RelianceOne™ Trusted Platform

Key Management

RelianceOne Trusted Platform is a flexible security architecture for building secure launch solutions. It is a collection of integrated security capabilities – measured boot, firmware independent key management, secure remote updates, and out-of-band runtime protection – that customers can deploy incrementally to match threat levels and budget constraints.

With the RelianceOne Trusted Platform – Key Management, any Intel x86 platform can be turned into a fully automated, secure platform by seamlessly integrating Key management and secure key release for full disk encryption (FDE) solutions such as self-encrypting drives (SDEs) or encrypted file systems or eliminate manual authentication (such as, passwords and smart cards), fulfill secure boot and data at rest requirements, eliminate integration cost and risk, and keep sensitive keys safe from compromise.

KEY MANAGEMENT DELIVERS

Enhanced Trust

- Keys to decrypt drives are only released in a limited, "known-good" environment and system configuration.

Unintended Operation – No Manual Password Entry

- Fully automated boot.
- Compatible with untrusted operator.
- Perfect for edge-deployed, high-availability, mission-critical systems.

Eliminates BIOS/SED Compatibility Issues

- No vendor-specific BIOS updates or compatibility fixes required.
- Deploy any compliant Full-Disk Encryption/Self-Encrypting Drive (FDE/SED) with confidence on commodity hardware.
- Works with any Trusted Computing Group (TCG) Opal/Enterprise 2.0+ SED regardless of firmware version.

Flexible Design

- Supports both local and network boot.
- Trivially extended to incorporate additional forms of authentication – Hardware Security Module (HSM), smart card, etc.

Secure Updates Without Reprovisioning

- Updates can be delivered remotely, without reprovisioning hardware or resetting keys.
- Cryptographically signed updates verified before installation.
- Fleet-wide deployment capability for long-lifecycle defense systems.

Access to Stored Data Can Be Temporarily or Permanently Removed

- Provides rollback prevention – trusted updates can be delivered to prevent drive unlocking securely remove keys and invalidate all previous versions.
- Alternative to drive erasure.

IDEAL USE CASES

Defense and Intelligence: Tactical edge servers, unmanned systems, Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) with zero-downtime requirements.

Critical Infrastructure: Industrial control, healthcare, financial systems requiring tamper-evident security.

Any Application Needing: Full disk encryption without operational overhead, hardware-rooted boot integrity, automated secure boot, protection against sophisticated physical or remote attacks.

TECHNICAL HIGHLIGHTS

Platform: Intel® x86 | TPM 2.0.

Storage: Self-Encrypting Drives (TCG Opal/Enterprise 2.0+) or LUKS/dm-crypt.

OS: Any Linux® distribution (RedHat®, Ubuntu, CentOS) | Legacy BIOS or UEFI.

Security: TPM 2.0 key sealing/unsealing | Measured boot with PCR extension | Cryptographic verification of boot components.

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 5100 tel

Learn more
Visit: mrcy.com/
Contact: mrcy.com/contact-us