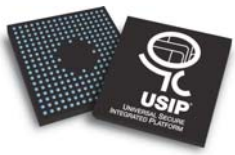
USIP® Universal Secure Integrated Platform

Professional IC

Universal Secure Integrated Platform for trusted terminals



USIP® Professional IC
actual size : 15 x 15 mm

USIP® Professional IC is a secure System on Chip (SoC) providing all the functionalities required to build new generations of trusted terminals and readers.

USIP® Professional IC is dedicated to applications that need a high level of security and confidentiality such as financial transactions and payment (EMV and GP/STIP), healthcare, identity, access control, mobile applications, Pay TV, biometry.

Main Features

- MIPS®4KSd™ 32-bit RISC processor
- Embedded memories (SRAM, ROM, Flash)
- Patented security and cryptographic features
- Controllers, analog and digital interfaces (smart card, USB, SPI, etc)
- Power Management

Benefits

- Offers Single-Chip Solution
- Reduces drastically the Bill of Materials
- Facilitates Certification (EMV PCI PED compliance)
- Speeds up Time To Market
- Enables Migration to Open Platforms
- Enables new Form Factor Devices

INNOVA CARD

ZI Athélia II - Avenue Coriandre - 13704 La Ciotat Cedex - France
Tel : + 33 (0) 4 42 98 14 80 – Fax : + 33 (0) 4 42 08 33 19 – E-mail : contact@innova-card.com
www.innova-card.com

USIP® Universal Secure Integrated Platform

Professional IC

Innova Card is a semiconductor fabless company that designs complex Systems on Chip and supplies secure hardware and software solutions for trusted terminals.

By extending the secure smart card technology onto chips for terminals, Innova Card offers the most secure and integrated circuit called: **USIP® Professional IC.**

INNOVA CARD

ZI Athélia II - Avenue Coriandre
13704 La Ciotat Cedex - France

Tel. : + 33 (0) 4 42 98 14 80
Fax : + 33 (0) 4 42 08 33 19

E-mail : contact@innova-card.com

www.innova-card.com

Product Features

32-bit RISC Processor

- **USIP® Professional IC** embeds the MIPS32® 4KSd™ secure processor from MIPS® Technologies.
- It is a high-performance, low-power core designed for custom system-on-silicon applications.

Main characteristics

- 1.35 MIPS/MHz (Dhrystone) 129,6 MIPS@96MHz
- Specific instruction set for cryptographic applications (smart MIPS)
- 8 KByte data cache and 8 KByte instruction cache memories
- 5-Stage Pipeline
- 16-bit code compression via MIPS16e™ ASE

Memories

- 128 KBytes of SRAM
- 128 KBytes of ROM
- 256 KBytes of Flash Memory with locked features
- 256 Bytes of OTP
- Universal Memory Controller (UMC) to manage external SRAM/SDRAM/Flash Memory (1.8V or 3.3V supported)

Security Aspects

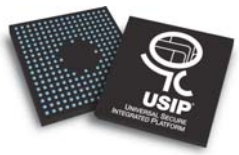
- **USIP® Professional IC** provides developers with a large set of security features that facilitates software developments for secure applications and enhances the security level.
- Secure Memory Management Unit (MMU): protection of pages individually programmable (execute, read, and write) – 1KByte of granularity
- Unique chip Serial Number (USN)
- **USIP®** Crypto Interface (UCI): efficient on-the-fly encryption of memories based on the NIST FIPS-197 Standard AES
- Firewall for USB Access
- Protected Storage Area
- Tamper protection, internal sensors (voltage, frequency, temperature, active metal shield) and external sensors input – also operate in power down mode
- True Random Number Generator: NIST and DIEHARD tests passed
- AES crypto processor
- Secure Boot Loader with dynamic authentication based on AES

Controllers, analog and digital Interfaces

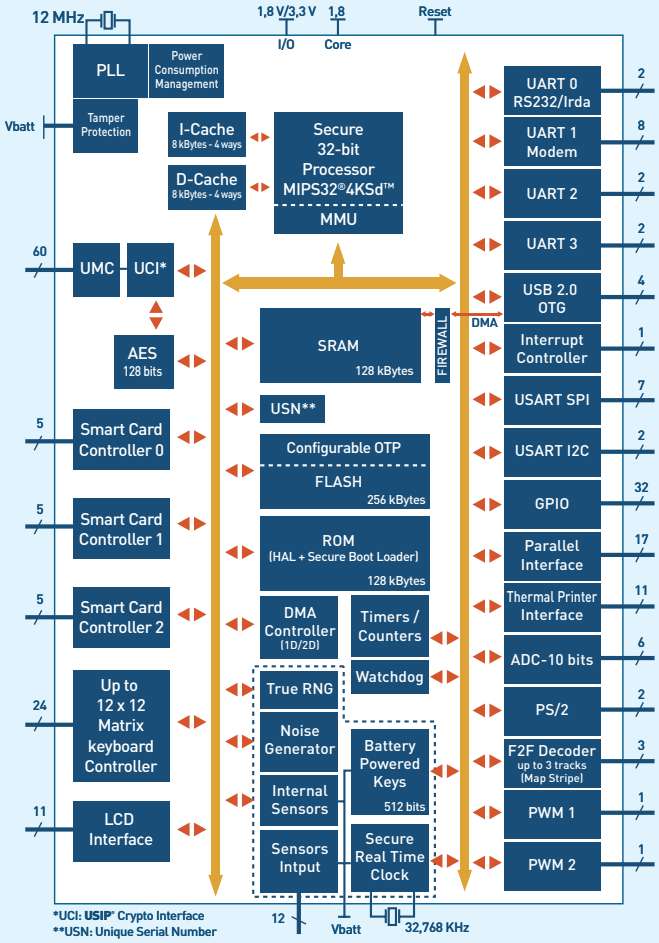
- 3 reversible smart card controllers: ISO-7816 (T=0 and T=1) UARTs with EMV Level 1 driver. They are able to manage up to 10 smart cards
- 3 channels F/2F decoder: digital part of the Magnetic Stripe Reader interface (up to 3 tracks supported and two-way reading)
- Thermal printer interface: it can drive any thermal print head in serial mode. It includes the stepper motor control
- Secure Real Time Clock powered by an independant battery
- Keyboard controller: a 12x12 Matrix Keyboard interface with hardware scanning and debouncing features
- LCD interface
- DMA controller
- Communication interfaces: USB OTG 2.0 full speed, UARTs, UART Modem, SPI master / slave, I2C master / slave, Parallel, PS2, IrDA/UART
- General purposes: 32 GPIOs, 2 PWMs, Watchdog, 4 Timers/Counters, 6 ADC inputs (10-bit resolution)

Power Management

- Dynamic Frequency Management from 12 to 96 MHz
- Low Power Core Consumption
- Gated Clock on each block
- Power Supply Supervisor
- Interrupt Based System
- Running / Idle / Power Down Modes



Block Diagram of USIP® Professional IC



Graphic Design : www.bruno-r.com