A Non-Disclosure Agreement (NDA) is required for full disclosure of details. Contact factory for more information.

DS5250
High-Speed Secure Microcontroller

www.maxim-ic.com

GENERAL DESCRIPTION

The DS5250 is a highly secure, 4 clocks-per-machine cycle, 100% 8051-instruction-set-compatible microprocessor in the Secure Microcontroller family from Dallas Semiconductor. It was designed to be the cryptographic engine of PIN pads, financial terminals, and any other application in which data security is paramount. A key feature of the device is that it encrypts its program memory with a hardware-based single or triple (3) DES (data encryption standard) algorithm, making it nearly impossible to extract information. Another DES (3DES) hardware block is available to the user for encrypting arbitrary information in data memory space. This makes the device ideal for storage and transmission of passwords, personal identification numbers, encryption keys, and other highly confidential information.

APPLICATIONS

PIN Pads
Financial Terminals
Applications that Require Data Security

ORDERING INFORMATION

PART	TEMP RANGE	MAX CLOCK SPEED (MHz)	PIN-PACKAGE
DS5250F-825	0°C to +70°C	25	80 Plastic MQFP
DS5250F-125	0°C to +70°C	25	100 Plastic MQFP
DS5250F-8N5	-40°C to +85°C	25	80 Plastic MQFP
DS5250F-1N5	-40°C to +85°C	25	100 Plastic MQFP

Pin Configurations appear on page 2.

FEATURES

- **Drop-In Upgrade to the Dallas DS5240**
- **Feature-Rich, 8051-Compatible, Highly Secure Microcontroller**
  - Accesses Up to 4MB Program and 4MB Data Memory (All Nonvolatile)
  - In-System Programmable through Serial Port
  - In-Application Programmable through User Software; Allows Self-Modification of Program/Data Memory
  - Four 8-Bit Ports/One 6-Bit Port
  - Three 16-Bit Timer/Counters
  - 256 Bytes of Scratchpad RAM
- **Advanced Features**
  - CRC-16/32 Generator
  - 5kB Internal SRAM (Optional 1kB Stack)
  - Single or 3DES Engine
  - Partitionable Memory Segments Variable from 4kB to 256kB
- **High-Speed Architecture**
  - 4 Clocks-per-Machine Cycle
  - DC-to-25MHz Operation
  - Single-Cycle Instruction in 160ns
  - Dual Data Pointers can Increment or Decrement Independently
  - Automatic Data Pointer Selection Available
  - Programmable Speed MOVX Instructions
  - 1kB On-Chip Instruction Cache
- **High-Reliability Operation**
  - Power-Fail/Overvoltage Reset
  - Early-Warning Power-Fail Interrupt
  - Watchdog Timer
- **Nonvolatile Functions**
  - On-Chip Real-Time Clock with Alarm Interrupt
  - 2kB Battery-Backed Internal SRAM
- **Security Features**
  - Designed to Meet the Physical Security Requirements of FIPS-140 and Common Criteria Certifications
  - Program Memory Integrity Checking
  - Executes Single/3DES-Encrypted Programs to Prevent Observation
  - Separate Program/Data Cryptograph
  - Two Self-Destruct Inputs
  - 4096-Bit Modulo-Arithmetic Accelerator (MAA) for PKI Operations
  - Built-In Sensors Detect Attack and Cause Security Response
  - Programmable Attack Countermeasures
  - Secure Bootstrap Loader
  - True Random-Number Generator (RNG)
  - Unique ID Number in Every Device

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 DS5250 errata, contact the factory.

DETAILED DESCRIPTION

The DS5250 has a user-selectable, program memory integrity-checking feature that triggers a tamper response if the decrypted program memory does not match a precalculated checksum, indicating a possible attack. In addition, all encryption keys for encrypted memory are stored in internal battery-backed SRAM so they can be erased instantaneously in the event tamper activity is detected. The battery-backed memory architecture subjects critical application data and encryption keys stored internally to instantaneous zeroization, as defined in Federal Information Processing Standard (FIPS) 140-1 as a tamper response. Additionally, power is removed from external memory, and all data and address lines are collapsed as an additional response to tamper detection.

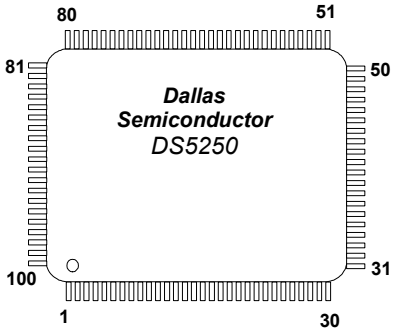
The DS5250 incorporates the most sophisticated security features available in any microprocessor. The security features resist multiple levels of threat, including observation, analysis, and physical attack. Attempts to discover the device's encryption keys result in their erasure, rendering useless the encrypted external memory. Such measures require a massive effort to acquire any information about the memory contents. Sophisticated internal sensors monitor various environmental parameters, and trigger a tamper response if they deviate from acceptable levels. A microprobe shield covers the top of the microcontroller die and deters tampering by triggering a destructive reset if it is breached. Other security measures implement defenses against known direct and side-channel attacks. Specific security-related hardware includes a 4096-bit MAA for public key infrastructure (PKI) calculations, a random-number generator, a CRC-16/32 generator, and a user-available DES (or 3DES) engine.

In addition to the internal sensors, two external self-destruct input (SDI) pins allow the designer to trigger a tamper response based on user-defined external stimuli. One SDI input controls destruction of program memory, external data memory, cache memory, key registers, and all the internal 5kB RAM. The second SDI functions as an interrupt, allowing the application software to appropriately respond to a detected attack. Other security methods include optional timed-access-write restrictions to the parallel I/O port pins, making certain attack practices ineffective.

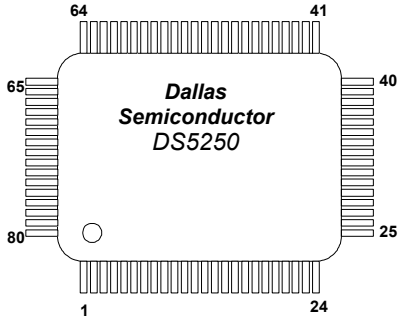
Program loading is accomplished using a secure ROM-based serial port bootloader. The battery-backed nature of the DS5250, combined with an internal ROM-based bootloader, allows frequent modification of secure information, either program or data, through a secure loading mechanism. An optional challenge-response protection of access to the bootstrap-ROM loader ensures that only trusted agents can load programs into the device. Once the challenge response has been successfully completed, communications between the host system and the microcontroller are conducted in a 3DES cipher-block-chained data stream to prevent communication interception. Alternatively, a user can create a custom bootloader using the microcontroller's encryption tools.

PIN CONFIGURATIONS

TOP VIEW

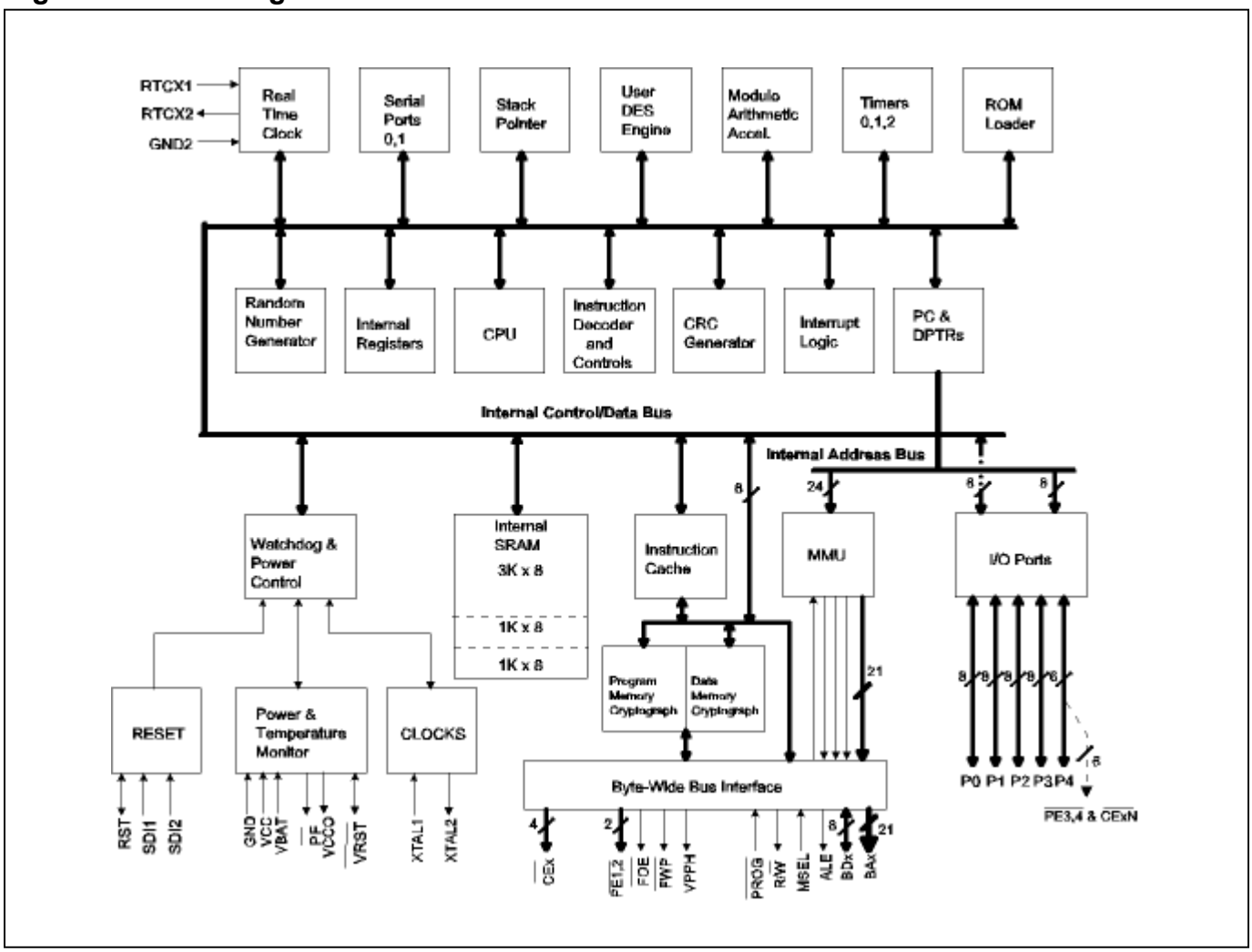


MQFP



MQFP

Figure 1. Block Diagram



Maxim Integrated Products, 120 San Gabriel Drive, Sunnyvale, CA 94086 408-737-7600