

SmartMIPS® Architecture

Smart Card Extensions

The next-generation
architecture for secure,
multi-application
smart cards

Today's smart cards must support multiple applications and deliver uncompromising levels of security. The SmartMIPS® extensions to the MIPS32® architecture, jointly defined with Gemplus SA—the world's number one provider of smart cards—provide a complete solution, delivering unparalleled security and cryptography performance.

The SmartMIPS architecture marries cryptography enhancements, Secure Memory Spaces, code compression and virtual machine performance enhancements to enable an inexpensive, low-power and complete smart card processor solution.

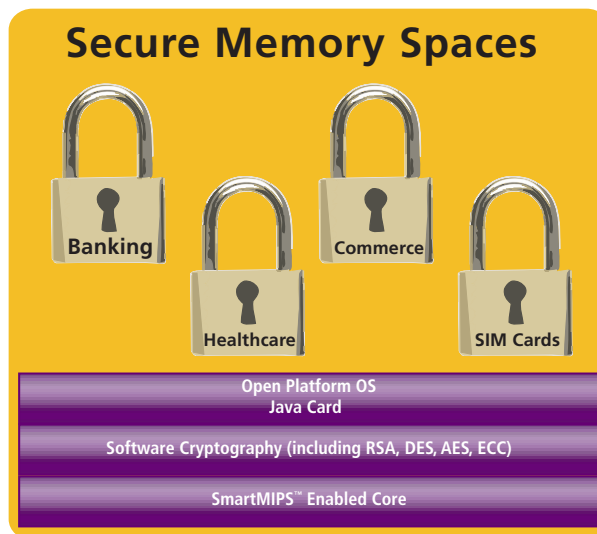
SECURE SMART CARD PERFORMANCE

The SmartMIPS® architecture improves information protection and application flexibility with a powerful combination of software cryptography and enhanced security features resulting in an industry-standard architecture for multi-application smart cards.

- The SmartMIPS architecture's cryptography enhancements speed public- and secret-key data security algorithms, eliminating the need for dedicated coprocessors, and reducing die size and total system cost
- Software cryptography allows easy field upgrades of cryptography algorithms. Therefore, a potential breach in the security algorithm doesn't require a recall of the actual cards
- Accelerated software cryptography enables choice of algorithm (such as RSA, DES, AES, and elliptic curve cryptography) on a per-application basis
- Secure Memory Spaces protect sensitive consumer data by application, preventing unauthorized data access by rogue applications
- Code-compression minimizes memory use, preserving scarce memory resources
- Designed to support and accelerate key operating systems such as Sun Microsystems' Java Card™ technology

SmartMIPS® Architecture Smart Card Extensions

The SmartMIPS architecture: High-performance cryptography and security for low-power, multi-function smart card processors



Secure Memory Spaces encapsulate applications and safeguard sensitive customer information, providing an unprecedented level of security for smart cards.

SmartMIPS ARCHITECTURE FEATURES

- Accelerated Software Cryptography
- Java Card
- Code Compression
- Secure Memory Spaces

MIPS® ARCHITECTURE BENEFITS

- Industry standard 32-bit MIPS architecture provides, low-risk, leading-edge technology
- Supported by hundreds of third-party development tools, software and applications for fast time-to-market and a shortened design cycle

MIPS Technologies' Software Cryptography Strategy

Today's security technology using dedicated hardware coprocessors is inadequate for next-generation multi-function smart cards. The need for longer keys and newer, more secure algorithms such as AES and elliptic curve cryptography require more flexible cryptography solutions than fixed-function hardware blocks allow. The high performance software-based cryptography enhancements in the SmartMIPS architecture allow a wide choice of algorithms and permit reuse rather than replacement of deployed smart cards when algorithms change.

The SmartMIPS architecture was designed to support a wide variety of algorithms, including RSA, DES, AES, and elliptic curve cryptography. The SmartMIPS architecture provides the flexibility demanded by next-generation multi-function smart cards.

Support for Interpreted Language Acceleration

Multi-function smart cards require platforms that support interpretive languages. This strategy provides a portable and secure framework for multi-application smart cards. However, there are competing interpretive languages that fulfill this requirement. MIPS Technologies has chosen to provide maximum flexibility to licensees by extending the SmartMIPS architecture in ways that accelerate interpretation in general, rather than any one interpretive language.

Secure Memory Spaces

Smart cards are subject to all manners of attacks that endeavor to compromise their integrity. A smart card architecture must increase overall system security and not provide a point of vulnerability. The architecture must support secure programming and secure operating systems.

The SmartMIPS architecture is specifically designed to provide all the memory management mechanisms necessary to support secure programming and verifiably secure operating systems. User code is separated from system code; applications can be encapsulated in their own memory areas and execute-, read-, and write-only page-protection attributes are individually programmable.



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

www.mips.com

