THE DATASHEET OF

DS3644EVKIT#

DS3644

DeepCover Security Manager with 1KB Secure Memory and Programmable Tamper Hierarchy

Tamper-Detection Hierarchy with On-Chip Nonimprinting Memory Safeguard Critical Data

Overview | Technical Documents | Ordering Info | Related Products | User Comments (0) | All

Status

Active: In Production.

Data Sheet

Request Full Data Sheet
NDA Required

Description

DeepCover™ embedded security solutions cloak sensitive data under multiple layers of advanced physical security to provide the most secure key storage possible.

The DeepCover Security Manager (DS3644) is a secure supervisor with 1024 bytes of SRAM for the secure storage of sensitive data and the physical tamper-sensing response functions required in cryptographic processors and data security equipment.

One of the DS3644's primary features is the on-chip nonimprinting memory, consisting of eight 128-byte banks incorporating a high-speed, direct-wired clearing function. The 1KB memory is constantly complemented in the background to prevent memory imprinting of data. The DS3644 architecture allows the user to clear selective banks of the memory based upon specified tamper events. In the event of a qualified tamper event, the desired bank(s) of memory are rapidly cleared and a negative bias can be applied to erase external memory.

The DS3644 includes a seconds counter, watchdog timer, CPU supervisor, nonvolatile (NV) SRAM controller, and on-chip temperature sensor. In the event of a primary power failure, an external battery source is automatically switched in to keep the memory, time, and tamper-detection circuitry active. The DS3644 provides low-leakage, tamper-detection inputs for interface to external sensors, interlocks, and antitamper meshes. The DS3644 also invokes a tamper event on absolute temperature, if the temperature rate-of-change exceeds programmed limits, or if the crystal oscillator frequency falls outside a specified window. The tamper event is latched and timestamped for fault-recovery purposes.

Access to the timer, tamper monitoring, memory, and device configuration is conducted through an I²C-compatible interface. The DS3644 is assembled in a Pb-free, 7mm x 7mm x 0.8mm CSBGA package.

Key Features

- Memory
  - 1024-Byte Nonimprinting Memory with High-Speed Erase
  - 64 Bytes General-Purpose RAM (Not Cleared)
  - External SRAM Control and Optional Tamper-Event Erasure
  - Segmented Tamper-Detection Memory Hierarchy with Programmable Tamper-Event Sources
- Tamper
  - On-Chip Programmable Temperature Sensing with Proprietary Rate-of-Change (ROC) Detector
  - Two General-Purpose Tamper-Detect Logic Inputs
  - Four Uncommitted Tamper-Detect Comparator Inputs
  - Four Window Comparators with On-Chip Reference Voltage
  - Latching and Timestamping of Tamper Events
  - Crystal Oscillator Tamper Monitoring
- Other
  - Programmable Power-Consumption Options for Very Low Standby Current
  - 64-Bit Unique Silicon Serial Number
  - On-Chip Random-Number Generator (RNG)
  - Designed to Meet NIST FIPS 140-2 Requirements
  - 32-Bit Seconds Counter with Watchdog Timer and Alarm Output
  - CPU Supervisor
  - I²C-Compatible Interface

Applications/Uses

- Access-Control Security Systems
- ATMs
- Cryptographic Processors
- E-Commerce Servers
- Gaming Systems
- Network Routers and Switches
- Network Storage Servers
- PIN Pads
- Point-of-Sale Terminals
- Secure Communications
- Set-Top Boxes
- Smart Card Readers
- Software-Defined Radios

Key Specifications:

Security Managers

Part Number	Analog Voltages Monitored	Digital Inputs Monitored	Internal Key Memory (Bytes)	Ext. Memory Cntrl.	Random Number Gen.	Over Voltage Monitor	Battery Monitor	Package/Pins	Smallest Available Pckg. (mm^2) max w/pins	Oper. Temp. (°C)
DS3644	4	2	1024	Yes	Yes	Yes	Yes	CSBGA/49	49	-55 to +95

See All Security Managers (11)

Pricing Notes:

This pricing is BUDGETARY, for comparing similar parts. Prices are in U.S. dollars and subject to change. Quantity pricing may vary substantially and international prices may differ due to local duties, taxes, fees, and exchange rates. For volume-specific prices and delivery, please see the price and availability page or contact an authorized distributor.

Technical Documents

App Note 3976 Embedded Security Going Forward
App Note 4244 Secure Managers Provide Multifaceted Monitoring to Ensure System Security
App Note 4297 Battery Selection for Secure Supervisor Applications
App Note 4728 Using Window Comparators in Secure Managers
App Note 5049 Using the DeepCover Security Manager (DS3645) Power-Management Mode
App Note 5524 Securing Critical Data with Hardware AES Engines

Product Guides

Microprocessor Supervisory (PDF)
Real-Time Clocks (PDF)

Reliability Reports

Reliability Report: DS3644.pdf

Product Change Notices

Device	Issue Date	Area	Product Change Notice
DS3644B+	2011-12-22	DESIGN	Product Change Notice 934 (PDF, 30.8kB)
	2011-09-13	ASSEMBLY	Product Change Notice 968-ERRATA (PDF,
	2011-09-13	ASSEMBLY	45.8kB)
	2009-11-18	ASSEMBLY	Product Change Notice 968 (PDF, 45.7kB)
	2009-09-18	ASSEMBLY	Product Change Notice 707 (PDF, 166.4kB)
			Product Change Notice 696 (PDF, 121.2kB)

Disclaimer

PCN's displayed are for notification only and are effective on the date distributed.

Software/Models

none

Ordering Information

Filters: Part Number [ ] Package: Any Temperature: Any Tape and Reel Sample Go

Part Number	Free Sample	Buy	Status	Package: TYPE PINS FOOTPRINT DRAWING CODE/VAR *	Temp	RoHS/Lead-Free? Materials Analysis
DS3644B+	Sample	Buy	Active	CSBGA;49 pin;49 mm^2 Outline Drawing:21-0356 (PDF) Land Pattern: 90-0318 (PDF) Use pkgcode/variation: X49+3*	-40°C to +85°C	RoHS/Lead-Free: Lead Free Materials Analysis
DS3644B+DIE	Sample	Buy	Active	DICE SALES;NA pin;CSBGA; Land Pattern: Not Applicable Use pkgcode/variation: DICE12+*	-40°C to +85°C	See data sheet
DS3644B+TRL		Buy	Active	CSBGA;49 pin;49 mm^2 Outline Drawing:21-0356 (PDF) Land Pattern: 90-0318 (PDF) Use pkgcode/variation: X49+3*	-40°C to +85°C	RoHS/Lead-Free: Lead Free Materials Analysis
DS3644B+W		Buy	Active	CSBGA;49 pin;49 mm^2 Outline Drawing:21-0356 (PDF) Land Pattern: 90-0318 (PDF) Use pkgcode/variation: X49+3*	-40°C to +85°C	RoHS/Lead-Free: Lead Free Materials Analysis
DS3644B/TR+W		Buy	Active	CSBGA;49 pin;49 mm^2 Outline Drawing:21-0356 (PDF) Land Pattern: 90-0318 (PDF) Use pkgcode/variation: X49+3*	-40°C to +85°C	RoHS/Lead-Free: Lead Free Materials Analysis
DS3644EVKIT#		Buy	Active	KIT; Land Pattern: Not Available		See data sheet

Notes:
1. Other options and links for purchasing parts are listed at: http://www.maximintegrated.com/sales.
2. Didn't Find What You Need? Ask our applications engineers. Expert assistance in finding parts, usually within one business day.
3. Part number suffixes: T or T&R = tape and reel; + = RoHS/lead-free; # = RoHS/lead-exempt; -D = drypack; -U/+U on DS parts = cut tape. More: See Full Data Sheet or Maxim Product Naming Conventions.
4. * Some packages have variations, listed on the drawing. "PkgCode/Variation" tells which variation the product uses. Note that "+", "#", "-" in the part number suffix describes RoHS status. Package drawings may show a different suffix character.

Similar Products by Function

See All Security Managers (11 Products)

Similar Products by Application

Building Block Advisor > Battery Backup
Building Block Advisor > Secure Microcontroller
Building Block Advisor > Temperature Sensors
Building Block Advisor > Watchdog Timers
Computers: Desktops and Workstations > Microprocessor Supervisors
Computers: Desktops and Workstations > Nonvolatile Memory (NV SRAM)
Computers: Desktops and Workstations > Single, Low-Voltage Supervisors
Computers: Desktops and Workstations > Real-Time Clocks
Computers: Desktops and Workstations > Thermal Management
PIN Pads and Kiosks > Secure Microcontroller
Point-of-Sale (POS) Terminals > Security Manager
Programmable Logic Controllers (PLCs) > Security Manager
Smart Electricity Meters > Tamper Detect

More Information

New Product Press Release [2010-06-01]

Your Comments

Login or register to post a comment.

Didn't Find What You Need?

- Next Day Product Selection Assistance from Applications Engineers
- Parametric Search
- Applications Help

Information Index

Overview
Description
Key Features
Applications/Uses
Key Specifications
Diagram
Notes and Comments

Technical Documents
Data Sheet
Technical Documents
Evaluation Kits
Reliability Reports
Software/Models

Ordering Info
Price and Availability
Samples
Buy Online
Package Information
Lead-Free Information

Related Products
Similar Products by Function
Similar Products by Application
Evaluation Kits
Products with Similar Part Numbers
Products Used With This

Rev 1; 2010-11-30
This page last modified: 2012-10-29

Looking for pricing, stock, or lifecycle information?

Click below to explore more details on WIN SOURCE:

- View DS3644EVKIT# on WIN SOURCE
- Maxim Integrated Information

Optimize Your Supply Chain with WIN SOURCE Solutions

- Global Sourcing Solution
- Obsolete Management
- Cost Control Management
- Shortage Management
- Alternative Solution
- Excess Inventory Management