MS1000

32 bit Microcontroller with Embedded Security Engine for IoT

Complete Root-of-Trust, Dedicated Crypto Engine & Certification Authority

Product Brochure — Feburary 2016

Introduction

The MS1000 is an ARM® Cortex-M3™ based microcontroller with security engine for embedded applications featuring a high level of integration and low-power consumption.

The MS1000 operates at CPU frequencies up to 100 MHz. The ARM Cortex-M3 CPU includes a built-in Wakeup Interrupt Controller (WIC) and Nested Vectored Interrupt Controller (NVIC) with an integrated System Tick (SysTIck).

The MS1000 features a security engine called tRoot Suite. The tRoot Suite consists of tRoot, SPAcc, and TRNG. It protects the device and its data at boot time, run time and during the communication with other devices or with the cloud.

The peripheral complement of the MS1000 includes up to 192 KB of internal SRAM, 8 KB One-Time Programmable (OTP) memory for bootloader, key storage, External Memory Interface, 4 SPI interface controllers, 2 DMA controllers, 2 Advanced Timers supporting PWM, 2 General Purpose Timer, a Real-Time Clock (RTC) domain consisting of the RTC and a back-up SRAM, Windowed Watchdog Timer, SDMMC interface, 4 UARTs, 4 I2C, and up to 80 fast general purpose I/O pins.

With its low-power, high performance, diverse connectivity options, and security features, the MS1000 is ideal for IoT applications such as Smart home applications, Smart metering, Tele-monitoring, and Remote Healthcare.

Key Features

32-bit ARM® Cortex™-M3 CPU

- Up to 100 MHz operation frequency
- Built-in Nested vectored interrupt controller (NVIC) for fast deterministic interrupt processing
- Wake-up Interrupt Controller (WIC) allows automatic wake from any priority interrupt
- 3 Low-power modes (Sleep/Deep-sleep/Standby)

Memories

- 192 KB SRAM
- 8 KB OTP Memory

Security Engine

- **tRoot (Secure Hardware Root of Trust)**
  - Secure Boot
    - Primary security capability of tRoot which is used to brings up a device into a secure state and ensure that it runs only trusted firmware
  - Secure identification and authentication
    - Ensures the integrity of various authentication protocols as well as ensure the confidentiality of shared secrets between devices
  - Secure provisioning, storage, and management of keys and other secrets
    - HW protected Device Unique Key and Platform Key — not accessible by SW
- **SPAcc (Security Protocol Accelerator)**
  - Supporting for all ciphers, hashes and MAC algorithms used in major security protocols
    - MACsec, IPsec, SSL/TLS/DTLS, SRTP, WiMAX, WiFi, content protection, and 3GPP/LTE/LTE-A
  - Built-in scatter/gather DMA capability offloads system CPU
  - Secure key port to access secrets stored in tRoot
- **TRNG (Smart True Random Number Generator)**
  - Designed for compliance with FIPS 140-2 and FIPS 140-3 (draft)
  - High speed operation
    - 50 Mbps at 200 MHz
  - Shift register compatible output stream for direct access by tRoot
    - Differential Power Analysis
    - Timing Analysis

Power Management

- PLL for high frequency clock generation

- Low Dropout (LDO) regulator for main/battery supply
- Power-on Reset
- Built-in Brown-out detection (BOD) circuit for monitoring 3 supply voltage levels

Peripherals

- External Memory Interface for Async/Sync/Muxed SRAM, NOR (8-bit/16-bit)
- Two 2-channel Direct Memory Access (DMA) controllers
- Two 4-channel Advanced Timers for supporting PWM
- 8-channel 1MSPS SAR A/D Converter (ADC)
- Two 2-channel General Purpose Timers
- Real-Time Clock operating at battery domain
- 16-bit Programmable Windowed Watchdog Timer
- SDMMC supporting eMMC 4.41 & SD 3.01
- Four UARTs with S protocol ENDEC
- Four 16-bit Serial Peripheral Interfaces (SPI)
- Four I2C modules
- Up to 16 GPIO pins under control
- Internal RC Oscillator

MISC Features

- Peripheral Coprocessor for autonomous peripheral operation
- Flexible pin muxing

Main Supply Voltage

- 3.3V (3.0V~3.6V)

IO Voltage

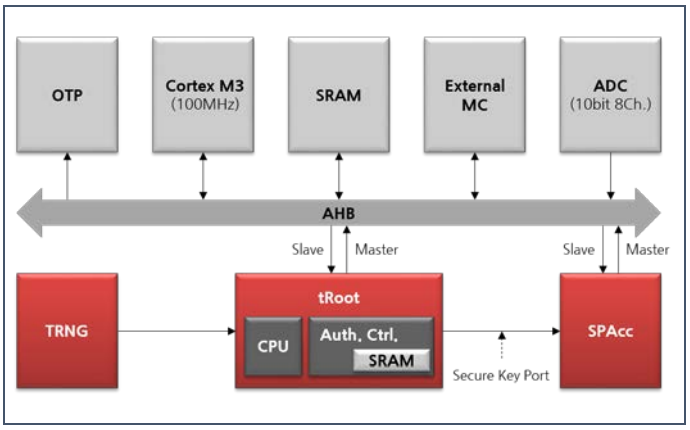
- 3.0V~3.6V

Applications

- **Home Entertainment**
  - Smart TVs
  - Set-top-boxes
  - Gaming Consoles
- **Internet of Things**
  - Smart Automotive
  - Smart Payment
  - Smart Grid
  - Smart Medical
- **ETC**
  - Home Appliances
  - Electronic devices linked to the Internet

Functional Diagram

This diagram shows the superset of features for the MS1000 microcontroller.



Package Information

- 121-pin BGA
- Ball Pitch: 0.65 mm
- Package Width x Length: 8 mm x 8 mm

For more information, please visit: http://www.e-wbm.com.
For sales inquiries, please email to: info@e-wbm.com

eWBM Co. Ltd. ♦ 344 Pangyo-ro, 3F, IDIS Tower, Bundang-gu, Seongnam-si ♦ Gyeonggi-do, Korea
Main: +82-31-707-5600 ♦ Fax: +82-31-789-0080 ♦ http://www.e-wbm.com