

Safe-SOC™

Security in Silicon

Comprehensive Security for Content-Driven Consumer Electronics Markets

Stringent security is critical in the consumer electronics market, especially in the set-top box, conditional access, network storage and mobile markets where valuable digital content needs to be protected. The Safe-SOC™ security platform from MIPS Technologies and msystems provides a comprehensive security solution by tightly integrating msystems' patented mSafe™ cryptographic cores with MIPS Technologies' entire line of CPUs for a robust, flexible and tested security solution. In addition, the Safe-SOC platform includes msystems' MIPS®-optimized cryptographic protocols, APIs and drivers.

FEATURES

The Safe-SOC platform combines msystems' security IP with the industry-leading MIPS® architecture.

- Higher level of security based on MIPS Technologies' unique and ubiquitous Co-Processor 2 (CoP2) interface
- Guaranteed bandwidth availability with lower latency
- Multiple levels of security, including protecting different security peripherals from each other
- Tight integration
 - Cryptographic and trust elements in a single solution
 - Dedicated CoP2 interface provides tighter coupling than the traditional peripheral bus (e.g., AHB) approach
- Compatible with all existing and future MIPS cores with CoP2 interface
- Modular design
 - Implement only the required crypto cores using the exact size of each core based on performance, power and gate count considerations
 - Shortens product time-to-market while minimizing development risks
- Minimal area impact: does not exceed 1 mm² area when using 130nm technology
- Highly flexible solution with almost limitless combination of crypto cores in typical applications
- Licensing and support from msystems for Safe-SOC and from MIPS Technologies for its CPU cores

msystems

MIPS
TECHNOLOGIES

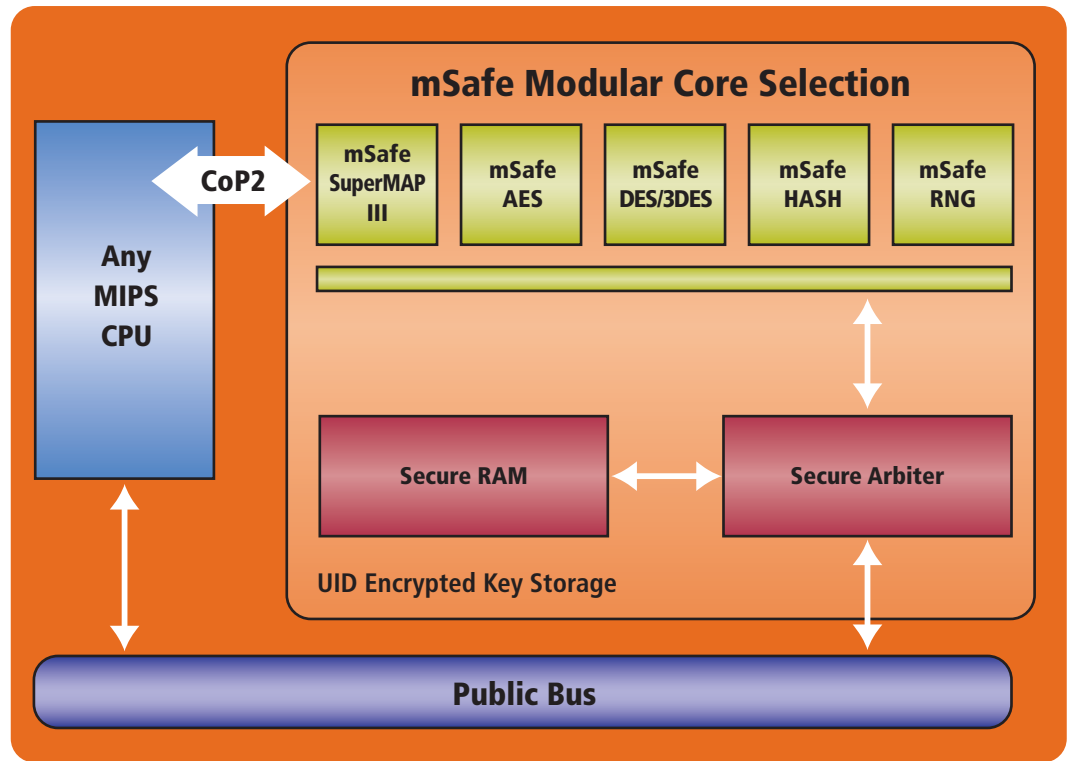
At the core of the user experience.®

PRODUCT BRIEF

Safe-SOC™

Safe-SOC™:
optimized and
integrated
security solution

Safe-SOC Platform: Superior Security in a Trusted Environment



SPECIFICATIONS

- Hardware-protected domain for secret keys
- Crypto cores available:
 - SuperMAP III for PKI algorithms, including: RSA, DH, DSS, ECDH, ECDSS in GF(p) and GF(2ⁿ)
 - AES supports 128-, 192- and 256-bit key length
 - DES/3DES supports 56-, 112- and 168-bit key length
 - HASH supports SHA1 and MD5
 - RNG
- Crypto cores are customizable to fit performance, power and gate count tradeoffs
- Built-in protection against hardware and software attacks
- Support for “on the fly” data encryption for HASH and block ciphers
- Optional MPU implementation for software domain protection
- Crypto library for hardware management
 - Optional secure storage and secure boot functionality
 - Extendable to support DRM and other applications

FEATURES

- Works with all current and future MIPS cores with CoP2 interface
- Management and protection of secured assets
- Full set of crypto services
- Cryptographic hardware acceleration utilizing msystems' mSafe family
- MIPS-optimized crypto software, protocols, APIs and drivers
- Highly power-efficient design
- Off-the-shelf solutions for various markets and applications including STB, DTV, IPTV, consumer electronics, smart cards, communications and automotive



At the core of the user experience.®

MIPS Technologies, Inc.
1225 Charleston Road
Mountain View, CA 94043-1353
Phone: (650) 567-5000
Fax: (650) 567-5158
Email: Safe-SOC@mips.com
www.mips.com



msystems
7 Atir Yeda St.
Kfar Saba 44425, Israel
Phone: +972-9-763-2511
Fax: +972-3-548-8666
Email: mSafe@m-systems.com
www.msystems.com