TECHNICAL DATA SHEET

SecRun

Integrated FPGA/ASIC Security Platform

State-of-the-art system security against cyber and physical threats

- Proven SCA countermeasures eliminate ASIC/FPGA vulnerabilities
- Protect cryptographic keys throughout the device operational lifecycle
- Store sensitive data in secured commodity off-chip memories
- Deploy rapidly with hardware-ready integrated security

Highlights

- Full chip security with integrated key and external memory management
- Protection against side-channel attacks
- Secure off-chip volatile storage
- Key lifecycle protection
- Isolated networks protect "red" keys against cyber-attacks
- NIST-compliant functionality
- Strongest at-rest defense with device-unique fingerprinting integration
- Customizable to fit any application

Cyber and physical security are imperative to protect sensitive data and maintain system integrity. SecRun utilizes SecBoot, InCipher and KeyGuard technologies to provide systems with side-channel attack (SCA) countermeasures (CM), internal encrypted key storage and distribution and enhanced threat responses.

Maintaining defenses across key storage at rest, initialization at power-on, and use of keys at runtime is critical for side channel analysis resistance. SecRun offers a fully pre-integrated security platform featuring SCA countermeasures on key management and NSA Suite B/Commercial National Security Algorithm Suite (CNSA) ciphers and algorithms. When integrated with secure boot (SecBoot) and runtime transparent memory encryption (InCipher) modules, SecRun delivers system security from FPGA/ASIC initialization through system power-off.

SecBoot

SecRun's secure system controller module, SecBoot, optimizes secure device initialization to maximize throughput while reducing buffer memory usage. It provides a convenient, secure bring-up that reuses the resources required by SecRun's runtime operations. SecBoot also addresses potential bootloader and bootimage attacks by employing a secure secondary bootloader that evolves over time.

CONTACT US

InCipher

SecRun's memory encryption module, InCipher, applies leakage reduction and protocol CM during encryption to protect memory contents before device boundary exposure. Providing SCA protection for keys to over a billion encryption cycles, it also employs a strategic key refresh schedule with multiple keys that replace keys before attacks can conceivably be mounted.

KeyGuard

SecRun's KeyGuard key manager provides complete key lifecycle protection by ensuring keys never leave SCA protections. It performs all necessary system key services: generation, import, export, and distribution of private keys and other critical security parameters (CSPs).

KeyGuard delivers red/black separation by isolating red keys from the system bus and host processor, replacing memory mapped key interfaces with direct point-to-point key distribution channels.

Hardware Agnostic

SecRun with SecBoot, InCipher, and KeyGuard is available as part of a bundle on supporting Mercury embedded processing hardware or as a standalone capability that may be integrated into any existing system that leverages FPGA and ASIC technologies.

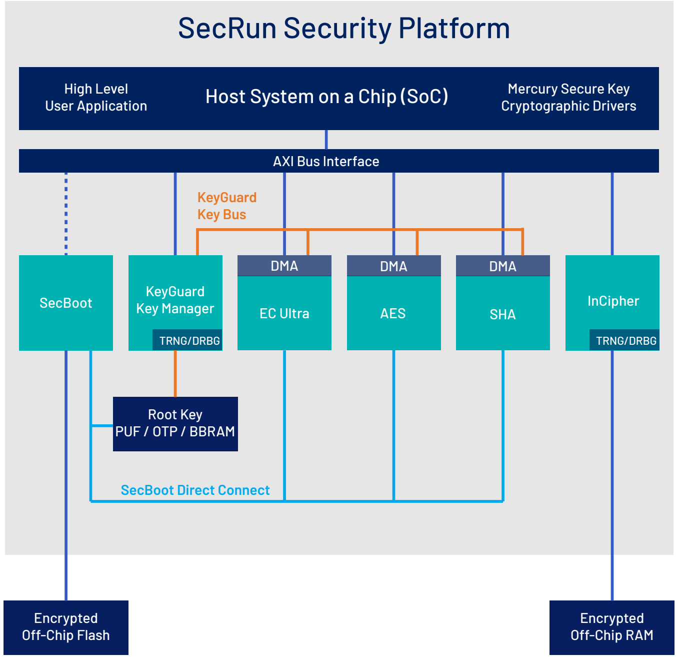

Figure 1: An example system secured by KeyGuard with private connections to EC, PK, AES, MAC, and SecBoot/InCipher integrations.

Customize to Fit Any Application

Configurable to support a multitude of devices, applications and performance levels, SecRun's subcomponents can be configured to range from minimal area for small edge devices to the extreme performance for datacenter applications.

mercury

Corporate Headquarters

50 Minuteman Road
Andover, MA 01810 USA
+1 978.967.1401 tel
+1 866.627.6951 tel
+1 978.256.3599 fax

International Headquarters
Mercury International

Avenue Eugène-Lance, 38
PO Box 584
CH-1212 Grand-Lancy 1
Geneva, Switzerland
+41 22 884 51 00 tel

Learn more

Visit: mrcy.com/secureservers

The Mercury Systems logo and the following are trademarks or registered trademarks of Mercury Systems, Inc.: Mercury Systems and Innovation That Matters. Other marks used herein may be trademarks or registered trademarks of their respective holders. Mercury believes this information is accurate as of its publication date and is not responsible for any inadvertent errors. The information contained herein is subject to change without notice.

MADE IN USA

8192.02E-1122-DS-SECRUN