Three Reasons for Adopting Open Architecture Access Control Solutions

Open, Secure, Connected.

Better make it Merc.

HID®

Paving the way for the future of access control, Mercury Security anticipates the continued growth and adoption of open-architecture solutions throughout 2019 and beyond.

Consultants, integrators and end-user organizations are increasingly demanding industry-leading solutions that are optimized to meet the full range of their evolving technology requirements for access control. Open architecture hardware is the first critical step in making this possible. Additionally, open access control systems are interoperable with widely available hardware platforms, so organizations can utilize a broad range of applications, software, technologies, and solutions from a variety of different manufacturers to achieve best of breed building security. This freedom of choice and flexibility is why organizations are increasingly moving to an open model--the key for ensuring increased ROI, scalability and cybersecurity throughout the lifecycle of their access control system.

Why Open Architecture?

#1. Scalability, flexibility and ease of integration:

Embracing open architecture components at the controller hardware level will enable access control infrastructures to meet both current and future needs within the evolving security industry landscape. This will be especially important for end user organizations seeking to simplify the integration of new access control technologies, elevator control, building automation, IoT applications and third-party solutions into a common platform. An open architecture model makes it possible for end-user organizations to choose from industry-leading access control software providers--both at time of product selection or in the future--should their system requirements change over time. By providing each software partner with access to the same set of development tools, end customers that standardize on open architecture hardware for their access control infrastructure have the freedom to choose the software platform that best fits their needs.

The adoption of mobile and more connected environments is also shifting the role of access control systems and fueling the need for more scalable infrastructures. Access control systems initially aimed at simply securing buildings and doors are moving to serve as the backbone for a range of buildings systems to achieve overall facility security and management. The open model is the lynchpin for easily adopting the latest technologies in access control to meet these constantly changing requirements; it addresses the need to incorporate building automation and other smart building capabilities into a single, streamlined infrastructure as more connected environments become the norm. Access control hardware and solutions built on open standards for interoperability, such as MQTT, PSIA, OSDP and BACnet, will be the first step to ensuring flexibility in future systems. These standards enable extreme flexibility and make it possible to manage disparate systems more efficiently via a single infrastructure.

Increased security and operational efficiency with Open Supervised Device Protocol (OSDP)

- OSDP is an access control communications standard developed by the Security Industry Association to improve interoperability among access control and security products. OSDP is the leading industry protocol that enables secure and open communication between readers and controllers and is widely adopted by many physical security device manufacturers. OSDP also supports IP communications and point-to-point serial interfaces, enabling customers to flexibly enhance system functionality as needs change and new threats emerge. Beyond its security features, OSDP has two main advantages over previous access control communications methods:

1. it is communication protocol (bi-directional, more secure, uses fewer wires, longer range, and multi-drop), and

2. it is extensible offering a multitude of application enhancements (biometric support, high assurance authentication, and interactive display terminals) which enables organizations to proactively add new capabilities through phyiscal access control systems.

Easy building systems integration via BACnet

- The Building Automation Control Network (BACnet) standard is a data communication protocol for building automation and control networks; it enables interoperability between different building systems and devices in building automation and control applications. Open access control hardware supporting BACnet discovery services allows connections to a wide range of BACnet Clients on IP networks performing building control services. This enables access control partners to add access control integration for HVAC, building automation, lighting and other third-party building applications. Eliminating the need to run wires and add relays, making it possible for access and building systems to interact with each other in real time.

The Authentic Mercury open platform delivers quality assurance derived from the most proven and reliable hardware in the industry. Authentic Mercury hardware is designed as an access control platform that easily encompasses emerging technologies, changing industry standards and evolving system environments.

AUTHENTIC MERCURY™

"Access control is becoming more dynamic than ever as new technologies and sophisticated cyber threats compel the industry towards a more forward-looking approach to security,"
Steve Lucas, Vice President of Sales & Marketing, Mercury Security

"Plug-and-play" access control with PSIA compliance

- The Physical Security Interoperability Alliance (PSIA) is a global network of physical security manufacturers and integrators focused on promoting interoperability between access control and other security solutions. The alliance develops open specifications (Profiles) for interoperability of access control components through its Area Control working group. In practice, these open specifications remove the need for security administrators to view each of systems separately. They can manage a singular view of a variety of systems and devices that are integrated via PSIA Area Control open standards.

Connecting more IoT systems and devices with MQTT:

- Machine-to-machine (M2M)/"Internet of Things" connectivity (MQTT) is a protocol for how devices communicate with each other in a more connected environment -- specifically for the Internet of Things. Open access control hardware supporting MQTT enables PACS panels to communicate with third-party systems. An example of using MQTT to create more connected and streamlined experiences is the integration of access control panels into elevator destination dispatch systems that offers tenants and visitors personalized elevator service while improving the flow of building traffic. Instead of pressing traditional up or down buttons, passengers enter their destination floors using keypads or interactive touch screens before entering an elevator. This is one of the many use cases where IoT protocol integration enables a more connected, intelligent building environment.

#2. Cyber security

It is crucial to begin addressing cybersecurity at the hardware level to establish a strong foundation of protection for an access control system. Hardware platforms that focus on a comprehensive approach through security design best practices, latest standards with encryption and communications, and protection of data at rest should be the basis for any physical security implementation. One example of this approach is through standardization of the OSDP protocol developed by SIA. Already in wide use by many leading manufacturers, OSDP provides many benefits including simple line supervision, encryption and authentication, as well as certificate management between devices.

Beyond the hardware, an equally important aspect of cybersecurity is solutions that feature encrypted and secure communications end to end. Software manufacturers should carefully control all possible connection points supported by their applications and partner with best in breed hardware platforms that emphasize cybersecurity as part of the core technology. Additionally, both hardware and software manufacturers should regularly engage the services of professional labs that analyze product cyber strength to foster the continuous improvement over the product lifecycle. It is also critical for end-users to collaborate with their IT teams to establish policies for a multi-layered approach to security that guards against breaches throughout their organizations. This holistic approach – from a security-by-design approach to system hardware employing the latest cyber security standards, to software management and end-user due diligence in identifying and protecting against threats – will establish the strongest line of defense to safeguard organizations.

#3. Increased ROI

The access control industry's move to open standards is cultivating a broad range of interoperable products with enhanced features, advanced security, and greater ability to scale – all of which impact an organization's return on investment (ROI). Increasing ROI is accomplished by lowering the cost of integration and reducing any cost impacts related to system upgrades and migrations. True open architecture systems will integrate with peripheral devices, applications, solutions and enable interoperability with the industry leading software providers. Additionally, an open access control hardware platform with a consistent, ubiquitous API ensures organizations can protect their largest investment in a physical access control system (PACS) while significantly reducing total cost of ownership by eliminating proprietary, customized applications.

Standards-based open architecture also ensures that solutions can be easily upgraded to support changes in technology and applications—without ripping and replacing existing systems. Open hardware provides a streamlined path to move organizations from proprietary and/or obsolete systems to an open, flexible and interoperable platform for systematic access control. It also enables a time efficient, cost effective migration by re-using most of the existing legacy system infrastructure and gives users the confidence that investments in today's technologies can be leveraged in the future.

Organizations will begin to see the pay-off of using cyber-secure, interoperable solutions that leverage the cloud and IoT as customers embrace open hardware as the foundation for their physical access control systems.

Steve Lucas added, "As the importance for access control and security systems comes into sharper focus within organizations, expectations for open architecture and interoperability as well as adherence to cyber security best practices are driving the future requirements for access control. All of these factors have created the perfect climate for a major paradigm shift in the security industry."

About Mercury Security

Mercury Security (www.mercury-security.com), part of HID Global, is the global leader in the supply of OEM access control hardware with the largest installed base of over three million panels sold. With over 26 years in the market, Mercury provides open platform hardware that addresses the full spectrum of access control requirements. This ensures OEM partners, installers and end customers spanning virtually all vertical markets can select from a variety of Authentic Mercury solutions to meet their needs. Mercury's open hardware platform is specifically designed to support the latest technologies, changing industry standards and evolving network environments. This makes it possible for organizations to proactively meet dynamic system requirements, especially as buildings become smarter and more connected. Authentic Mercury hardware significantly reduces total cost of ownership by eliminating the need for heavy customization, thus accelerating system development and implementation.

Better make it Merc.

www.mercury-security.com

2355 Mira Mar Avenue
Long Beach, CA 90815

HID®

In 2017, Mercury was acquired by HID Global®, an ASSA ABLOY Group brand, and a worldwide leader in trusted identity solutions. Customers benefit from a tighter, more seamless integration of intelligent controllers with readers and credentials, as well as from our shared vision for an open, flexible approach to the access control ecosystem.