RelianceOne™ Trusted Platform

Secure Remote Update

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.

Maintain security posture for years without physical access to deployed systems. Secure Remote Update enables field updates to deployed systems without requiring local provisioning or manual key management.

Deploy once, update anywhere with no per-system manual intervention. Updates are packaged, cryptographically signed, and deployed remotely with automated Trusted Platform Module (TPM) resealing. Hardware-enforced rollback protection ensures systems can only advance to newer, authorized versions—preventing attackers from downgrading to vulnerable software.

Each update package is sealed to specific hardware and boot configurations, maintaining security integrity throughout the system lifecycle.

SECURE REMOTE UPDATE DRIVERS

Provision-Free Field Update Drivers

- Update OS, kernel, initramfs, and boot configurations remotely without running provisioning processes on protected systems.
- Updates are packaged centrally using a single key and deployed as signed, sealed packages.
- Protected systems receive ready-to-deploy packages – no provisioning infrastructure or tools required locally.
- Automated TPM resealing maintains security without manual intervention.

Hardware-Enforced Rollback Protection

- Systems can only advance to newer versions – TPM monotonic counter prevents downgrade attacks.
- Counter value is embedded in update package and verified before installation.
- Attempting to install older software will fail cryptographic verification.
- Protects against attackers reverting to vulnerable versions with known exploits.

Hardware and Configuration Binding

- Update packages sealed to specific hardware platform and boot configuration.
- Package only installs on authorized systems with matching TPM and Platform Configuration Register (PCR) values.
- Prevents update packages from being used on unauthorized or compromised systems.
- Stolen or leaked update packages cannot be applied to attacker-controlled hardware.

Cryptographically Verified Update Chain

- MMKEK-based packaging ensures update authenticity and confidentiality.
- Digital signatures verified before any installation occurs.
- Update metadata includes version, counter value, target hardware, and boot state requirements.
- Complete audit trail of what was updated, when, and on which systems.

Secure Key Material Handling

- Encryption key never leaves secure provisioning environment.
- Update packages encrypted so contents protected during distribution.
- TPM unseals package decryption keys only after verification of hardware, boot state, and counter value.
- Keys automatically resealed to new measurements after successful update.

Fleet-Wide Deployment at Scale

- Single update package deployed across entire fleet of identical configurations.
- Centralized management — no per-system provisioning required.
- Updates applied automatically on boot after verification.
- Reduces operational burden and eliminates human error in update process.

Maintains Security Posture Through Lifecycle

- Long-lifecycle systems updated without breaking trust chain.
- Security patches deployed without physical access to fielded systems.
- Respond to emerging threats without system recall or depot-level maintenance.
- Critical for tactical edge, forward-deployed, and geographically distributed platforms.

IDEAL USE CASES

Defense and Intelligence: Forward-deployed systems, tactical edge platforms, unmanned systems requiring security updates without physical access.

Long-Lifecycle Platforms: Industrial control systems, mission computers, embedded systems requiring years of security maintenance.

Geographically Distributed Fleets: Systems deployed globally where physical access is impractical or impossible.

High-Assurance Environments: Classified systems, mission-critical platforms with mandatory update integrity and rollback prevention.

Any Application Needing: Remote security updates, protection against downgrade attacks, hardware-bound updates, elimination of local provisioning processes.

TECHNICAL HIGHLIGHTS

Platform: Intel® x86 | TPM 2.0.

Rollback Protection: TPM monotonic counter in non-volatile RAM.

Hardware Binding: Update packages sealed to TPM identity and PCR values.

Updatable Components: OS kernel, initramfs, bootloader configuration, kernel command-line parameters, kernel modules.

Verification: Cryptographic signature validation, counter verification, hardware/configuration matching.

Deployment: Network-based distribution, auto-install on boot.

Resealing: Automatic TPM PCR resealing to new measurements after verified update.

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