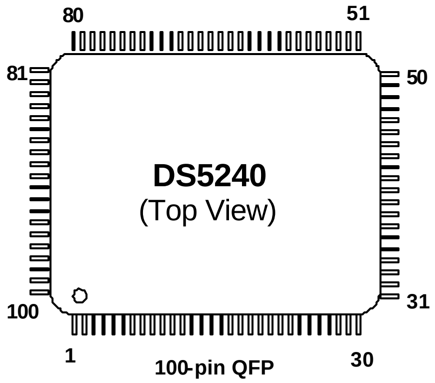
**An NDA is required for full disclosure of details. Contact factory.**

# DS5240
## High-Speed Secure Microcontroller

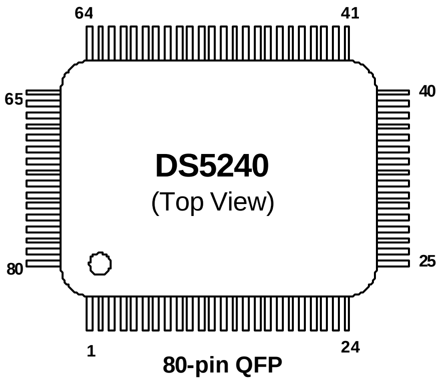
www.maxim-ic.com

## FEATURES

- **Security features**
- – Designed to meet the physical security requirements of FIPS140 and Common Criteria certifications
- – Fine-line, top-level metal pattern detects intrusion of the chip’s cryptographic boundary
- – Additional on-chip sensors detect out-of-range environmental conditions that generate a tamper response
- – The equipment enclosure can be monitored by tamper response inputs for added protection
- – Fast write SRAM technology causes rapid “zeroization” of secure information as a tamper response
- – Eavesdropping on the external memory bus prevented by single or triple-DES encryption of the programs
- – Internal chip clock isolated from external system clock by phase-locked loop
- – Asynchronous internal ring oscillator provides clock for arithmetic operations
- – Resources inside cryptographic boundary include:
    - – Modulo Arithmetic Accelerator (MAA) for up to 4096-bit (e.g., PKI)
    - – DES and 112-bit key triple-DES engines available for secret key cryptography
    - – Random number generator
    - – Memory Management Unit and 1kB cache
    - – Firmware bootstrap loader resides in a 16kB factory-programmed ROM
- **8051 compatible with expanded addressing**
- – Linear address space directly accesses up to 8MB of external memory
- – Dedicated memory and parallel I/O bus saves port pins
- – Four 8-bit ports, one 6-bit port
- **Advanced features**
- – CRC-16/32 generator provides strong error detection of memory contents
- – True-time clock with alarm interrupt and wake-up
- – 5kB internal SRAM with 1kB that can be allocated to a stack for high-level language support
- – Programmable length MOVX instructions allow a combination of fast and slow devices
- – On-chip power detection/selection circuits provide power-up/down processor reset and early-warning power-fail interrupt
- – Watchdog timer
- **Proven 4-clock/machine cycle architecture**
- – Single-cycle instruction executes in 160ns
- – Runs up to 25MHz clock rates
- – Dual data pointers can increment or decrement independently
- – Automatic data pointer selection available



100-pin QFP



80-pin QFP

**Note:** Some revisions of this device may incorporate deviations from published specifications known as errata. Multiple revisions of any device may be simultaneously available through various sales channels. For information about DS5240 device errata, contact the factory.

# DESCRIPTION

The DS5240 is a high-speed 8051 compatible security processor with built-in system features designed to meet the stringent FIPS-140 and Common Criteria validations required by banking regulations worldwide. Based on Dallas Semiconductor's battery-backed technology and fast-erase SRAM design, the DS5240 supports rapid "zeroization" of secure information as a tamper response. Security-related features included on-chip are a fine-line top-level metal grid to protect underlying circuitry from tampering, a Modulo Arithmetic Accelerator (MAA) using words up to 4096-bits in length for calculations including Public Key Infrastructure (PKI), a random number generator for key creation, multiple on-chip environmental sensors to detect out-of-range conditions and generate a tamper response, and a user-available DES engine for arbitrary data encryption. The user DES engine supports both single and triple-DES (3DES) cryptographic operations. Other on-chip features include a true-time clock with alarm interrupt/wake-up capability, a CRC-16/32 generator, a phase-locked loop (PLL) to simplify crystal selection and to isolate internal chip clocks from external system clock, extended memory addressing of up to 4MB program and 4MB data and a 1kB stack (part of 5kB total SRAM) for high-level language support, circuitry to control battery backing of certain internal circuits and external SRAM for storage of program and/or data, and sleep, idle and power management modes for low power applications.

The DS5240's comprehensive security measures create a trusted computing environment for the most sensitive applications. These measures include an array of features specifically designed to resist known threats including observation, analysis, and physical attack. They are designed such that a massive effort would be required to obtain information about the contents of the chip (e.g., stored encryption keys) and/or external memory. Furthermore, the "soft" nature of the DS5240 (SRAM storage) allows frequent modification of secure information, either program or data.

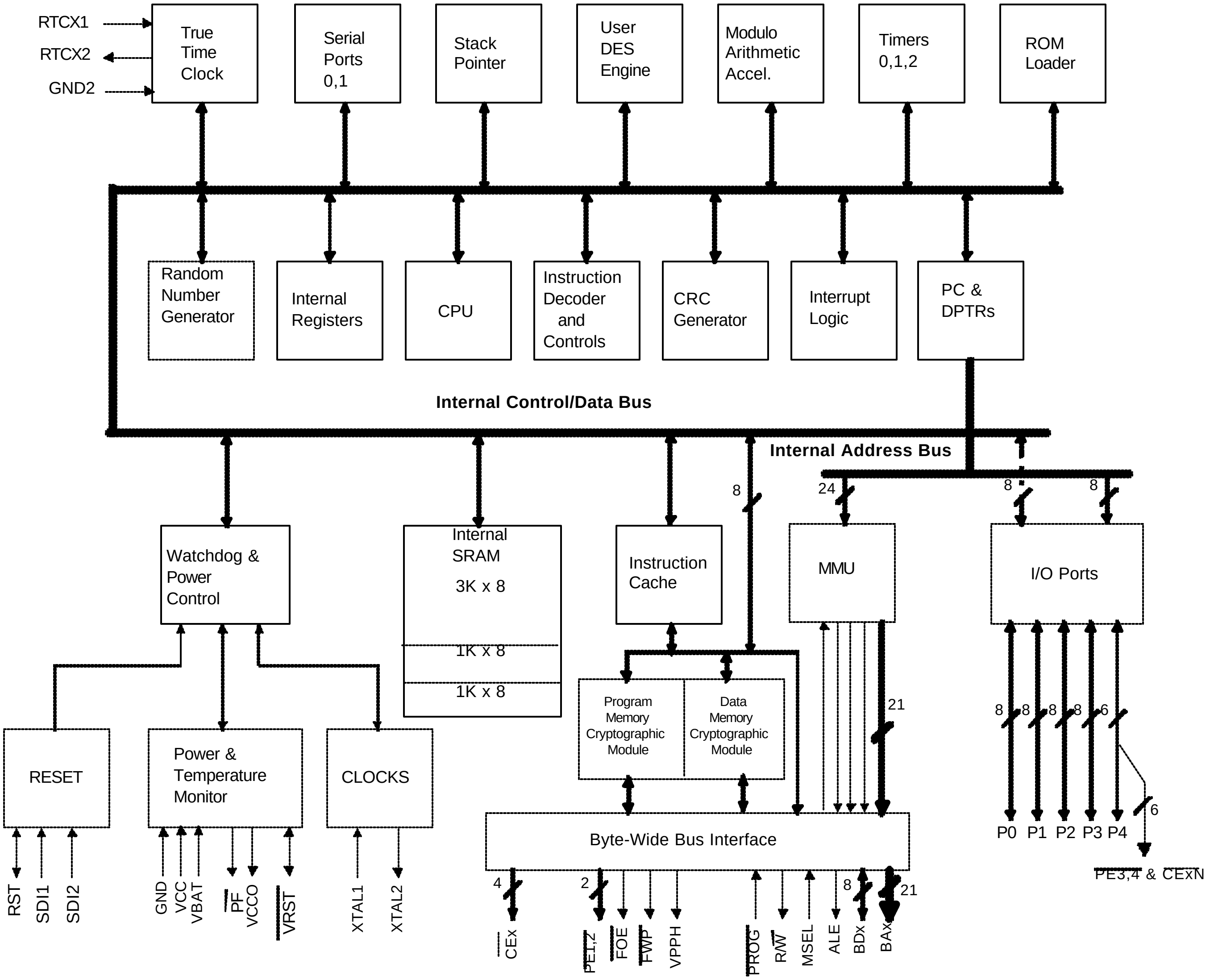
The DS5240 implements a physical and logical security system that is more extensive than found in its predecessor, the DS5002 secure microcontroller. Like the DS5002, the DS5240 executes application software from encrypted storage. However, on the DS5240, the encryption implemented is a true block cipher, according to the Data Encryption Standard (DES or triple-DES). Attempts to discover the keys through physical tampering result in their erasure, rendering the encrypted contents of external memory useless. Up to 4MB of program space and 4MB of data space can be accessed through a dedicated, nonmultiplexed byte-wide bus leaving all port pins available for I/O functions. The contents of external memory are maintained during power-off by power from a battery connected to the DS5240. In the absence of $V_{CC}$, battery power maintains the memory. A small lithium coin cell can provide more than 10 years of data retention.

All the security features of the DS5002 are implemented in the DS5240, with two distinctions. First, encryption of the address bus is not employed for external program memory (only the program information on the data bus is encrypted) and second, there are no dummy read cycles performed on the embedded bus. Strong new security measures are added to the DS5240, including selectable 3DES encryption of program memory where the encryption is based on 112-bit (two word) keys that are automatically generated by the random number generator. There are also two self-destruct inputs (SDI) provided. One SDI controls destruction of external program and data, cache memory, key registers and selected areas of internal SRAM. The second SDI functions as an interrupt, allowing the user to take advantage of the DS5240's ability to respond to a detected attack under software control. The DS5240 also offers a number of selectable built-in countermeasures against known attack methodologies. The device incorporates on-chip sensors to monitor "out-of-range" conditions, and these sensors can force the device to undergo a special destructive reset if desired. Finally, the DS5240 supports optional timed-access write operations to the parallel I/O port pins, making certain attack approaches ineffective.

## ORDERING INFORMATION

| PART | PIN-PACKAGE | MAX CLOCK SPEED (MHz) | TEMP. RANGE |
|---|---|---|---|
| DS5240F-825 | 80-Plastic MQFP | 25 | 0°C to +70°C |
| DS5240F-125 | 100-Plastic MQFP | 25 | 0°C to +70°C |
| DS5240F-8N5 | 80-Plastic MQFP | 25 | -40°C to +85°C |
| DS5240F-1N5 | 100-Plastic MQFP | 25 | -40°C to +85°C |

Figure 1. **BLOCK DIAGRAM**


RTCX1
RTCX2
GND2
True Time Clock
Serial Ports 0,1
Stack Pointer
User DES Engine
Modulo Arithmetic Accel.
Timers 0,1,2
ROM Loader
Random Number Generator
Internal Registers
CPU
Instruction Decoder and Controls
CRC Generator
Interrupt Logic
PC & DPTRs
Internal Control/Data Bus
Internal Address Bus
8
24
8
8
Watchdog & Power Control
Internal SRAM
3K x 8
1K x 8
1K x 8
Instruction Cache
MMU
I/O Ports
Program Memory Cryptographic Module
Data Memory Cryptographic Module
21
8 8 8 8 6
6
RESET
Power & Temperature Monitor
CLOCKS
Byte-Wide Bus Interface
P0 P1 P2 P3 P4
PE3,4 & CExN
RST
SDI1
SDI2
GND
VCC
VBAT
PF
VCCO
VRST
XTAL1
XTAL2
4
2
8
21
CEx
PE1,2
FOE
FWP
VPPH
PROG
R/W
MSEL
ALE
BDx
BAx