Micron Authenta™ Flash Memory

Authenticated Core Root of Trust for Measurement (A-CRTM) Rev. 1.6 Feature Set and Replay Protected Monotonic Counter (RPMC) Security Addendum - BRIEF
MT25Q Devices

Introduction

This brief version of the Authenta™ addendum provides an introductory information on Micron Authenta flash device.

This addendum does not provide detailed device information. The standard device data sheet provides a complete description of device functionality, operating modes, and specifications unless specified herein.

This document does not provide detailed information on Authenta security features: replay protected monotonic counter (RPMC) and authenticated core root of trust for measurement (A-CRTM), the full Authenta addendum (available under NDA) provides a complete description of those security features.

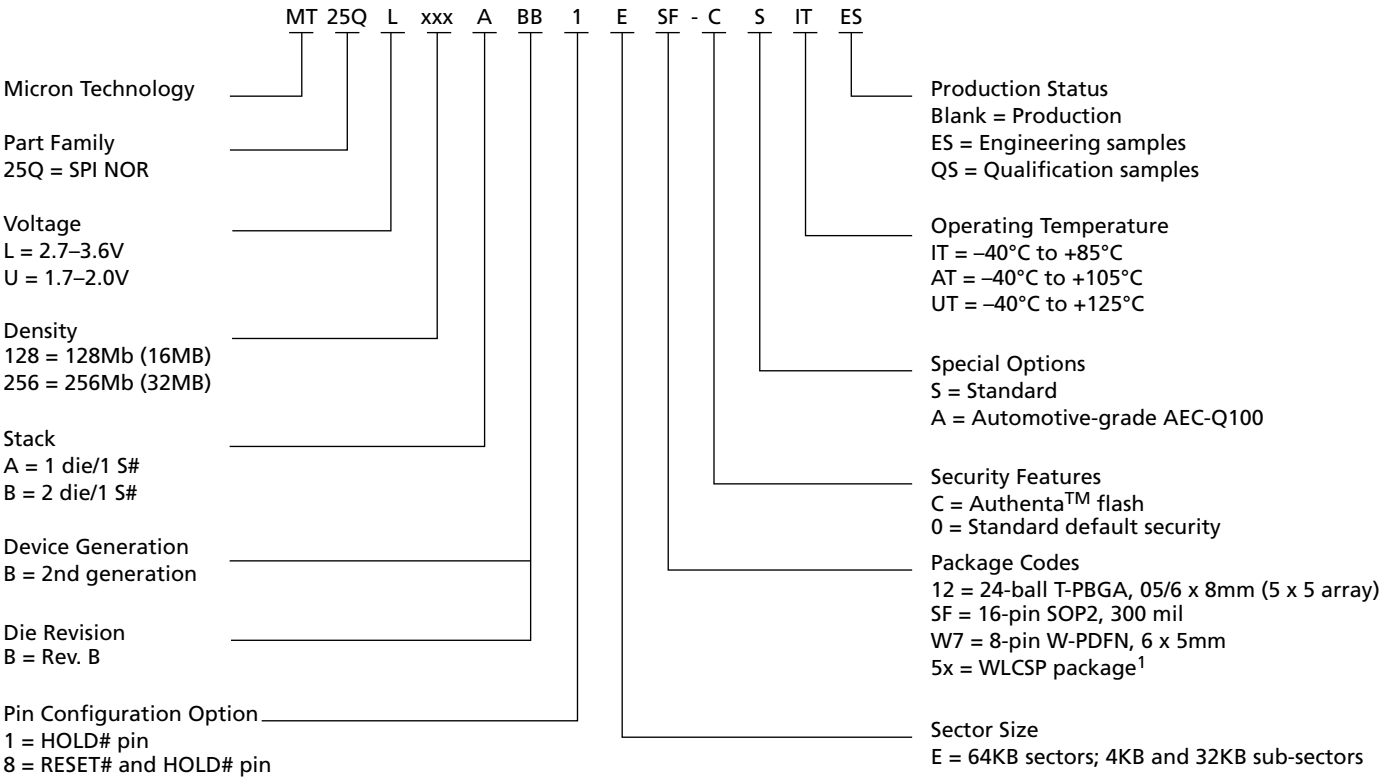
Features

- SPI-compatible serial bus interface
- Single and double transfer rate (STR/DTR)
- Clock frequency
  - 133 MHz (MAX) for all protocols in STR (3.0V)
  - 166 MHz (MAX) for all protocols in STR (1.8V)
  - 90 MHz (MAX) for all protocols in DTR
- Dual/quad I/O commands for increased throughput up to 90 MB/s
- Supported protocols in both STR and DTR
  - Extended I/O protocol
  - Dual I/O protocol
  - Quad I/O protocol
- Execute-in-place (XIP)
- PROGRAM/ERASE SUSPEND operations
- Volatile and nonvolatile configuration settings
- Software reset
- Additional reset pin for selected part numbers
- Dedicated 64-byte OTP area outside main memory
  - Readable and user-lockable
  - Permanent lock with PROGRAM OTP command
- Erase capability
  - Bulk erase
  - Sector erase 64KB uniform granularity
  - Subsector erase 4KB, 32KB granularity
- MT25Q basic security features available
  - Volatile and nonvolatile locking and software write protection for each 64KB sector
  - Nonvolatile configuration locking
  - Password protection
  - Hardware write protection: nonvolatile bits (BP[3:0] and TB) define protected area size
  - Program/erase protection during power-up
- Advanced security features available
  - Replay protected monotonic counter (RPMC)
  - Advanced cryptographic security based on 256-bit HMAC, including:
    A-CRTM feature set
    Local and remote provision/deprovision
    One set of nonvolatile, programmable CRTM pointers
    Cryptographically secured flash digest and block locking
    Programmable automatic measurement and recovery
    Server root key that can be updated
- Electronic signature
  - JEDEC-standard 3-byte signature
  - Extended device ID: two additional bytes identify device factory options
- JESD47H-compliant
  - Minimum 100,000 ERASE cycles per sector
  - Data retention: 20 years (TYP)
- Packages: JEDEC-standard, RoHS-compliant

Part Number Ordering

Micron Serial NOR Flash devices are available in different configurations and densities. Verify valid part numbers by using Micron's part catalog search at www.micron.com. To compare features and specifications by device type, visit www.micron.com/products. Contact the factory for devices not found.

Figure 1: Part Number Ordering Information



Note: 1. WLCSP package codes, package size, and availability, are density-specific. Contact the factory for availability.

Important Notes and Warnings

Micron Technology, Inc. ("Micron") reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions. This document supersedes and replaces all information supplied prior to the publication hereof. You may not rely on any information set forth in this document if you obtain the product described herein from any unauthorized distributor or other source not authorized by Micron.

Automotive Applications. Products are not designed or intended for use in automotive applications unless specifically designated by Micron as automotive-grade by their respective data sheets. Distributor and customer/distributor shall assume the sole risk and liability for and shall indemnify and hold Micron harmless against all claims, costs, damages, and expenses and reasonable attorneys' fees arising out of, directly or indirectly, any claim of product liability, personal injury, death, or property damage resulting directly or indirectly from any use of non-automotive-grade products in automotive applications. Customer/distributor shall ensure that the terms and conditions of sale between customer/distributor and any customer of distributor/customer (1) state that Micron products are not designed or intended for use in automotive applications unless specifically designated by Micron as automotive-grade by their respective data sheets and (2) require such customer of distributor/customer to indemnify and hold Micron harmless against all claims, costs, damages, and expenses and reasonable attorneys' fees arising out of, directly or indirectly, any claim of product liability, personal injury, death, or property damage resulting from any use of non-automotive-grade products in automotive applications.

Critical Applications. Products are not authorized for use in applications in which failure of the Micron component could result, directly or indirectly in death, personal injury, or severe property or environmental damage ("Critical Applications"). Customer must protect against death, personal injury, and severe property and environmental damage by incorporating safety design measures into customer's applications to ensure that failure of the Micron component will not result in such harms. Should customer or distributor purchase, use, or sell any Micron component for any critical application, customer and distributor shall indemnify and hold harmless Micron and its subsidiaries, subcontractors, and affiliates and the directors, officers, and employees of each against all claims, costs, damages, and expenses and reasonable attorneys' fees arising out of, directly or indirectly, any claim of product liability, personal injury, or death arising in any way out of such critical application, whether or not Micron or its subsidiaries, subcontractors, or affiliates were negligent in the design, manufacture, or warning of the Micron product.

Customer Responsibility. Customers are responsible for the design, manufacture, and operation of their systems, applications, and products using Micron products. ALL SEMICONDUCTOR PRODUCTS HAVE INHERENT FAILURE RATES AND LIMITED USEFUL LIVES. IT IS THE CUSTOMER'S SOLE RESPONSIBILITY TO DETERMINE WHETHER THE MICRON PRODUCT IS SUITABLE AND FIT FOR THE CUSTOMER'S SYSTEM, APPLICATION, OR PRODUCT. Customers must ensure that adequate design, manufacturing, and operating safeguards are included in customer's applications and products to eliminate the risk that personal injury, death, or severe property or environmental damages will result from failure of any semiconductor component.

Limited Warranty. In no event shall Micron be liable for any indirect, incidental, punitive, special or consequential damages (including without limitation lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort, warranty, breach of contract or other legal theory, unless explicitly stated in a written agreement executed by Micron's duly authorized representative.

Device ID Data

The device ID data is read by the READ ID and MULTIPLE I/O READ ID operations.

In the following table is displayed the device ID data for Authenta flash devices. Please note that device ID data for Authenta flash devices is different from the device ID data of standard (that is, nonAuthenta) flash devices.

Table 1: Device ID Data

Byte #	Name	Content Value	Assigned By
Manufacturer ID (1 byte total)			
1	Manufacturer ID (1 byte)	20h	JEDEC
Device ID (2 bytes total)			
2	Memory type (1 byte)	BAh = 3V	Manufacturer
		BBh = 1.8V	
3	Memory capacity (1 byte)	18h = 128Mb	
		19h = 256Mb	
Unique ID (19 bytes total)			
4	Number of remaining ID bytes (1 byte)	12h	Factory
5	Extended device ID (1 byte)	See table below	
6	Device configuration information (1 byte)	8Ch = RPMC and A-CRTM	
7:22	Customized factory data (16 bytes)	Unique ID code (UID)	

Table 2: Extended Device ID Data, First Byte

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2[1]	Bit 1	Bit 0
Reserved	Device Generation 1 = 2nd generation	Reserved	Reserved	HOLD#/RESET#: 0 = HOLD 1 = RESET	Additional HW RESET#: 1 = Available 0 = Not available	Sector size: 00 = Uniform 64KB	

Notes: 1. Available for specific part numbers. See Part Number Ordering Information for details.

Replay Protected Monotonic Counter (RPMC)

RPMC is a flash device security feature that enables a secure system boot plus enhanced platform security.

The RPMC feature is enabled on Micron Authenta flash devices. However, if the user does not want to make use of RPMC, the following Opcode/Sub-Opcode combinations should not be sent to the memory interface; this will prevent unintentionally activating any RPMC-related functionality. The full Authenta addendum (available under NDA) provides a complete description about RPMC usage.

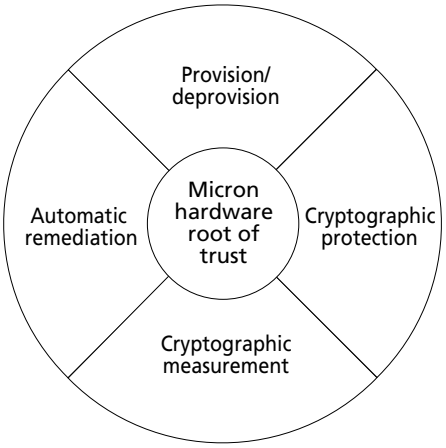
Table 3: RPMC Command Set

Opcode	Sub-Opcode
9Bh	00h
9Bh	01h
9Bh	02h
9Bh	03h

Authenticated Core Root of Trust for Measurement (A-CRTM)

The MT25Q A-CRTM feature set consists of four capabilities: provision/deprovision, cryptographic protection, cryptographic measurement and automatic remediation.

Figure 2: A-CRTM Capabilities



As default condition, the A-CRTM security features are not enabled on Micron Authenta flash devices, and the memory will behave like a standard device. If the user does not want to make use of A-CRTM functionality, the following Opcode/Sub-Opcode combinations should not be sent to the memory interface; this will prevent unintentionally activating any A-CRTM-related functionality.

The full Authenta addendum (available under NDA) provides a complete description about A-CRTM usage.

Table 4: A-CRTM Command Set

Opcode	Sub-Opcode
9Bh	34h
9Bh	35h
9Bh	36h
9Bh	37h
9Bh	38h
9Bh	39h
9Bh	3Ah
9Bh	3Bh
9Bh	3Ch
9Bh	3Dh
9Bh	3Eh
9Bh	3Fh

Serial Flash Discovery Parameter Data

The serial flash discovery parameter (SFDP) provides a standard, consistent method to describe serial flash device functions and features using internal parameter tables. The parameter tables can be interrogated by host system software, enabling adjustments to accommodate divergent features from multiple vendors. The SFDP standard defines a common parameter table that describes important device characteristics and serial access methods used to read the parameter table data. Data in the SFDP tables is read by the READ SERIAL FLASH DISCOVERY PARAMETER operation.

Micron's SFDP table information for MT25Q family aligns with JEDEC-standard JESD216 for serial flash discoverable parameters. Refer to JEDEC standard JESD216B for a complete overview of the SFDP table definition.

See Micron's technical note, TN-25-06: Serial Flash Discovery Parameters for MT25Q Family, for more information on the standard features of the MT25Q family of devices. For the RPMC- and Authenta-specific features, refer to the following table.

Table 5: Authenta Additions to SFDP Table

Description	Byte Address	Value	Notes
SFDP revision (MIN/MAX)	04h	06h	JEDEC has specified revision as 1.6
	05h	01h	
Number of parameter headers	06h	03h	Four parameter headers
Monotonic counters parameter headers	18h	03h	03h: Even parity value for a function-specific table: RPMC
	19h	00h	Intel has defined this function-specific table revision as 1.0
	1Ah	01h	
	1Bh	02h	RPMC-specific table length is two DWORDs
	1Ch	00h	24-bit address; RPMC-specific table starts at location 100h
	1Dh	01h	
	1Eh	00h	
	1Fh	FFh	FFh through 80h are defined by the JEDEC 42.4 committee
Secure packet read and secure packet write parameter headers	20h	8Eh	Parameter 4 ID LSB = 0Fh: secure read/write
	21h	00h	JEDEC defined this function-specific table revision as 1.0
	22h	01h	
	23h	04h	Secure read/write table length is four DWORDs
	24h	20h	24-bit address; security-specific table starts at location 120h
	25h	01h	
	26h	00h	
	27h	FFh	FFh through 80h are defined by the JEDEC 42.4 committee

Table 5: Authenta Additions to SFDP Table (Continued)

Description	Byte Address	Value	Notes
Monotonic counter features	100h	3Ch	Flash hardening supported; MTC size: 32 bits; busy polling method: READ SR; number of counters: 4
	101h	9Bh	Opcode 1 (secure write opcode)
	102h	96h	Opcode 2 (secure read opcode)
	103h	F0h	Update rate: 5s
Monotonic counter delay parameters	104h	E6h	Polling delay read counter: 6ms
	105h	E3h	Write counter polling short delay: 3ms
	106h	C2h	Write counter polling long delay: 256ms
	107h	FFh	Reserved
Secure packet read/write parameters	120h	00h	00h = proprietary; secure read/write table
	121h	FFh	Reserved
	122h	FFh	Reserved
	123h	00h	0-byte Command Modifier field; 64-byte buffer; same latency for secure read as for fast read
x1 and x2 SDR secure packet opcodes	124h	9Bh	x2 SDR secure write
	125h	96h	x2 SDR secure read
	126h	9Bh	x1 SDR secure write
	127h	96h	x1 SDR secure read
x4 and x8 SDR secure packet opcodes	128h	00h	x8 SDR secure write (not supported)
	129h	00h	x8 SDR secure read (not supported)
	12Ah	9Bh	x4 SDR secure write
	12Bh	96h	x4 SDR secure read
x4 and x8 DDR secure packet opcodes	12Ch	00h	x8 DDR secure write (not supported)
	12Dh	00h	x8 DDR secure read (not supported)
	12Eh	9Bh	x4 DDR secure write
	12Fh	96h	x4 DDR secure read

Notes: 1. Addresses from 108h to 11Fh are filled with FFh.
2. Addresses from 20h to 27h and from 120h to 12Fh are under discussion by the JEDEC committee (subject to change).

Revision History

Rev. A – 4/2022

- Initial release

8000 S. Federal Way, P.O. Box 6, Boise, ID 83707-0006
208-368-4000, micron.com/support

This data sheet contains initial characterization limits that are subject to change upon full characterization of production devices.