SECURITY FEATURES THE IMPORTANT STUFF.

One-Time-Programmable (OTP) Segment

Configuration Script controls settings

- Dev/Prod Modes
- Secure Boot

Encryption Keys Provisioned here:

- QSPI FW Keys - on-the-fly fw decryption
- User Data Keys - application keys
- Public Keys - secure boot authentication

Segment	Bytes	Description	OTP Address
1	1024	**Configuration Script** ~100 registers write operations	0x00000C00
2	256	**QSPI FW Decryption Keys Area – Payload** write/read protected when secure mode enabled in CS Secure mode connects those (8 * 256-bits) keys to QSPI Controller	0x00000B00
3	256	**User Data Encryption Keys – Payload** Write/Read protected when secure mode enabled in CS. Secure mode connects those (8 * 256-bits) keys to AES engine	0x00000A00
4	32	**QSPI FW Decryption Keys Area – Index** Eight entries for eight 256-bit keys	0x000009E0
5	32	User Data Encryption Keys – Index 8 entries for 8 256-bit keys	0x000009C0
6	256	Signature Keys Area – Payload	0x000008C0
7	32	Signature Keys Area – Index	0x000008A0
8	2208	Customer Application Area (Secondary bootloader, binaries, and so on)	0x00000000

Bit field	Description
FORCE_DEBUGGER_OFF	This bit will permanently disable the M33 debugger
FORCE_CMAC_DEBUGGER_OFF	This bit will permanently disable the CMAC debugger
PROT_QSPI_KEY_READ	This bit will permanently disable CPU read capability at OTP offset 0x00000B00 and for the complete segment
PROT_QSPI_KEY_WRITE	This bit will permanently disable ANY write capability at OTP offset 0x00000B00 and for the complete segment
PROT_AES_KEY_READ	This bit will permanently disable CPU read capability at OTP offset 0x00000A00 and for the complete segment. The AES sections are only used by the application SW, but protecting the key area from read/write makes it secure after leaving the manufacturing facilities
PROT_AES_KEY_WRITE	This bit will permanently disable ANY write capability at OTP offset 0x00000A00 and for the complete segment. The AES sections are only used by the application SW, but protecting the key area from read/write makes it secure after leaving the manufacturing facilities
PROT_SIG_KEY_WRITE	This bit will permanently disable ANY write capability at OTP offset 0x000008C0 and for the complete segment. This is for protecting public keys from being written (used by ECC only)
SECURE_BOOT	This bit will enable authentication of the image in the FLASH while the system is booting

ENCRYPTION AT REST 

Defensible external storage of user applications? Encryption!

- Keys loaded into OTP (QSPI Area)
- Application encrypted with provisioned key
- HW Engine decrypts application as its executed
- AES-CTR Mode
  - Allows decryption of arbitrary blocks
    - Performance / Execute-In-Place (XIP)