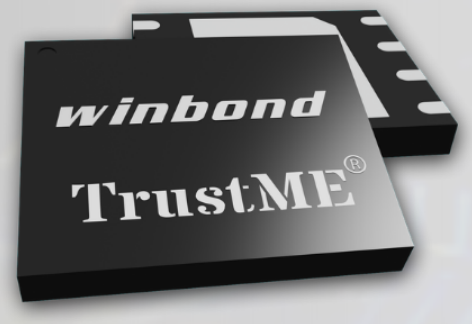
TrustME®
Secure Flash-W77Q

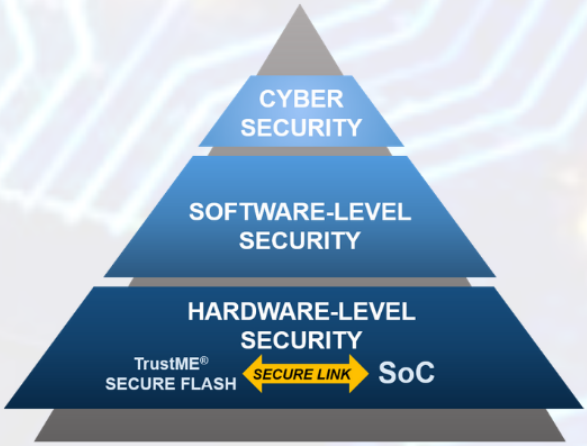


Revolutionized IoT security with a new drop-in replacement Secure Flash memory

Secure Flash Memory enabling trust and providing scalability.

Hardware security is the foundation of cyber security

Secure Storage is the core of hardware security



Serial SPI NOR Flash W77Q is based on the popular W25QJW family

- 100% Drop-in replacement for SPI Flash
- No need to redesign board or MCU

Advanced security features:

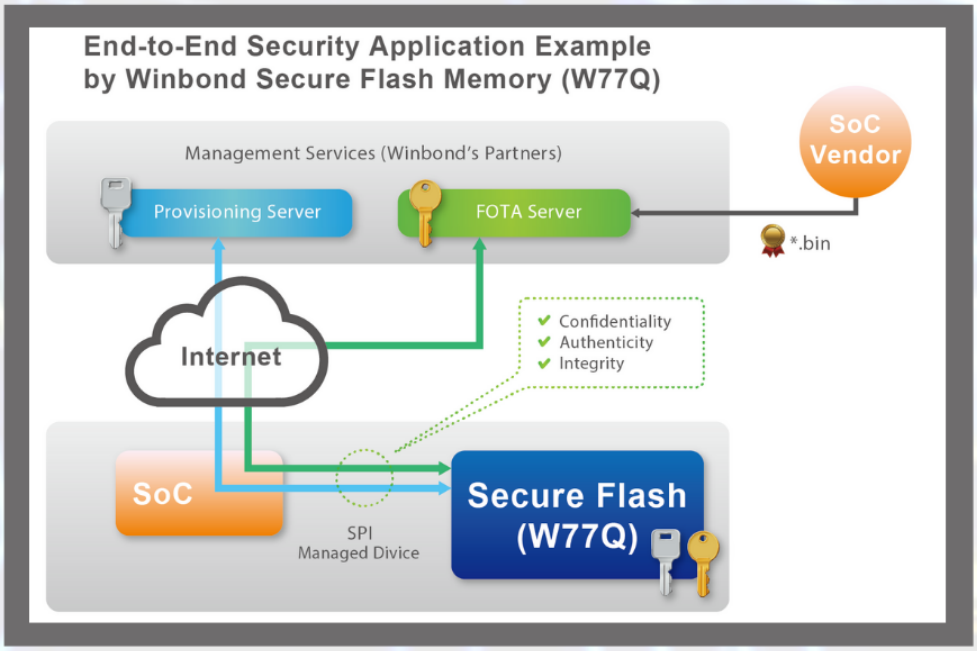
- Root of trust and secure boot
- Secure Over-The-Air firmware update
- Resilience: protection, detection and recovery
- Secure data storage

Certified secure memory = Trusted and Proven Solution!

- Security assessment by external lab
- CC EAL2 (in progress), SESIP(in progress)

Design is based on pure digital logic, no integrated MCU

Optimized for cost sensitive platforms



Comprehensive Security Functionality

The W77Q (32 Mbit) TrustME® Secure Serial Flash memory provides a secure storage solution for systems with limited space, pins and power, that meets Common Criteria EAL2 Security Certification requirements.

The W77Q is a drop-in replacement for standard Serial NOR Flash devices, offering security, flexibility, and performance well beyond ordinary NOR Flash devices. It is ideal for secure code storage with support for secure eXecute In Place (XIP), cryptographic key distribution, management and storage, secure data storage, and general data storage.

The W77Q features sophisticated cryptographic encryption of the communication channel, personalization of each device with unique keys, cryptographic read and write locks, protection of data integrity, secure over-the-air (OTA) firmware update, RoT functions, secure read, write and erase operations.

The W77Q series supports Single, Dual and Quad SPI as well as QPI modes of operation, running at up to 133 MHz. Dual Transfer Rate (DTR) is supported at rates up to 66 MHz.

Single Die Secure Solution

- Meets CC EAL2 Security Certification Requirements
- Secure Root of Trust (RoT) for IoT Devices
- Ultra Fast Secure Boot
- Secure Code and Data Storage
- Secure Code Update with Rollback Protection
- Secure Over-The-Air (OTA) Firmware Update
- Local and Remote Secure-Channel, Encrypted,
- Authenticated, Replay-Protected
- Firmware Integrity Protection
- On-chip Data Hash for Fast Code
- Authentication
- Platform Firmware Resiliency Assurance
- Authenticated Watchdog Timer
- Secure & Unique Device ID
- Cryptographically Secured Write Protection
- Secure Key Provisioning and Storage
- Replay Protection Monotonic Counter

Standard SPI-Flash Drop-In Replacement

Highest Performance Secure Serial Flash

- Execute In Place (XIP)
- 133 MHz SPI Single/Dual/Quad/QPI
- 66 MHz Dual Transfer Rate (DTR) Mode
- Over 100,000 Erase/Program Cycles Per Block
- More than 20-year data retention

Read and Write Access Control

Continuous Read and Burst Read with Wrap

Flexible Architecture with 4kB Blocks

- Uniform 4K-Bytes Block Erase
- Page Program up to 256 Bytes Per Command
- Erase/Program Suspend & Resume

Low Power, Single 1.8V Supply

Wide Temperature Range

- -40°C to +105°C (Industrial Plus)

Offered as Known Good Die (KGD) Wafers and Variety of Space-Saving Packages: 8-pin SOP, 8-pad WSON, 16-pin SOP, 24-ball TFBGA

Version: Aug.2020

Website: www.winbond.com | Email: TrustME@winbond.com

winbond