ABRIDGED DATA SHEET

Rev 1; 2/10

EVALUATION KIT AVAILABLE

High-Performance, Secure, 32-Bit MIPS Microcontroller Supporting Linux OS

USIP PRO

General Description

The USIP™ Professional IC (USIP PRO) is a secure microcontroller designed to provide an interoperable, secure, and cost-effective environment for new generations of trusted devices. This secure platform is fully compliant with EMV® and PCI PED standards. The USIP PRO is based upon the most secure, 32-bit, RISC core (MIPS32® 4KSd™) from MIPS Technologies. While providing superior performance (1.35MIPS/MHz), this low-power core adds special instructions to accelerate cryptographic operations and security functions to enforce system integrity. Complemented by a secure memory management unit (MMU), the USIP PRO can run feature-rich operating systems such as Linux® in a secure way.

System security is enhanced by a number of physical and logical protection mechanisms including environmental sensors (temperature, voltage, and frequency), active metal shield, real-time clock (RTC), and 512 bits of secure NVM storage (BPK) with instant erase capability upon tampering. For greater privacy, external memory content is fully protected through a universal cryptographic interface (UCI) that performs on the fly AES-128 encryption/decryption. The USIP PRO is one of the most integrated solutions for financial and other trusted terminals. It includes 128KB of SRAM, 128KB of ROM, 256KB of flash, and 256 bytes of OTP. Additionally, the USIP PRO accommodates external memories such as NOR flash, SRAM, and SDRAM.

The device provides extensive communication support with USB On-The-Go (OTG), UART, SPI™, I²C, PS/2, IrDA, and parallel SPP. In addition, the USIP PRO offers a unique set of peripherals such as smart card controllers, LCD interface, thermal printer interface, GPIO, PWM, watchdog, general-purpose timers, and a built-in ADC.

Applications

EFTPOS
PIN Pads
ATM Keyboards
Healthcare Reader
Electronic Metering

USIP is a trademark of Maxim Integrated Products, Inc.

EMV is a registered trademark of EMVCo, LLC.

MIPS32 is a registered trademark and 4KSd is a trademark of MIPS Technologies, Inc.

Linux is a registered trademark of Linus Torvalds.

SPI is a trademark of Motorola, Inc.

Features

- **MIPS32 4KSd RISC Processor**
  - 130 MIPS at 96MHz
  - 2 x 8KB Cache
  - Memory Management Unit
  - Dedicated Cryptographic Instructions
- **Memories**
  - 128KB of SRAM
  - 256KB of Lockable Flash Memory
  - 256 Bytes of User OTP
  - 128KB of ROM (HAL, EMV Level 1, Secure Bootloader)
  - Memory Controller Supporting One SDRAM and Up to Four Static Memories (Flash or SRAM)
- **Security Features**
  - Encryption Engine for External Memories
  - Hardware AES-128 Engine
  - Unique Serial Number (USN)
  - 512-Bit Battery-Powered Key Area (BPK) with Instant Erase Upon Tampering
  - Integrated Tamper Sensors (Frequency, Voltage, Temperature, Die Shield)
  - 12 External Sensor Inputs
  - True Random-Number Generator (TRNG)
  - Secure RTC with Interrupt Alarm
  - Secure Keyboard Controller (12 x 12)
- **Interrupt Controller**
- **1D/2D DMA**
- **LCD Interface: 8-Bit Bus, 6800 Compatible**
- **Three ISO 7816 Controllers**
- **Thermal Printer Interface**
- **USB 2.0 OTG Full Speed with 16 Endpoints**
- **Four UARTs (IrDA and Full Modem Support)**
- **I²C Master/Slave**
- **SPI Master/Slave with Up to Seven Slaves**
- **6-Channel, 10-Bit ADC**
- **32 GPIOs**
- **Four 16-Bit Timers/Counters**
- **Two PWMs with One 15mA Output**
- **Watchdog Timer**
- **JTAG Boundary Scan**

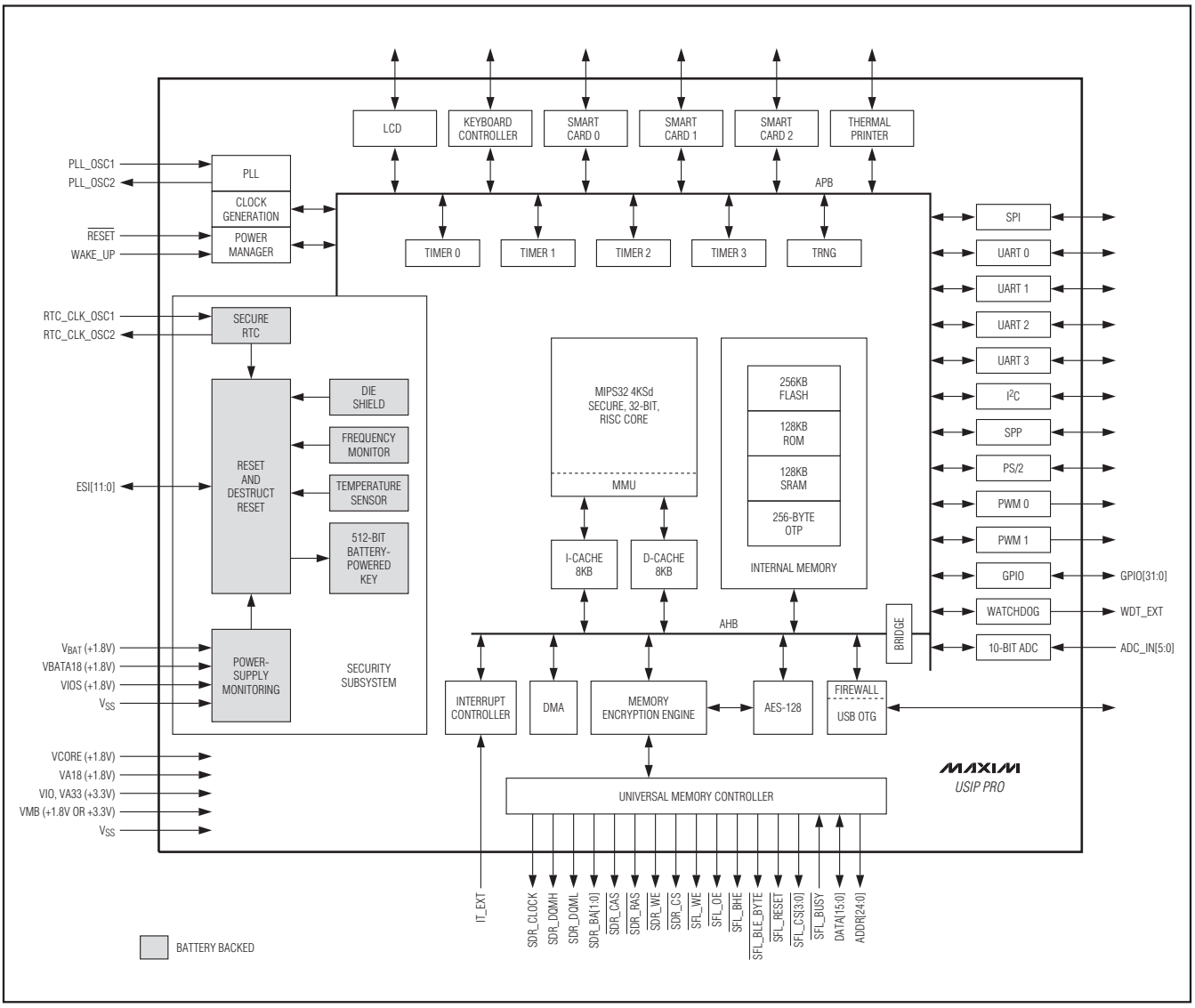
Ordering Information

PART	TEMP RANGE	PIN-PACKAGE	JTAG
IC0400C778BF+	-40°C to +85°C	256 LFBGA	No
IC0400K778BF+	-40°C to +85°C	256 LFBGA	Yes

+Denotes a lead(Pb)-free/RoHS-compliant package.

High-Performance, Secure, 32-Bit MIPS Microcontroller Supporting Linux OS

Functional Diagram



Note to readers: This document is an abridged version of the full data sheet. To request the full data sheet, go to **www.maxim-ic.com/USIP** and click on **Request Full Data Sheet**.