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)**

SECURE BOOT

Validates the application against public key stored in OTP

Once activated the following is enforced:

- Cannot be disabled
- Applications must be signed
- Applications must be encrypted
- OTP Key section read disabled
    - Keys can be revoked