

Low-power,
high-performance
core for secure data
applications

Baseline Specifications

Product	MIPS32 4KSd core
Process	0.13 μm G
Frequency (MHz) (Worst case)	90–211
Max. Performance (DMIPS)	322 @ 200 MHz 1024-bit RSA signature generation in less than 15 ms @ 200 MHz
Power (mW/MHz)	0.29-0.32 @ 1.2V, excluding caches
Core area (mm²) Core only	1.0-1.4

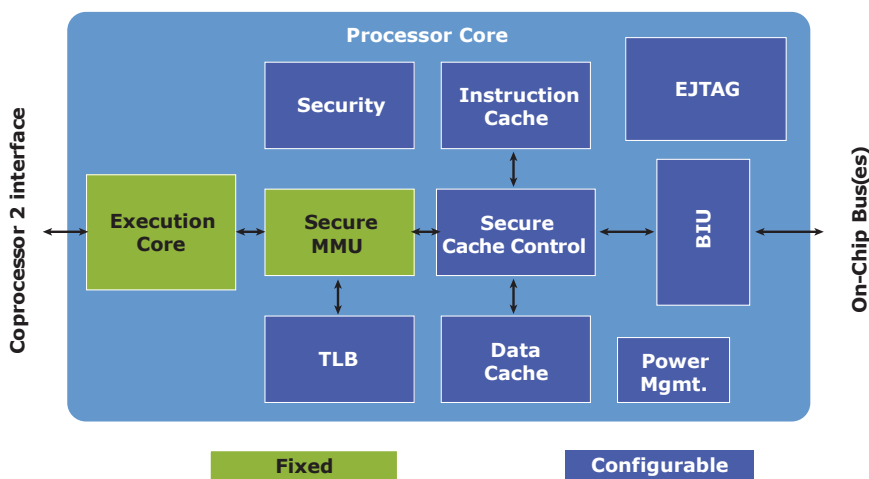
Notes:

Frequency, power consumption and size depend upon configuration options, synthesis, silicon vendor, process and cell libraries. Worst case is slow silicon, 1.08V, 125C.

MIPS32® 4KSd™

The MIPS32® 4KSd™ secure data core is a high-performance processor that meets the needs of emerging secure data applications and the stringent power, security and size requirements for smart cards. This core has the performance required to implement software programmable cryptography without the need of a coprocessor, reducing SoC size and power consumption. The 4KSd core is the most secure, licensable, 32-bit processor available.

The 4KSd is an integrated, fast time-to-market solution for building secure SoCs. It includes the industry-standard SmartMIPS™ ASE that provides advanced software cryptography and data security features. Special anti-tampering features resist external attacks via noninvasive techniques. The 4KSd core sets the standard for low power, software-programmable cryptography and security.



MIPS32 4K Core Highlights

- Extensive security features disguise processor activity, resist external attacks and prevent tampering through power analysis and other techniques
- MIPS cryptography enhancements speed public- and secret-key cryptography algorithms for data security without additional dedicated hardware or coprocessor modules
- Secure memory spaces protect sensitive consumer data by application and prevent unauthorized data access by rogue applications
- CorExtend™ capabilities allow expert designers to further differentiate their secure SoC applications by adding their own instructions to create unique security features
- Meets the high-performance requirements for emerging secure data markets and the small size and low-power consumption necessary for next generation smart cards
- Low interrupt latency allows the core to respond more quickly to external events
- MIPS16e™ code-compression allows usage of smaller memories, reducing power consumption and die size
- Based on the enhanced MIPS32 industry-standard architecture, with hundreds of third-party development tools and applications

Features

Security Features

- Multiple techniques implemented to disguise processor activity and resist invasion by power analysis and other non-invasive techniques
- Lowest interrupt latency of any secure 32-bit core allows faster response to external events

SmartMIPS Secure ASE

- Speeds public- and secret-key cryptography algorithms and eliminates the need for coprocessors, reducing die size and total cost
- Supports multiple encryption algorithms
- Secret key: DES, 3DES and AES (Rijndael)
- Public key: RSA, elliptic curve (especially GF [2n])
- New cryptography standards as they become available
- Increases performance of virtual machines
- Designed to support Sun Microsystems' Java Card™ technology

Memory-Management Unit

- 16 dual-entry JTLB with variable page sizes, from 16MB down to 1KB
- Workstation-class virtual memory support
- Read-only, write-only and execute-only page attributes
- Secure memory spaces protect sensitive consumer data by application and prevent unauthorized data access by rogue applications
- Each application resides in a different virtual space

User Defined Instruction Set Extensions

- Maintains MIPS32 compatibility
- Supported by industry standard development tools
- Single- or multi-cycle instructions

MIPS16e™ Code Compression

- Reduces application code size by up to 40%

Fully Integrated Cache Controller

- Improves performance with slow memories
- Individually configurable 0–64KB instruction and data caches
- Direct-mapped, 2-, 3-, or 4-way set-associative (0KB, 1KB, 2KB, 4KB, 8KB, or 16KB per way)
- Write-back or write-through

Optional EJTAG Debugging

- May be disabled for production silicon
- Supports PC and data trace

Low-power,
high-performance
core for secure data
applications

Worldwide Offices

Headquarters
MIPS Technologies, Inc.
955 East Arques Avenue
Sunnyvale, CA 94085
United States
Phone: 408-530-5000
Fax: 408-530-5150
www.mips.com
info@mips.com

MIPS Technologies, Inc. (Oregon)
Beaverton, Oregon
Phone: 503 597-5091
Fax: 503 924-1110

MIPS Technologies (Shanghai) Co., Ltd.
Shanghai, China
Phone: +86 21 6385 8383
Fax: +86 21 5306 0833

MIPS Technologies B.V.
Jhubei, Taiwan
Phone: +886 3 6583 561
Fax: +886 3 6583 563

MIPS Technologies B.V.
Tokyo, Japan
Phone: +81 3 5733 9541
Fax: +81 3 5733 9545

MIPS Technologies B.V.
Halver, Germany
Phone: +49 170 6365 370
Fax: +49 2353 666 920

MIPS Technologies B.V.
Nesher 36841, Israel
Derech Bar Yehuda 53 - POB 12034
Phone: +972 (545) 441 579
Fax: +972 (153) 545 441579



© MIPS Technologies, Inc. All rights reserved.
MIPS, MIPS32, MIPS16e, 4KSd, SmartMIPS, CorExtend
MIPS and MIPS-Verified are trademarks or registered
trademarks of MIPS Technologies, Inc. in the United
States and other countries. All other trademarks referred
to herein are the property of their respective owners.
Printed in the USA. Rev 0605