Keywords: AES, authentication, physical tamper, FIPS, secure memory, hardware security, DeepCover

APPLICATION NOTE 5524

Securing Critical Data with Hardware AES Engines

Nov 28, 2012

Abstract: This application note describes how the MAX36025 DeepCover™ tamper-reactive cryptographic-node controller enables an effective physical tamper protection to help designers overcome security challenges in their current and next-generation systems.

A similar version of this article appeared on *Embedded*, October 24, 2012.

Security requirements are rapidly increasing across all end equipment categories. This trend, combined with the risk of software viruses, is resulting in an increased prevalence of hardware-security implementations. Designers thus face many security concerns in their current and next-generation systems, including how to securely encrypt data and protect encryption keys.

For any security solution to be effective, physical tamper protection must be implemented, because even the most sophisticated secure microprocessors, field-programmable gate arrays (FPGAs), smart cards, and other security components remain vulnerable to certain attack scenarios. This threat requires maintaining some active circuitry while the system is down to detect potential attacks that aim to extract critical information. To accomplish this, security devices must consume low power and interface with multiple sensors to detect threats. These devices also need to create a secure boundary around the circuitry that contains sensitive content. Additionally, if a security component can protect encryption keys as well as securely encrypt data, it can provide an even higher level of protection to the system and ease some of the concerns that designers currently face.

The MAX36025 DeepCover™ tamper-reactive cryptographic-node controller does just that. It stores encryption keys in a patented* non-imprinting memory (1KB), protects keys by monitoring for physical tampers, as well as encrypts and decrypts data in two hardware Advanced Encryption Standard (AES) engines. Taking the security attributes of existing Maxim security managers, which provide a secure memory to store critical information, the MAX36025 also has an authentication gateway to first authenticate any processor that tries to communicate with it by sending a challenge response. The authentication process takes place via an encrypted I2C interface when two known keys are successfully exchanged between the microprocessor and the device. The known keys are loaded in the MAX36025 in a secure location. If authentication does not successfully take place, the device will not allow access to the internal secure memory. Once authentication is successful, the encryption keys can be loaded in the non-imprinting secure memory. Additionally, access is given to set up the tamper parameters as well as data routing through the two AES engines.

The AES engines can operate in many scenarios (see **Figures 1** through **3**) to either encrypt, decrypt, or both encrypt and decrypt critical data at a throughput rate of 9Mbps. The AES engines are accessed via two separate bidirectional SPI interfaces. Additionally, a serial flash interface can store large amounts of encrypted data into an external serial flash. This allows users to store data securely in a standard serial flash.

The MAX36025 is a newly released security manager that enables an easier method of implementing AES encryption into a system. As a state machine-based device, the MAX36025 does not require a code** to communicate with it, thus reducing design time. The part is unique to the market as it combines hardware AES engines with a robust set of security features, including a patented non-imprinting memory.

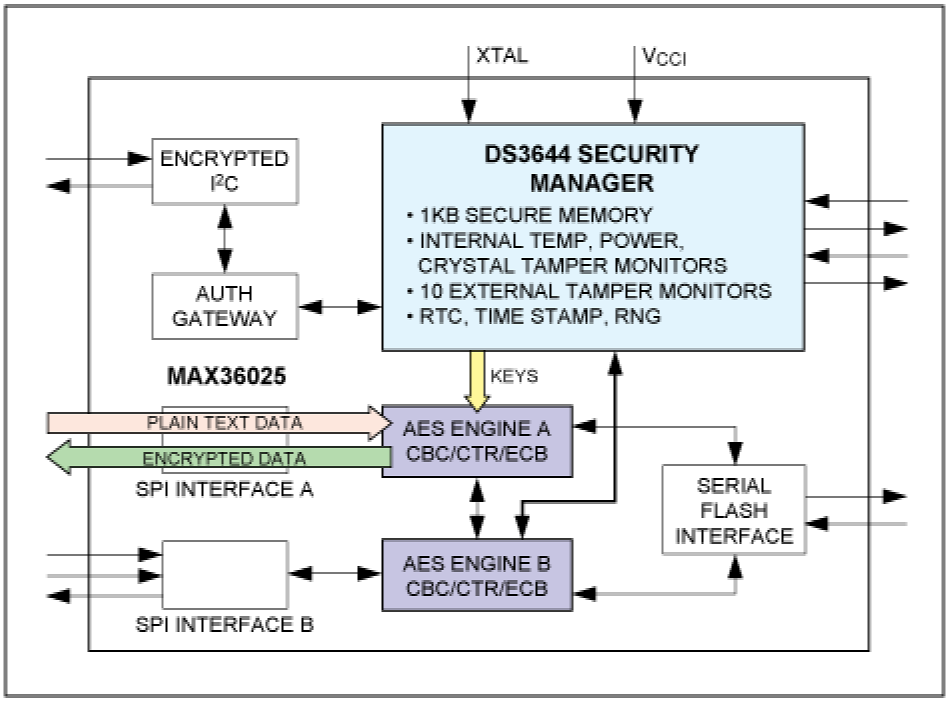

Figure 1. Using one AES engine to encrypt data.

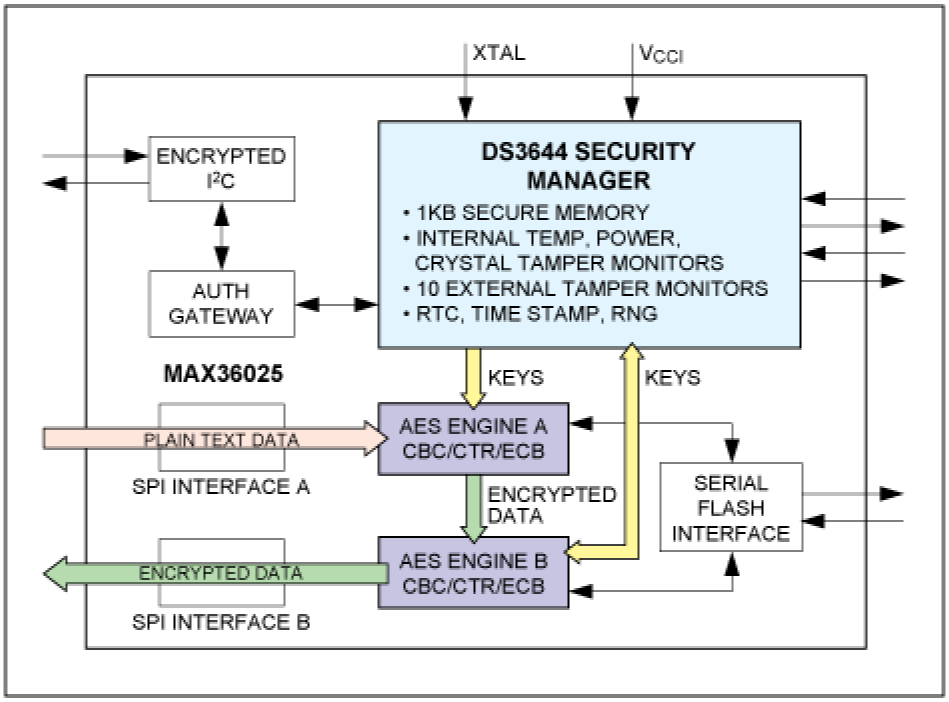

Figure 2. Using both AES engines to encrypt data.

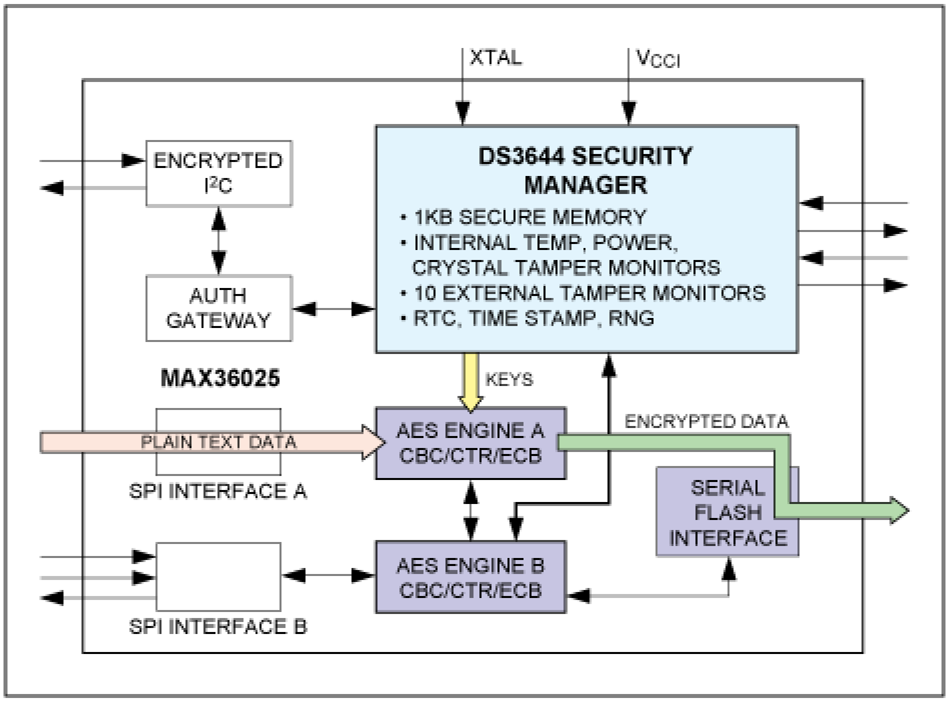

Figure 3. Storing encrypted data in an external serial flash.

**Patent #7,379,325.
**A small amount of code is required to complete the authentication process.

Related Parts		
DS3644	DeepCover Security Manager with 1KB Secure Memory and Programmable Tamper Hierarchy	Free Samples
MAX36025	DeepCover Security Manager for Tamper-Reactive Cryptographic-Node Control with AES Encryption and Nonimprinting Memory	

More Information
For Technical Support: http://www.maximintegrated.com/support
For Samples: http://www.maximintegrated.com/samples
Other Questions and Comments: http://www.maximintegrated.com/contact

Application Note 5524: http://www.maximintegrated.com/an5524
APPLICATION NOTE 5524, AN5524, AN 5524, APP5524, Appnote5524, Appnote 5524