and the functions of the three registers in this mode are exactly the same as in the WD2001 (refer to CA20C01 data sheet for detailed operational information). If WD2001 mode is in use in a CA20C03A device, pin 6 of the device can be connected to +5 V, or left unconnected.

Caution: *Pin 6 of a CA20C03A device must not be connected to +12 V as it will irreparably damage the device.*

Electronic Code Book without a Battery Back-up Key

The CA20C03A operates in this mode when bit 5 (BB), and bit 7 (CBC/$\overline{\text{ECB}}$) in the Command Register are set to logic 0. After the device is selected to be in this mode, it is initiated by setting bit 1 (ACT) in the Command Register to logic 1. The CA20C03A responds by activating the KEY REQUEST (KR, pin 26) output.

A0 must be deactivated (to allow the CA20C03A to internally address the Key Register) before loading the 64-bit *Key Word* into the Key Register. The Key Register is loaded with eight successive bytes (8-bit) by activating$\overline{\text{WE}}$ eight times (with $\overline{\text{CS}}$ active).

When $\overline{\text{WE}}$ is activated, the CA20C03A deactivates the KEY REQUEST (KR) output. When $\overline{\text{WE}}$ is deactivated, the CA20C03A activates the KR output. The CA20C03A activates eight *Key Requests* to fill up the Key Register.

Table 3-18 : CA20C03A Register Select

Register	$\overline{\text{CS}}$	A0	A1	$\overline{\text{CRPS}}$
Status	0	1	1	1
Command	0	1	0	1
Key, IV and Data	0	0	X	1

X = Don't care

The KR output can either be used for asynchronous handshaking (as in DMA control) or, after the first activated KR, further activations can be ignored and the Key Register can be loaded synchronously (as in programmed I/O) by eight successive activations of $\overline{\text{WE}}$.

Each byte of the *Key Word* is checked for odd parity when it is loaded into the Key Register (see Figure 3-11). If a parity error is detected, the CA20C03A sets bit 5 (KPE, KEY PARITY ERROR) in the Status Register to logic 1. If bit 2 (KEOE, KEY ERROR OUTPUT ENABLE) in the Command Register has been set, the device also activates the $\overline{\text{KPE}}$ (pin 22) output. Bit 5 (KPE, KEY PARITY ERROR) in the Status Register is reset to logic 0 when bit 1 (ACT, ACTIVATE) in the Command Register is reset to logic 0.

After loading the eighth byte of the *Key Word* into the Key Register, the CA20C03A sets DIR, DATA-IN REQUEST in the Status Register and activates the DATA-IN REQUEST (DIR, pin 27) output (see Figure 3-12). The 64-bit *Data Word* should then be loaded into the Data Register, which is loaded in the same manner as the Key Register by eight successive activations of DATA-IN REQUEST (DIR, pin 27) output and $\overline{\text{WE}}$ input.

After the eighth (last) byte of the *Data Word* has been loaded, the CA20C03A starts its operation internally by encrypting or decrypting the data to the DES algorithm. Upon completion of this operation, the encrypted or decrypted data is loaded into the Data Register, the CA20C03A sets bit 7 (DOR, DATA-OUT REQUEST) in the Status Register and activates the DATA-OUT REQUEST (DOR, pin 28) output (see Figure 3-13).

The *Data Word* must then be read from the Data Register in the same manner as it was loaded (by eight successive

activations of DATA-OUT REQUEST output and $\overline{RE}$ input).

After the first request, further activations of the DIR and DOR outputs can be ignored and the Data Register can be loaded or read by eight successive activations of $\overline{WE}$ or $\overline{RE}$.

After the eighth (last) byte of the Data Register has been read, the CA20C03A reactivates the DATA-IN-REQUEST. The cycle of loading the Data Register, encrypting or decrypting of the data to the DES algorithm, and reading the new data from the Data Register is repeated until all required data has been encrypted or decrypted with the current *Key Word*. Figures 3-11 to 3-13 are flowcharts which will aid in the understanding of the device operation in this mode.

When this is completed, bit 1 (ACT, ACTIVATE) in the Command Register should be reset to logic 0 to lock the last *Key Word* loaded into the CA20C03A. This prevents the access and use by an unauthorized user. To resume operation, the *Activate* bit must be reset to logic 1. This activates the *Key Request* and a new Key must be loaded before the Data Register can be accessed.

Plain data is encrypted by loading it into the Data Register, and encrypted data is read from the Data Register after $\overline{E}$/D, $\overline{ENCRYPT}$ /DECRYPT in the Command Register has been set to logic 0.

Data is decrypted by loading it into the Data Register, and plain data is read from the Data Register after $\overline{E}$/D, $\overline{ENCRYPT}$ /DECRYPT in the Command Register has been set to logic 1.

Caution: *To accomplish switching from encryption to decryption (or vice versa) with the same Key Word before a Data Word transfer is initiated, A0 must be set to 1 and A1 to 0. The CA20C03A then overrides the internal addressing of the Data Register and addresses the Command Register, which can now be reprogrammed. When A0 is deactivated, the device then internally addresses the Data Register, while awaiting the loading of the next Data Word.*

Cipher Block Chaining without a Battery Back-up Key

The CA20C03A operates in this mode when bit 5 (BB) and bit 7 (CBC/$\overline{EBC}$) in the Command Register are set respectively to logic 0 and logic 1. Once the device is programmed in this mode, it can be initiated by setting bit 1 (ACT) in the Command Register to logic 1. The CA20C03A now responds by activating the KEY REQUEST (KR) output. Refer to Table 3-18 for register selection.

A0 must be deactivated (to address the Key Register internally), and the Key Register must be loaded with the 64-bit *Key Word* in the same manner as performed in the Electronic Code Book mode without a Battery Back-up Key.

When the eighth (last) byte of the *Key Word* is loaded in the Key Register, the CA20C03A sets bit 3 (IV-IN REQUEST) in the Status Register and activates the IV-IN REQUEST (IVIR) output. The 64-bit *Initial Vector Word* must then be loaded into the IV Register in the same manner as the Key Register was loaded, that is, by eight successive activations of IV-IN REQUEST output and $\overline{WE}$ input.

After the eighth (last) byte of the *Initial Vector Word* has been loaded, the CA20C03A sets bit 6 (DATA-IN REQUEST) in the Status Register and activates the DATA-IN REQUEST (DIR) output. The 64-bit *Data Word* must then be loaded into the Data Register in the same manner as the Key Register was loaded, that is, by eight successive activations of DATA-IN REQUEST output and $\overline{WE}$ input.

The plain text is loaded into the Data Register when the $\overline{ENCRYPT}$ /DECRYPT bit has been set to logic 0. When this is completed, that is, after the eighth (last) byte of the plain Data Word has been loaded into the device, the contents of the IV Register are added to the plain text consecutively bit by bit with modulo 2 arithmetic and the CA20C03A begins the internal calculation of the DES algorithm for the cipher text.

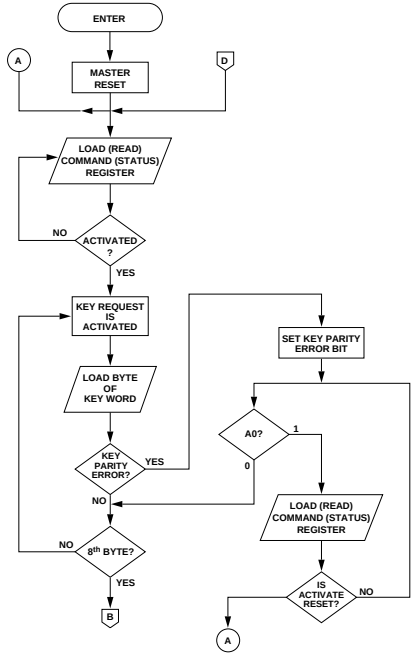


Figure 3-11 : Key Word Loading Procedure (ECB Mode Only)

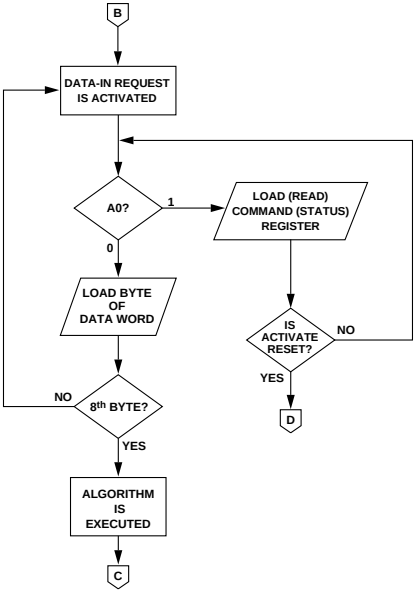


Figure 3-12 : Activating DIR Output Procedure (ECB Mode Only)

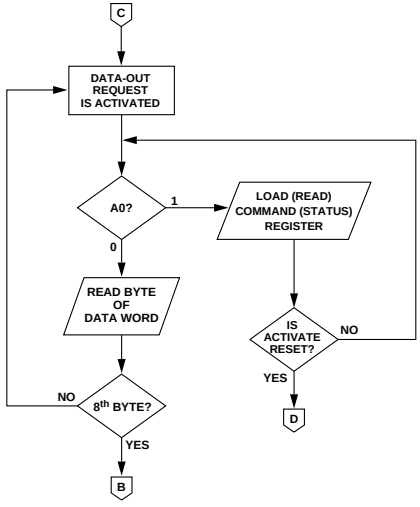


Figure 3-13 : Activating DOR Output Procedure (ECB Mode Only)

When completed, this data is loaded into both the Data Register and the IV Register (where it overrides the original *Initial Vector Word*). After (parallel) loading the new data into these two registers, the CA20C03A sets bit 7 (DATA-OUT REQUEST) in the Status Register and activates the DATA-OUT REQUEST (DOR) output.

The new cipher *Data Word* must then be read from the Data Register in the same manner as it was loaded, that is, by eight successive activations of DATA-OUT REQUEST output and $\overline{RE}$ input.

After the eighth (last) byte of the Data Register contents have been read, the CA20C03A reactivates the DATA-IN REQUEST and the next cycle can begin. This continues until all required (plain) data has been encrypted with the current Key Word in the manner previously described, that is, by:

- Loading the Data Register with plain text
- Adding the (previous) cipher text contents of the IV Register to the contents of the Data Register
- Calculating the DES algorithm for cipher text
- Loading it into the IV Register for operation (addition) to the 64-bit (plain) *Data Word*
- Reading it (cipher text) from the Data Register.

When decrypting, bits 1 (ACT) and bit 3 ($\overline{\text{ENCRYPT}}$ /DECRYPT) in the Command Register are set to 1 respectively. This activates the KEY REQUEST output indicating that the original key must now be loaded into the Key Register. After the key is loaded, the CA20C03A requests that the initial vector be loaded into the IV Register. When this is completed, the data request input pin is activated and the first eight bytes of cipher data need to be loaded into the Data Register. After the eight bytes of the cipher Data Word have been loaded into the device, the contents of the Data Register are transferred into the Temp Register and the CA20C03A begins the internal calculation of the DES algorithm for clear data. When completed, this data is added consecutively bit by bit to the contents of the IV Register using modulo 2 arithmetic. The modified plain text data is then loaded into the Data Register while the contents of the Temp Register are loaded into the IV Register, overriding the existing *Initial Vector.*

After completion of these operations, bit 7 (DATA-OUT REQUEST) in the Status Register is set and the DATA-OUT REQUEST (DOR) output is activated. The plain *Data Word* must then be read from the *Data Request* in the same manner as it was loaded, that is, by eight successive activations of DATA-OUT REQUEST output and $\overline{RE}$ input.

After the eighth (last) byte of the Data Register contents have been read, the CA20C03A reactivates the DATA-IN REQUEST and the next cycle can begin. This continues until all required (cipher) data has been decrypted with the current *Key Word* in the manner previously described:

- Load the Data Register with *cipher text*
- Load the contents of the Data Register into the Temp Register
- Calculate the DES algorithm for clear text
- Add the clear text contents in the Temp Register to the (previous) cipher text contents in the IV Register
- Load plain text into the Data Register
- Transfer the contents of the Temp Register to the IV Register for the next 64-bit cipher *Data Word*
- Read plain text from the Data Register.

As previously explained, for DATA-IN, IV-IN, and DATA-OUT, after the first request, further activations of DIR, IVIR, and DOR outputs aren't necessary. Loading the IV Register and the Data Register is performed by eight successive activations of $\overline{WE}$ and reading the Data Register is performed by eight successive activations of $\overline{RE}$.

When all required data has been encrypted or decrypted with the current *Key Word*, bit 1 (ACTIVATE) in the Command Register should be programmed to logic 0 to lock the last *Key* loaded into the CA20C03A. This prevents the access and use of it by an unauthorized user. To resume operation, the activate bit must be programmed to logic 1. This activates the *Key Request* and a new *Key* must be loaded before the Data Register can be accessed.

Caution: *At the end of each encrypted or decrypted file (or message), the CA20C03A is waiting for the Data Word, not for the reloading of the Initial Vector: that is, DIR output is active. In order to activate the IVIR output and re-load the Initial Vector, the device has to be restarted. This can be accomplished by deactivating the CA20C03A and then reactivating it once more. This forces the re-loading of the Key Word. This procedure should be followed even when it is desired to use the same Key Word for the encryption or decryption of the next file (or message).*

Electronic Code Book with a Battery Back-up Key

The CA20C03A operates in this mode when bit 5 (BB) and bit 7 (CBC/$\overline{ECB}$) in the Command Register are set respectively to logic 1 and logic 0. After the device is programmed for this mode, it is initiated by setting the ACT bit in the Command Register to logic 1. The CA20C03A responds in one of the following ways:

- When bit 6 (NK, NEW KEY) in the Command Register is set to logic 1, the CA20C03A responds by setting bit 1 (RLK, RELOAD KEY) and bit 4 (KR, KEY REQUEST) in the Status Register. It also sets the KEY REQUEST output in the *Key Reloading* state.

  Caution: *The RLK bit can only be reset by the Key Reloading process or by performing a Master Reset. Deactivating the device by writing to the Command Register will not reset this bit.*

  A0 needs to be deactivated to allow the CA20C03A to select the Key Register internally and load it with the 64-bit *Key Word* (in the same manner as in the Electronic Code Book mode without a Battery Back-up Key). Refer to Table 16 for register selection.

  When the eighth (last) byte of the *Key Word* has been loaded into the Static Key Register then bit 2 (SPECIAL PATTERN-IN REQUEST) in the Status Register is set and the SPECIAL PATTERN-IN REQUEST (SPIR, pin 4) output is activated.

  The 64-bit *Special Pattern* must now be loaded into the Data Register in the same manner as the Key Register, that is, by eight successive activations of SPECIAL PATTERN-IN REQUEST input and WE input.

  When the eighth byte of the *Special Pattern* has been loaded into the Data Register, the device starts to encrypt the *Special Pattern Word* in Electronic Code Book mode. Upon completion of the DES algorithm calculation, the cipher data is then loaded into the Static Data Register, and the CA20C03A resets RELOAD KEY bit and the KEY VERIFICATION bit in the Status Register. The device is now out of the *Key Reloading* state and continues in Electronic Code Book mode by setting bit 6 (DATA-IN REQUEST) in the Status Register and activating the DATA-IN REQUEST (DIR, pin 27) output.

- When bit 6 (NEW KEY) in the Command Register is set to logic 0 and bit 0 (KEY VERIFICATION) in the Status Register is set to logic 1, the CA20C03A responds by setting bit 2 (SPECIAL PATTERN-IN) in the Status Register. The device also activates the SPECIAL PATTERN-IN (SPIR) output, loads the contents of the Static Key Register into the Key Register in order to encrypt the *Special Pattern*, and enters the *Key Verification* state.

  A0 must be deactivated (to allow the CA20C03A to address the Data Register internally) and the Data Register must be loaded with the 64-bit *Special Pattern Word* in the same manner as the Key Register was loaded, that is, by eight successive activations of SPECIAL PATTERN-IN REQUEST output and $\overline{WE}$ input.

  When the eighth byte of the Special Pattern has been loaded into the Data Register, the CA20C03A starts to encrypt the *Special Pattern Word* in the *Electronic Code Book* mode. Upon the completion of the DES algorithm calculation, the cipher data is compared with the contents of the Static Data Register.

  If they are not the same, the CA20C03A sets bit 1 (RELOAD KEY) and bit 4 (KEY REQUEST) in the Status Register and activates the KEY REQUEST (pin 26) output to start the *Key Reloading* process as was previously described. Upon the completion of the *Key Reloading* operation, the device sets bit 6 (DATA-IN REQUEST) in the Status Register and activate the DATA-IN REQUEST (DIR, pin 27) output to start the Electronic Code Book mode.

  If the new cipher data and contents of the Static Data Register are the same, the CA20C03A resets bit 0 (KEY VERIFICATION), sets bit 6 (DATA-IN REQUEST) in the Status Register, and activates the DATA-IN REQUEST (DIR, pin 27) output to start the *Electronic Code Book* mode.

- When bit 6 (NEW KEY) in the Command Register is set to logic 0 and bit 0 (KEY VERIFICATION) in the Status Register is set to logic 0, the CA20C03A loads the contents of the Static Key Register into the Key Register, sets bit 6 (DATA-IN REQUEST) in the Status Register and activates the DATA-IN REQUEST (DIR, pin 27) output to start the Electronic Code Book mode. The operation is the same as previously described in the *Electronic Code Book* mode without a *Battery Back-up Key.*

Note that to accomplish switching from encryption to decryption (or vice versa) without deactivating the CA20C03A, and before a *Data Word* transfer is initiated, A0 must be set to 1 and A1 to 0 to address the Command Register and override the addressing of the Data Register internally. The Command Register can now be re-programmed. When A0 is reset to logic 0, the CA20C03A will now address the Data Register internally while awaiting the loading of the next *Data Word.*

Cipher Block Chaining with a Battery Back-up Key

The CA20C03A operates in this mode when the BB and CBC/$\overline{ECB}$ bits in the Command Register are set to logic 1. After the device is programmed for this mode, it is initiated by setting the ACT bit in the Command Register to logic1.

The CA20C03A responds in one of the three ways previously described in the section *Electronic Code Book with a Battery Back-up Key.* However, after completion of the *Key Reload* or *Key Verification* operations, the device starts operating in the Cipher Block Chaining mode instead of the *Electronic Code Book* mode. It sets INITIAL VECTOR-IN REQUEST in the Status Register and activates the INITIAL VECTOR-IN REQUEST (IVIR) output.

When the CA20C03A is in the *Cipher Block Chaining* mode, its operation is the same as previously described in *Cipher Block Chaining without a Battery Back-up Key.* A sample battery back-up circuit is shown in Figure 14.

Note that at the end of each encrypted or decrypted file (or message), the CA20C03A is waiting for the *Data Word*, not for the reloading of the *Initial Vector*; that is, DIR output is active. In order to activate the IVIR output and re-load the Initial Vector, the device has to be re-started by deactivating and then reactivating it. This restart procedure forces the re-loading of the *Key Word* and should be followed even when the same *Key Word* is desired for the encryption or decryption of the next file (or message).

Command Select Option

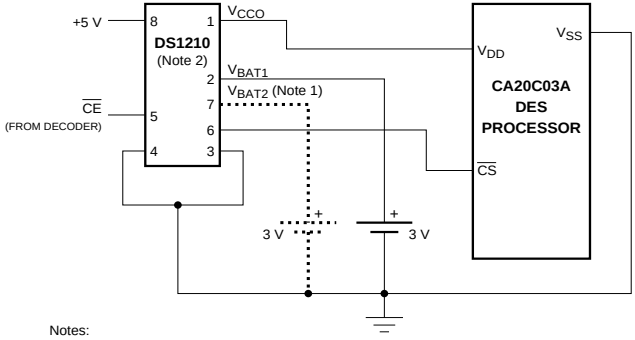
The CA20C03A can be programmed through the DAL bus lines or through the input pins. When the COMMAND REGISTER PIN SELECT ($\overline{\text{CRPS}}$, pin 20) input is set to logic 0, the (A1,O/$\overline{\text{N}}$), ACT, $\overline{\text{E}}$/D, BB, (A0,NK), and CBC/$\overline{\text{ECB}}$ pins are enabled as inputs which override bits 0, 1, 3, 5, 6, and 7 in the Command Register. This override allows input pins to control the CA20C03A. Bit 2 (KEOE) in the Command Register remains at logic 1.

The A1 and A0 bits are disregarded in this option, and the Command and Status Registers cannot be accessed using the DAL bus lines.

Note that the ACT pin must be toggled from logic 1 to logic 0 to clear a parity error detection when operating in this mode.

All other operations are the same as described previously.

Caution: *Upon* $\overline{\text{MASTER RESET}}$ *, while* $\overline{\text{CRPS}}$ *and A1,O/*$\overline{\text{N}}$ *pins are logic 0, the CA20C03A does not return to the 2001 mode, but stays in the CA20C03A mode and sets bit 0 (KV) in the Status Register.*



Notes:

1. V_{BAT2} is optional (use if double redundant back-up is required for failsoft operation).
2. Dallas Semiconductor DS1210 Non-volatile Controller.

Figure 3-14 : CA20C03A Battery Back-up Circuit Example

Table 3-19 : Test Data For Electronic Codebook (ECB) Mode

E-Key=D-Key= 0123456789ABCDEF		
Encryption		
Time	**Plain Text**	**Cipher Text**
1	4E6F772069732074	3FA40E8A984D4815
2	68652074696D6520	6A271787AB8883F9
3	666F7220616C6C20	893D51EC4B563B53
Decryption		
Time	**Cipher Text**	**Plain Text**
1	3FA40E8A984D4815	4E6F772069732074
2	6A271787AB8883F9	68652074696D6520
3	893D51EC4B563B53	666F7220616C6C20

Table 3-20 : Test Data For Cipher Block Chaining (CBC) Mode

E-Key = D-Key = 0123456789ABCDEF IVE = IVD = 1234567890ABCDEF		
Encryption		
Time	**Plain Text**	**Cipher Text**
1	4E6F772069732074	E5C7CDDE872BF27C
2	68652074696D6520	43E934008C389C0F
3	666F7220616C6C20	683788499A7C05F6
Decryption		
Time	**Cipher Text**	**Plain Text**
1	E5C7CDDE872BF27C	4E6F772069732074
2	43E934008C389C0F	68652074696D6520
3	683788499A7C05F6	666F7220616C6C20

Note for Table 3-19 and Table 3-20: The plain text in both cases is the ASCII code for “Now is the time for all …”. These seven-bit characters are written in hexadecimal notation: 0, b6, b5, b4, b3, b2, b1, b0.