

MIPS32[®] 4KSd[™]

Secure Data Core

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

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.

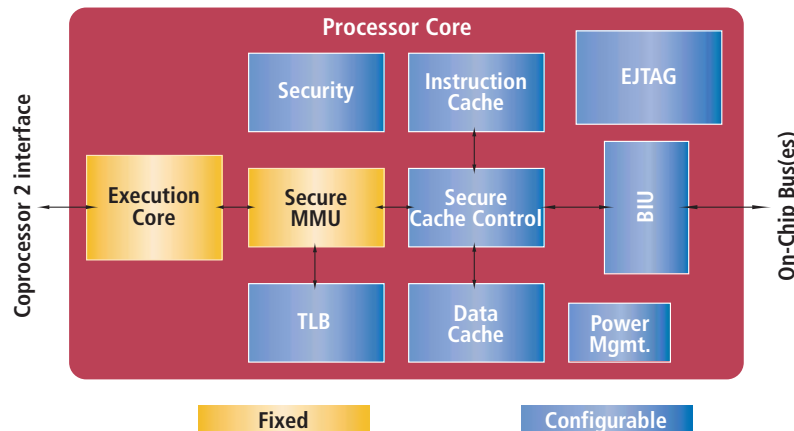
THE MOST SECURE CORE

The MIPS32[®] 4KSd[™] secure data core, with the SmartMIPS[™] application specific extension (ASE) to the MIPS32 architecture, provides unprecedented performance and security for emerging secure data applications and next generation smart cards. High-performance cryptography and enhanced security features make the 4KSd core the most secure, licensable, 32-bit processor.

- 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

MIPS32® 4KSd™ Secure Data Core

**MIPS32® 4KSd™
Secure Data Core:**
Low-power,
high-performance
core for secure data
applications



The MIPS32® 4KSd™ secure data core 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.

SPECIFICATIONS

Process	0.13 µm generic
Frequency	(worst case) 90–211 MHz
Performance	<ul style="list-style-type: none"> • 322 DMIPS @ 200 MHz • 1024-bit RSA signature generation in less than 15 ms @ 200 MHz
Power Consumption	0.29-0.32 mW/MHz at 1.2V, excluding caches
Core Size	1.0-1.4 mm ² , excluding caches

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

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



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

MIPS Technologies B.V.
Berghauser Strasse 62
42859 Remscheid
Germany
phone: +49 2191 900 200
fax: +49 2191 900 208

MIPS Technologies Japan
Landic Toranomon Bldg. No. 2
3-7-8, Toranomon, Minato-ku
Tokyo 105-0001 Japan
phone: +81 3 5733 9541
fax: +81 3 5733 9545

www.mips.com

