



Security Platform for MIPS® Architecture Powered by Discretix CryptoCell®

Overview

Security plays an important role in today's connected consumer devices. Smartphones, e-book readers, storage devices and media players rely on high-performance robust security solutions to enable premium content services. Security also protects the device and its software against hacking and malicious attacks. The Security Platform for MIPS® Architecture includes a security subsystem based on the Discretix CryptoCell®, providing the highest available level of device and application security.

Security Platform for MIPS® Architecture Powered by Discretix CryptoCell®

The security platform provides a comprehensive solution for a broad range of connected devices. Integrating the industry standard MIPS32® family of products with CryptoCell, the platform offers a superior level of security, while addressing the challenges of increased system complexity, high performance and low power consumption. CryptoCell's multi-layered architecture combines embedded coprocessors with a rich layer of security middleware.

The Security Platform for MIPS® Architecture offers many advantages to chipset manufacturers, device OEM's and consumers:

- **Platform protection and integrity** - Preventing unauthorized code modification and "break once run everywhere" attacks.
- **Anti-hacking** - Protect OEMs against reverse engineering, device cloning, illegal software updates and unauthorized access to run-time data.
- **Content protection** - Implementation of commonly used DRM and Conditional Access schemes enabling advanced content usage models; sharing content between devices, secure recording (DVR), video-on-demand.
- **IPSec** - Efficient processing of network security protocols.
- **E-commerce** - Protects key material, certificates, and data.

Features

- High throughput hardware cryptographic engines and random number generators
- Compact secure boot preventing unauthorized code modification; supporting software update with a boot load hierarchy
- Fault-tolerant secure database providing confidentiality and data integrity
- Robust key management handling all key material without exposing unencrypted keys
- Secure debug preventing software-based debug and test attacks
- High throughput for multimedia processing
- API support for various operating systems
 - Linux
 - Android
 - Windows phone 7
 - Symbian
 - Discretix APIs
- Easily integrated as a system-on-chip (SoC) peripheral
- Silicon-proven on multiple embedded systems and configurations

Security Platform for MIPS® Architecture Powered by Discretix CryptoCell®

The Security Platform for MIPS® Architecture features a wide array of customizable components to deliver attack-resistant implementation embedded security solutions.

Components	Benefit
Secure boot	Prevents modification or replacement of software code images residing in non-volatile storage
Secure execution environment (SEE)	Provides a robust hardware compartment for secure execution of security-sensitive code, such as rights-object handling and parsing as well as time and date enforcement
Cryptography acceleration	High performance, low power - a comprehensive set of state-of-the-art cryptographic engines (AES, DES, HASH, RC4, RSA, ECC), providing hardware acceleration of common cryptographic functions
Security services	A rich set of security middleware services provides key management functions, secure database, certificate handling and DRM enforcement functions
Secure storage	Keeping all security-related items protected for confidentiality and integrity; detects any modifications; and guards against power-downs and other system-level faults
Secure debug	Prevents debug and test attacks; supports multiple debug domains
Open security system	An SDK for application developers to write additional security services for execution in CryptoCell's secure execution environment
Run-time integrity checking	Verifies software image integrity at run time
Code encryption	Prevents reverse-engineering and software theft
Secure data path	Protected data processing flows for high value multimedia content

For more information please contact:

MIPS Technologies, Inc.

sales@mips.com
info@mips.com

T. +1 408 530 5000

www.mips.com

Discretix Inc.

marketing-dx@discretix.com

T. +1 408 969 9991
+972 73 255 8800

www.discretix.com

Lisa.Yang@discretix.com

T. +886 2 8792 9423

