

Embedded Security

Product Guide

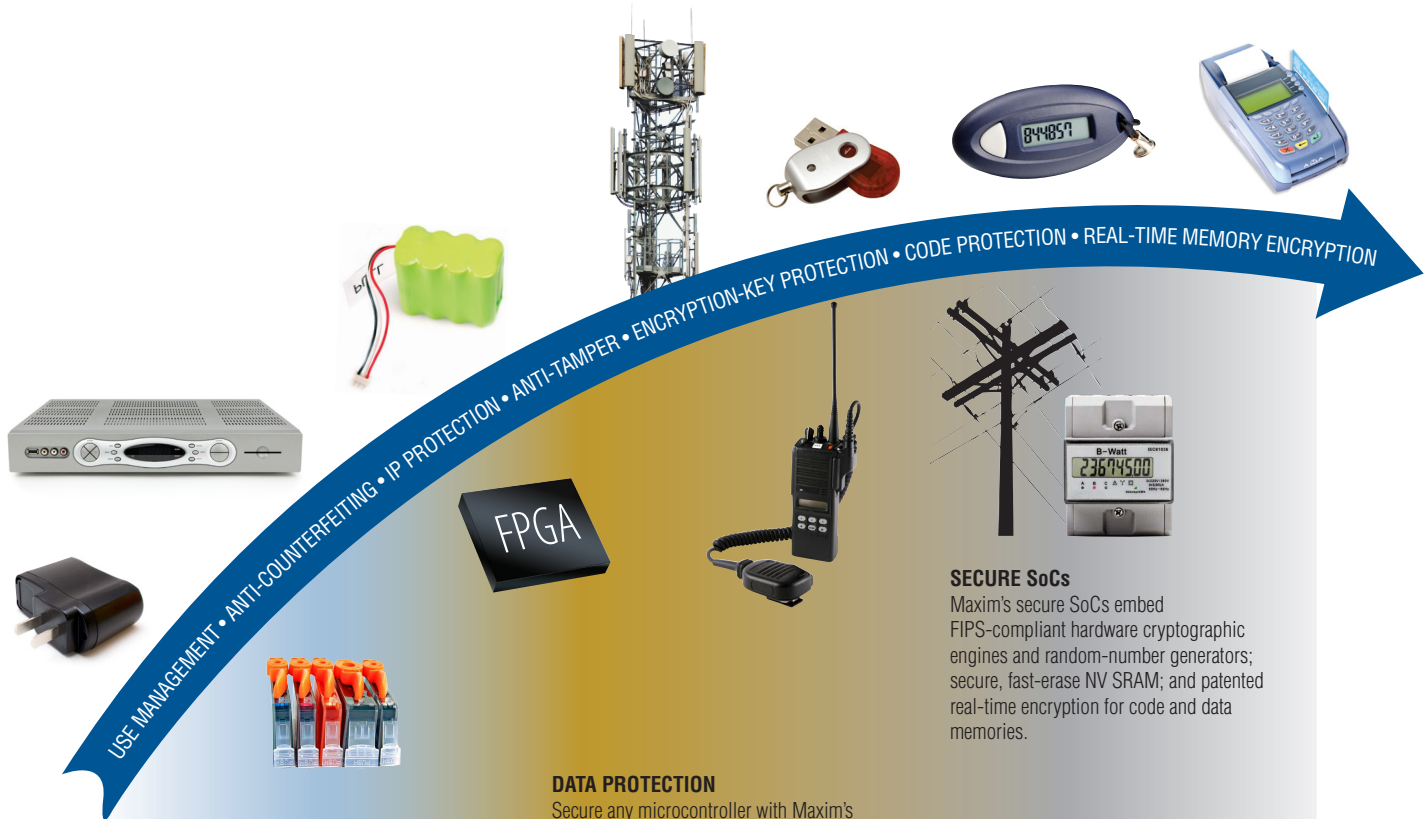


Inside:

- 2** Embedded Security Products and Applications
- 3** High-Performance TFT-Enabled Secure Microcontroller
- 6** Secure Authenticator Solutions for Counterfeiting Protection
- 7** High-Security and Tamper-Protected Security Managers

Complete Solutions. Complete Security.

The best protection schemes are secured by silicon. Whether you need to encrypt financial transactions, authenticate access or usage, or protect intellectual property (IP), Maxim's proven platforms will ensure that you and your customers are secure.



AUTHENTICATION

Secure memories provide crypto-strong secure authentication to protect your design investment and IP from cloning. They can also be used to implement limited-use sensors, manage reference design use, and securely set system features.

DATA PROTECTION

Secure any microcontroller with Maxim's security managers. These devices combine active tamper detection with a patented memory architecture that stores encryption-key data in on-chip nonimprinting memory, which is instantly and completely erased upon qualified tamper events.

SECURE SoCs

Maxim's secure SoCs embed FIPS-compliant hardware cryptographic engines and random-number generators; secure, fast-erase NV SRAM; and patented real-time encryption for code and data memories.

Go Meshless!

Secure SoC with On-the-Fly Memory Encryption

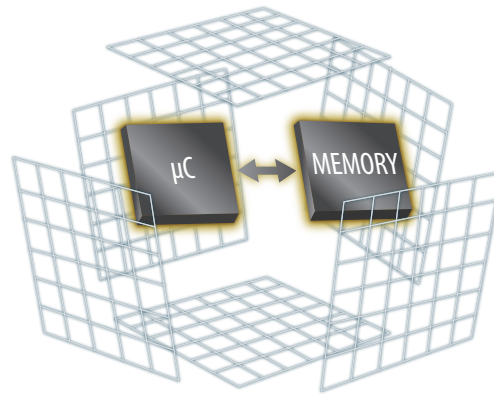
The MAX32590* (JIBE) is a secure, ARM9™-based, system-on-chip (SoC) μC with a 384MHz clock speed and Ethernet interface communication to meet stringent financial terminal requirements. Our patented on-the-fly encryption technology keeps your code safe without the hassle of expensive mesh. PCI PTS 3.1 certification is easy with an extensive board support package and Linux® OS support, innovative security mechanisms, and high integration. Replace the traditional mono LCD with a colorful TFT display to provide better visual effects for your designs.

Features

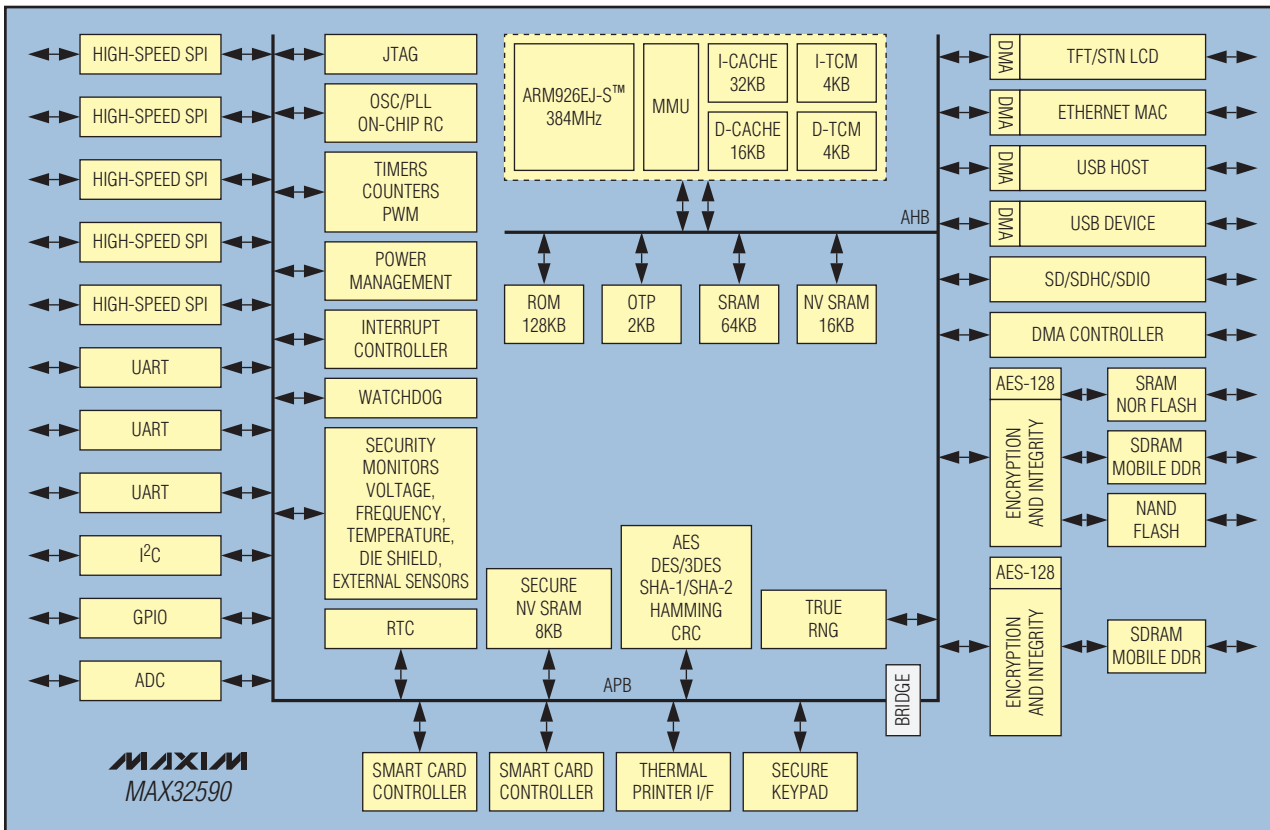
- Extensive security mechanisms (authenticated boot, secure NV SRAM with instant erase, OTP, AES/SHA engines, dynamic sensor controller, temperature/voltage and frequency monitors, secure package)
- High system integration (Ethernet, TFT LCD, 384MHz CPU, USB host and device)
- Real-time external memory encryption and integrity

Benefits

- Reduced BOM with fewer external communication controllers; better user experience with color TFT display
- Provides best confidentiality while removing the need for an additional security cover; prevents code injection
- Simplifies security architecture and eases PCI certification



Break Free from the Cage—
On-the-Fly Memory Encryption Lets You Trust Your Code.



*Future product—contact the factory for availability.

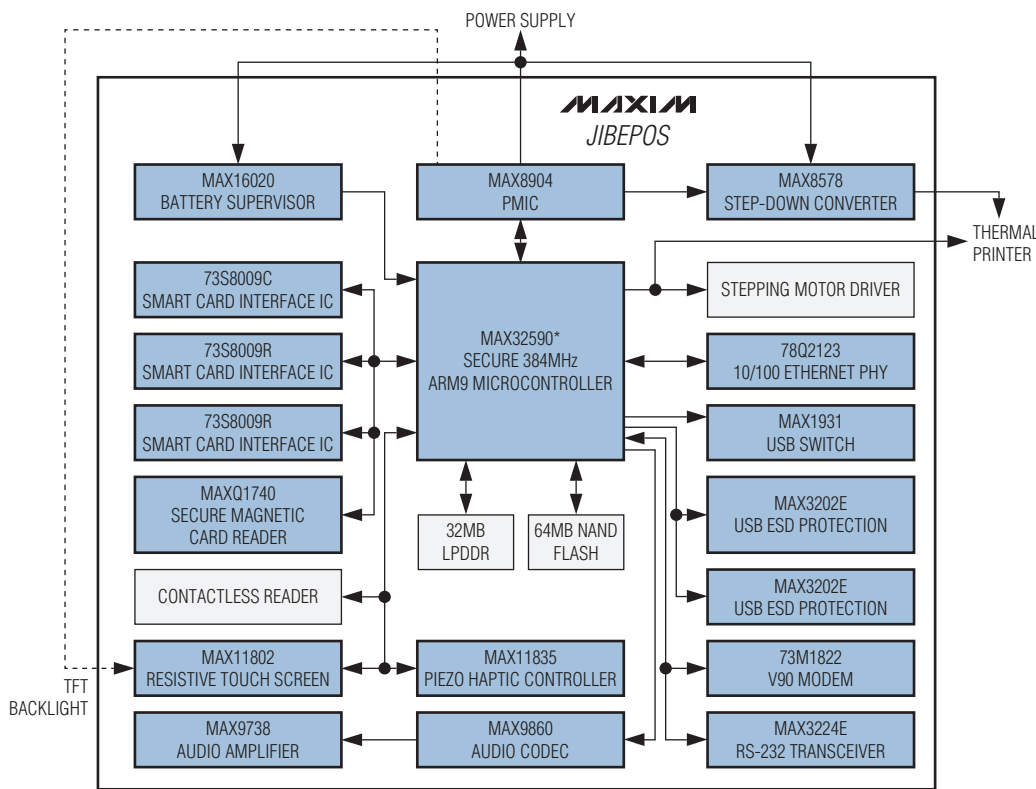
Your PCI PTS 3.1 Terminal...Now

JIBEPOS PCI PTS-Ready Reference Design Reduces Time to Market

Build your financial terminal with confidence that it will pass PCI evaluation.

Powered by the **MAX32590*** single-chip secure SoC μ C, the JIBEPOS reference design provides the fastest route to getting your terminal certified. Start with our meshless design, patented secure keypad layout, BOM-optimized hardware, SPA/DPA-resistant cryptographic library, certified EMV® L1 library, PCI PTS-compliant secure Linux OS, and a security handbook to adapt the design to your own enclosure.

- 3.5in TFT color display
- Haptic resistive touch screen
- Secure magnetic card reader
- Ethernet 10/100, V90 modem, USB
- NFC contactless reader
- Thermal printer
- On-board audio



Protect Magnetic Strip Data at the Source

End-to-End Encryption Made Easy

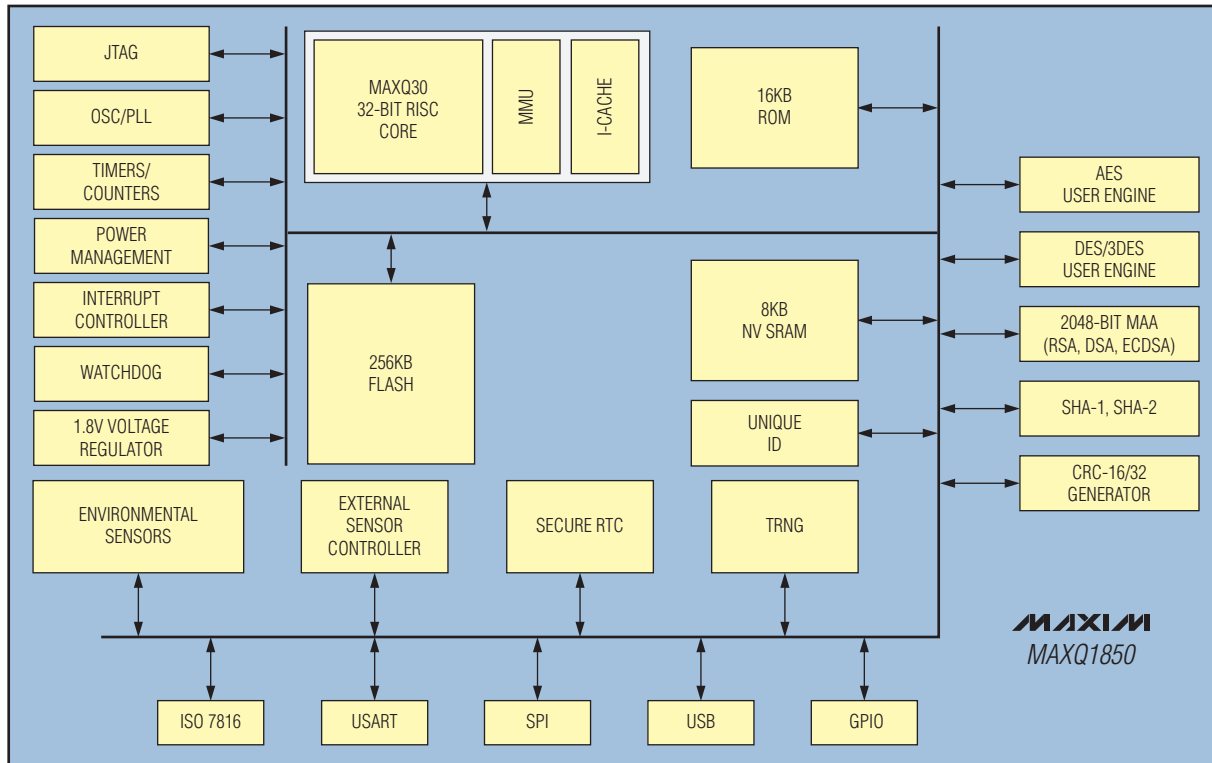
The **MAXQ1740** provides a high level of security for the magnetic stripe reader (MSR) by placing an ultra-secure μ C with high-speed hardware encryption inside the magnetic card reader head. Rather than transmitting sensitive data in cleartext, the **MAXQ1740** automatically encrypts the data at the swipe. Furthermore, the device provides a convenient, secure, nonvolatile storage space for storing various security keys that is protected against physical tampering.



*Future product—contact the factory for availability.

One-Chip PIN Pad Solution

The MAXQ1850 secure SoC features a single-cycle 16-/32-bit RISC processor and hardware-accelerated symmetric and asymmetric encryption engines, as well as extensive communication interfaces including ISO 7816, USB, and SPI. It has the flexibility to be a stand-alone controller for any PIN pad application or a coprocessor for other secure applications. System cost is optimized with integrated active tamper sensors. These sensors detect and react to attacks by erasing the 8KB of internal, secure battery-backed NV SRAM.



Security Features

- Hardware crypto engines for AES, 3DES, RSA, DSA, ECDSA, SHA-1, SHA-224, and SHA-256
- True random-number generator (TRNG)
- Multiple self-destruct inputs and environmental sensors
- 8KB of zeroizing NV SRAM (130nA leakage)
- Built-in voltage regulator for single power-supply operation

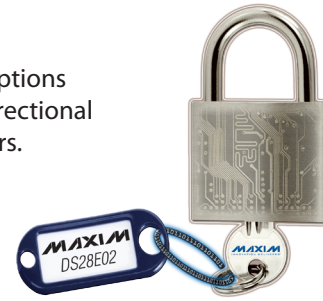
High-Performance μ C

- 16-/32-bit, single-cycle RISC core
- Internal 256KB of flash memory
- USB interface, ISO 7816 controller, RTC, USART, and SPI bus
- 6mm x 6mm, 40-pin TQFN or 7mm x 7mm, 49-pin CSBGA

Stop Counterfeiters and IP Theft

Protect your R&D investment with a proven, low-cost* authentication solution. Options range from secure, crypto-strong, FIPS 180-3-based challenge-and-response bidirectional authentication to customization of the 64-bit, factory-programmed serial numbers.

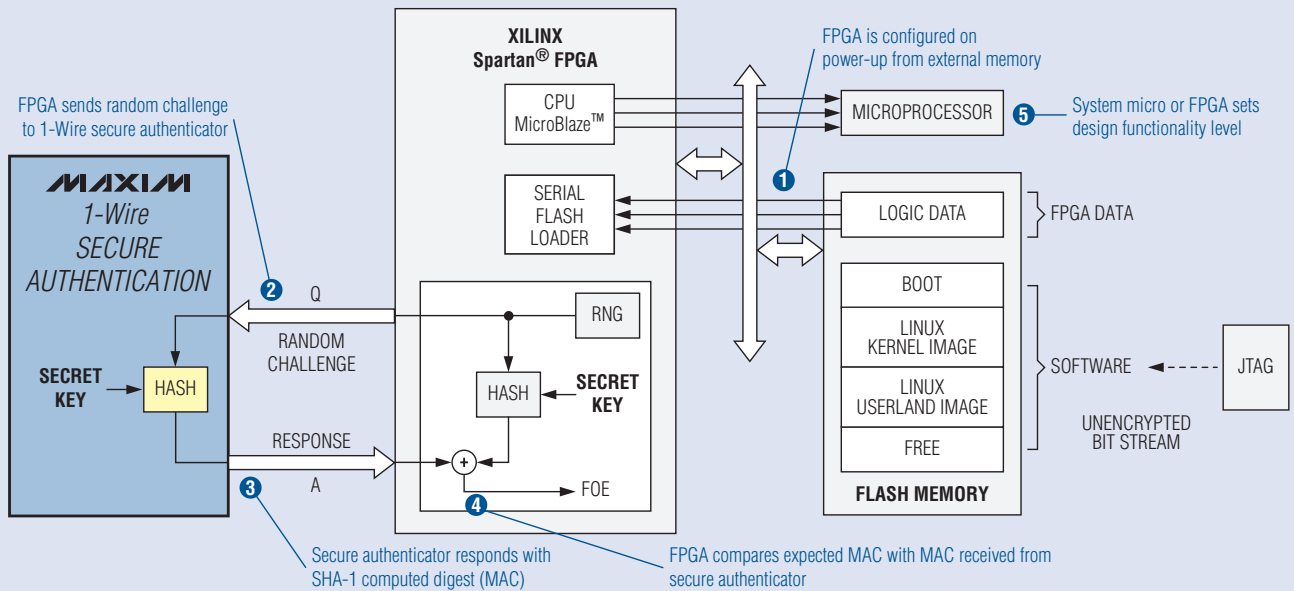
- OEM authentication
- System copy protection
- HW/SW license management
- Tamper-proof feature settings
- Safety/quality assurance



Part	Description	Host Interface	Authentication Feature
DS28CN01	SHA-1 with 1Kb EEPROM	I ² C/SMBus	Bidirectional challenge and response
DS28E01-100, DS28E02	SHA-1 with 1Kb EEPROM	1-Wire [®]	Bidirectional challenge and response
DS28E10	SHA-1 with 224b OTP EPROM	1-Wire	Challenge and response
DS2460	SHA-1 coprocessor	I ² C	Secure storage of system secret
DS28E25**	SHA-256 with 4Kb EEPROM	1-Wire	Bidirectional challenge and response
DS2465**	SHA-256 coprocessor with 1-Wire master	I ² C	Secure storage of system secret
DS2431	1Kb EEPROM	1-Wire	Customized 64-bit ROM, WP/OTP modes
DS2401, DS2411	64-bit ROM serial number	1-Wire	Customized 64-bit ROM
MAX66040, MAX66140	SHA-1 with 1Kb EEPROM	RF	Bidirectional challenge and response, ISO 14443B/15693

Secure FPGA Designs with One Pin

- Protects the FPGA designer's IP
- Low-cost alternative to expensive encrypted FPGAs
- 1-Wire interface requires only one FPGA pin to operate
- Data and power are multiplexed on the same pin
- FPGA SHA-1 engine and 1-Wire interface supported by major FPGA vendors
- For an FPGA protection tutorial, go to: www.maxim-ic.com/FPGA



www.maxim-ic.com/protect

*Authentication solutions starting as low as US \$0.15 for consumer electronics volumes. Prices provided are for design guidance and are FOB USA. International prices differ due to local duties, taxes, and exchange rates. Not all packages are offered in 1k increments, and some may require minimum order quantities.

**Future product—contact the factory for availability.

Keep Your Secrets Secure, Forever

Hardware AES Encryption with Anti-Tamper and Nonimprinting Memory Provides Highest Level of Security

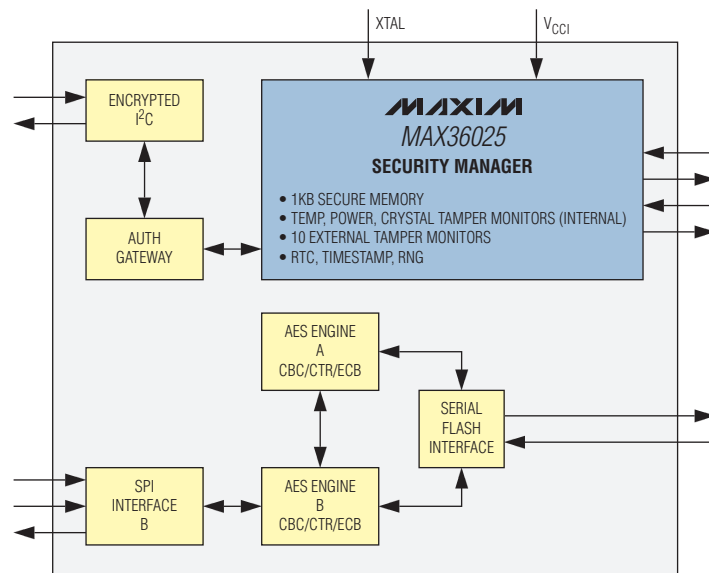
The MAX36025* security manager has hardware encryption and the most anti-tamper features offered in the market. As opposed to software encryption, on-chip hardware encryption and security provide the most secure method to encrypt/decrypt data and protect critical data (like encryption keys). The keys never leave the MAX36025 and are kept more secure with the tamper-detection features.

General Features

- Dual AES processors
- Supports 128-, 192-, and 256-bit keys
- ECB, CTR, and CBC modes
- Authentication via an encrypted I²C interface
- Bidirectional SPI ports
 - Use the same key to encrypt/decrypt data

Security Features

- 1KB nonimprinting memory for encryption key storage
 - Segmented memory to store two encryption keys
- Temperature, power, and oscillator tamper monitors
- External user-definable tamper monitor circuitry



No code needed to communicate with MAX36025 AES engine after authentication

No resident software development required

Easily Add System Security with Security Managers

Maxim's extensive security manager product line allows users to add security to systems using their existing system microprocessor. The ICs have a proprietary "nonimprinting" memory that stores critical data, but immediately and completely erases this memory upon qualified tamper events. The security managers also provide continuous tamper detection, regardless of the power source.

- Work with your existing microprocessor
 - I²C or SPI interfaces available
- Internal secure memory
 - Nonimprinting memory
 - Densities from 64B to 4KB
- Internal tamper monitors
 - Temperature, including rate of change
 - Power
 - Oscillator
- Monitor external circuitry for tampers
- Real-time clock/counter
 - Tamper-event timestamping
- Small CSBGA footprint and package
- Low power consumption during battery backup
- Monitor main power
 - Automatically switch from main power to battery
- Provide power and erase an external SRAM

www.maxim-ic.com/securitymanagers

*Future product—contact factory for availability.

Secure Microcontrollers

Part	Speed and Core	Internal Flash/SRAM Memory (KB)	Secure NV SRAM (KB)	External Memory	USB†	SPI	ISO 7816	GPIO	Battery Leakage (µA)	Package
MAXQ1004	6MHz, MAXQ20	16/640B	—	—	—	1	—	8	300nA	16-TQFN
MAXQ1010	12MHz, MAXQ20	128/2	128B	—	D	1	1	31	400nA	48-TQFN
MAXQ1011*, MAXQ1012*	12MHz, MAXQ20	64, 32/1	128B	—	D	1	1	31	400nA	48-TQFN
MAXQ1050	25MHz, MAXQ20	128/12	256B (secure) + 4KB (nonsecure)	—	D	1	1	20	240nA	40-TQFN
MAXQ1740	12MHz, MAXQ20	16/—	1152B	—	—	2	—	16	3	28-TQFN
MAXQ1850	16MHz, MAXQ30	256/—	8	—	D	1	1	16	130nA	40-TQFN, 49-CSBGA
USIP	96MHz, MIPS32® 4KSD™	256/128	512-bit	NOR flash, SRAM, SDRAM	O	1	3	32	2.9	256-CSBGA
ZA9L0	180MHz, ARM922T	—/64	4	NOR flash, SRAM, SDRAM	—	1	2	76	21	256-CSBGA
MAX32590*	384MHz, ARM926EJ-S	—/64	8 (secure) + 16 (nonsecure)	NOR flash, NAND SRAM, SDRAM LPDDR	D, H	5	2	160	10	324-LFBGA

†D = device port, O = OTG port, H = host port

Security Managers

Part	Temp Range (°C)	Power Consumption (typ) (µA)	Nonimprinting Memory (KB)	External Tamper Monitors	I/O	Authentication	AES Encryption ECB/CTR/CBC Modes	EV Kit	Package
DS3600, DS3605	-40 to +85	5.7	64B (DS3600)	4	3-wire/ I ² C	—	—	✓ (DS3600)	25-CSBGA
DS3640, DS3641	-40 to +85	6.5	1	4	4-wire/ I ² C	—	—	✓	25-CSBGA
DS3645	-55 to +95	12	4	8	I ² C	—	—	✓	49-CSBGA
DS3650, MAX36051	-40 to +85	3.0, 1.5	128B	2	4-wire	—	—	✓ (MAX36051)	16-CSBGA
MAX36025*	-55 to +95	9	1	8	SPI (2)	Encrypted I ² C	2 AES engines	✓	81-CSBGA

*Future product—contact factory for availability.

ARM9 and ARM926EJ-S are trademarks of ARM Limited.

EMV is a registered trademark of EMVCo LLC.

Linux is a registered trademark of Linus Torvalds.

MIPS32 is a registered trademark and 4KSD is a trademark of MIPS Technologies, Inc.

Spartan is a registered trademark and MicroBlaze is a trademark of Xilinx, Inc.

Maxim Integrated Products, Inc.
120 San Gabriel Drive
Sunnyvale, CA 94086
www.maxim-ic.com



For a complete list of Maxim's sales offices and franchised distributors, visit www.maxim-ic.com/sales.