

Features

32-bit ARM Cortex-M3 Core

- Nested Vectored Interrupt Controller(NVIC):
1 Wake up and 1 peripheral interrupt
- 16-bit or 32-bit System timer (Sys Tick):
System timer for OS task management
- Creation and Management of Cipher Key

On-chip Memory

- EEPROM
 - 128 KB
 - Configuration/Key/User data storage
 - 15 User Zones of 2 Kbits Each
 - Retention 10 years
 - Erase/Write Endurance: 100K
- SRAM
 - On chip 32 Kbytes

Serial Interface

- UART
 - Full duplex double buffer
 - Parity can be enabled or disabled
 - Built-in dedicated baud rate generator
 - Various error detection functions (parity error, framing errors, and overrun errors)
 - External x-tal for UART
- SPI0, SPI2
 - Slave, Mode 0
 - Up to 40 MHz SCK
 - Symmetric cipher core control
- SPI1
 - Master/Slave
 - Master: Up to 10 MHz SCK
 - Slave: Up to 1.5 MHz SCK
 - Mode 0, 1, 2, 3
- GPIO
 - 4 GPIOs

Clock, Reset and Voltage

- Clock
 - Built in OSC.
 - Main Clock: 50 fMHz
- Reset
 - Built in power on reset
 - Software reset
- 1.5V, 3.3V Supply Voltage

Debug

- Serial Wire Debug Port(SW-DP)

Low Power Consumption Mode

- The GPIO is sufficient to power up and down
- PMU clock gating of Cortex-M3

Asymmetric cipher function

- ECC-P256, RSA-4096
- ECDSA, ECDH

Symmetric cipher function

- AES-128/256, ARIA-128/256
- Modes of Operation: Confidentiality (ECB, CBC, CFB, OFB, CTR)
- Creation and Management of Cipher Key

Crypto Device function

- User ID, User Serial (Manufacture ID), MIDR, RVC
- PUF
- Generate random using two different phase counters

Application

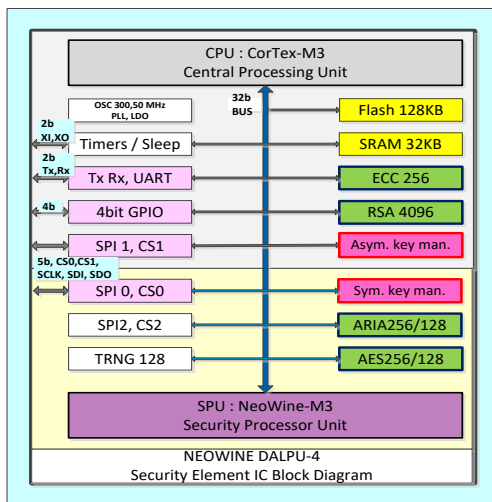
- Print cartridge, GPS, Navigation
- Mobile Device, IPC, CCTV, DVD
- Set-Top Boxes (STBs), Etc.

Standards

- ECC, RSA FIPS 186-3, 186-4
- AES-128/256 FIPS 140-2
- TRNG NIST SP 800-90B compatibility

Benefits

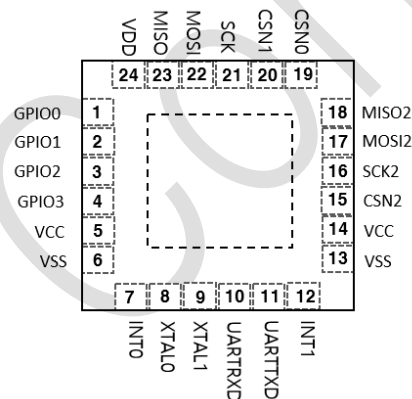
- Read/Write, Encrypted, or Read-only User Zone Options
- Ease use of Crypto Device to replace of existing EEPROM devices
- Authenticate Consumer products, Components, and Network equipment
- Protect Sensitive Firmware
- Securely Store Sensitive Data
- Manage Warranty Claims
- Securely Store Identity Data



Block Diagram

Package

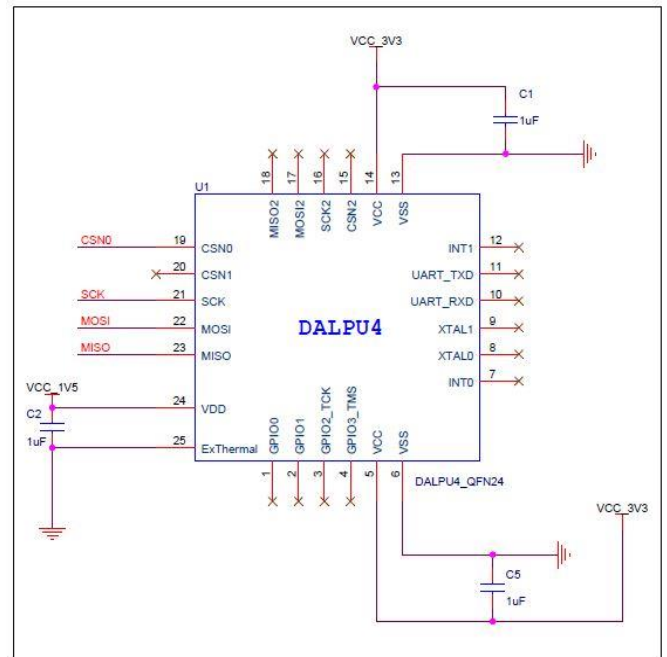
- QFN 4x4-25L (4mm X 4mm X 0.75mm)



Top view

Schematic Diagram

- Application Circuit



- DALPU-4 Power Circuit

