Mercury™

EBOOK

Transforming Access Control With Embedded Applications

Physical access control must evolve to support hybrid workplaces, integrate with IoT and deliver faster, more intelligent security. Legacy systems struggle with complexity, limiting integration and increasing risk.

Building Smarter, More Adaptive Access Solutions

The Mercury embedded application environment transforms access control by enabling applications to run directly on Mercury MP Intelligent Controllers. Edge processing minimizes delays, boosts reliability and maintains security even during network disruptions.

This platform bridges existing systems with future technologies, giving OEMs, technology partners and end users the flexibility to build tailored solutions. Scalable customization ensures adaptability for both current demands and future challenges.

Embedded applications transform Mercury MP Controllers into advanced IoT devices, supporting sophisticated local operations. Edge-based decision-making reduces latency and reliance on external systems.

Building a Unified Ecosystem Through Interoperability

Rooted in Mercury's commitment to openness, this platform prioritizes interoperability, enabling seamless integration across controllers, IoT devices, elevators, readers, locks and more.

Flexible APIs streamline development, deployment and management while reducing reliance on proprietary systems. This lowers barriers to scaling, allowing technology partners to adapt solutions as operational needs and technologies evolve — without requiring complete system overhauls. Partners can address diverse challenges, including:

- Lock integration for server cabinets
- Auxiliary authentication for the U.S. government
- Service assurance and cyber hygiene
- Reader management

Consistent architecture fosters long-term flexibility and collaboration, enabling hardware and software developers to align efforts with shifting customer needs. Organizations can expand system functionality over time while preserving operational consistency.

Core Technology Elements

Container

The development environment and runtime definition designedfor app authors

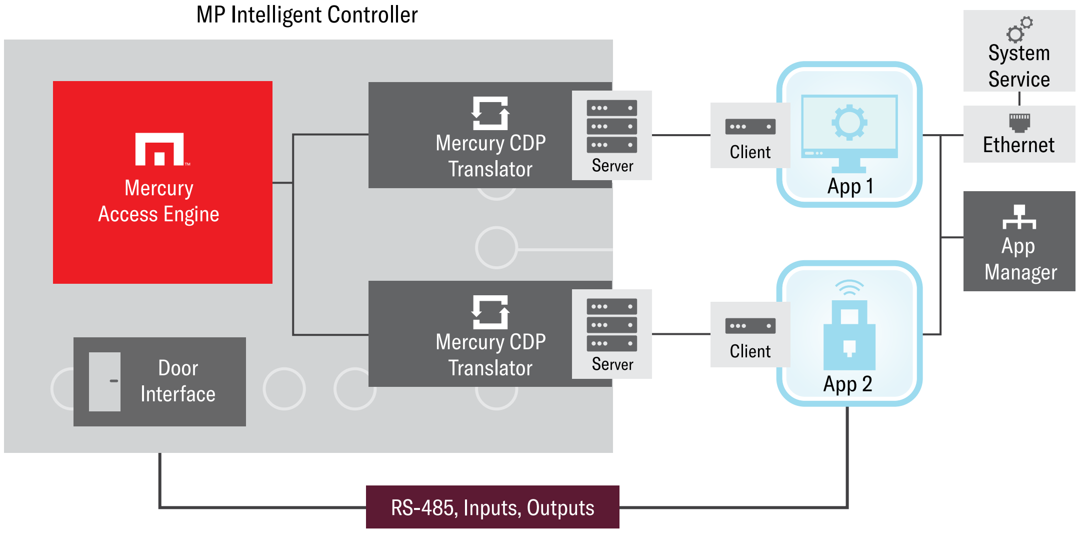
API Framework & SDK

For a given application (device, system, aux auth, or host), APIs are provided to app authors

Licensing and Architecture

Providing the entitlements and licensing system to install and run certified apps

Enabling Architecture



CDP = Common Device Protocol

Driving Real-Time Performance at the Edge

The platform enhances performance consistency and operational resilience by running workloads on the controller, even during network disruptions. This architecture addresses modern security and operational challenges with speed and reliability.

The embedded app supports a hybrid model for maximum adaptability in which edge processing manages real-time operations locally, and cloud- or server-based systems support multi-device management, monitoring and analysis. Edge-based analytics will enable local management of access events, biometric data processing and compliance monitoring.

Scalability Designed for Growth

The Mercury platform supports everything from single-site installations to complex, multi-site operations with seamless connectivity and interoperability. Its flexible architecture enables organizations to expand or reconfigure access control systems as needs evolve — without sacrificing performance.

Software-based functionality provides continuous access to new features, integrations and security updates through digital upgrades, minimizing disruption and reducing the need for costly system overhauls.

Scalability extends to both hardware and software integration. Organizations can add devices and applications incrementally, ensuring growth while preserving past investments. This approach builds a future-ready access control foundation that adapts to changing operational demands.

Expanding Value Across the Ecosystem

The Mercury embedded app environment delivers value for all stakeholders, fostering collaboration and innovation across technology partners, end users and OEMs.

- **Technology partners** integrate solutions with Mercury MP boards, leveraging an extensive OEM network and large install base to reach more users while driving broader adoption of emerging technologies
- **End users** access a wider range of IoT-driven security solutions, benefiting from real-time performance, enhanced reliability and scalable customization
- **OEMs** deploy custom business logic on Mercury MP Controllers, enabling tailored solutions with localized processing for faster decision-making

This connected ecosystem eliminates barriers to innovation, creating a unified platform for scalable, future-ready security solutions.

Invitation to Innovate

A Structured Process to Enhance Security, Value and Trust

Developing and deploying apps within Mercury's ecosystem follows a straightforward, step-by-step process that balances innovation with rigorous security. This structured approach guides developers from concept to deployment, ensuring applications meet strict security standards while delivering advanced functionality. Standards-based coding and verification enforce authenticated functionality, providing seamless integration with core access control features.

At a high level, the steps of this process include:

- **Partnership Request:** Prospective partners submit a proposal detailing their application concept. Mercury evaluates the submission based on their alignment with existing APIs and strategic priorities.
- **Technology Evaluation:** Mercury's development team reviews the application's technical requirements, collaborating with partners to refine functionality and define development timelines
- **Agreement and Development:** Partners sign an agreement and gain access to SDKs, APIs and development tools needed to build and test their applications
- **Testing and Qualification:** Mercury verifies that applications meet performance and security standards, qualifying them for deployment within the ecosystem

Empowering Developers With Modern Tools

The Mercury platform includes an SDK and structured APIs designed for flexibility, scalability and seamless integration across diverse systems. Key APIs include:

- **Host APIs:** Facilitate OEM partner management of core controller functions, such as access logic, event handling and system configuration
- **Device APIs:** Allow direct integration and control of third-party devices, including locksets, sensors, actuators and biometric readers
- **System APIs:** Enable secure, real-time communication with service assurance, cyber hygiene services and other enterprise systems, including databases, identity management platforms and cloud services
- **Auxiliary Authentication APIs:** Support advanced authentication protocols like biometrics, multi-factor authentication and custom credential formats

Mercury's embedded application environment empowers OEMs and technology partners to develop custom applications, integrate IoT technologies and extend edge capabilities, driving new solutions for modern security challenges.

End users benefit from more innovative, responsive access control systems that enhance security, streamline operations and adapt to evolving needs. By enabling tailored solutions and seamless integrations, Mercury invites its partners to innovate while delivering greater efficiency, reliability and long-term value to customers.

Learn how Mercury's new embedded app environment can redefine your access control systems. Visit mercury-security.com to get started.

Mercury Security
11165 Knott Avenue, Suite AB
Cypress, CA 90630
mercury-security.com

part of HID