ONVIF® | Standardizing IP Connectivity for Physical Security

ONVIF Profile A: Bringing New Functionality to Multi-Supplier Access Control

Bob Dolan, ONVIF Technical Services Committee and Director of Technology, Anixter

- **Access control has evolved more slowly due to system longevity and proprietary approach**
- **Profile A levels the playing field for smaller market manufacturers**
- **Standards provide freedom of choice for both software and hardware-related decisions**
- **ONVIF standards co-exist with other standards for a cohesive overall solution**

The need for interoperability, which is making different types of devices or technologies communicate with one another, is certainly nothing new in our industry. At Anixter, we have been testing interoperability in our Infrastructure Solutions LabTM for many years, connecting devices and clients from different suppliers to our test server site to ensure that integrations and multi-supplier solutions are going to work correctly for our customers in real-world scenarios.

Due to the proprietary way that access control security components have historically been designed and manufactured, achieving interoperability between different manufacturers' products hasn't always been easy. It sometimes has involved developing specific device drivers or creating workarounds to get readers, panels and other peripherals to share information and communicate with a common access control management platform.

A New Interface Driving Open Access Control

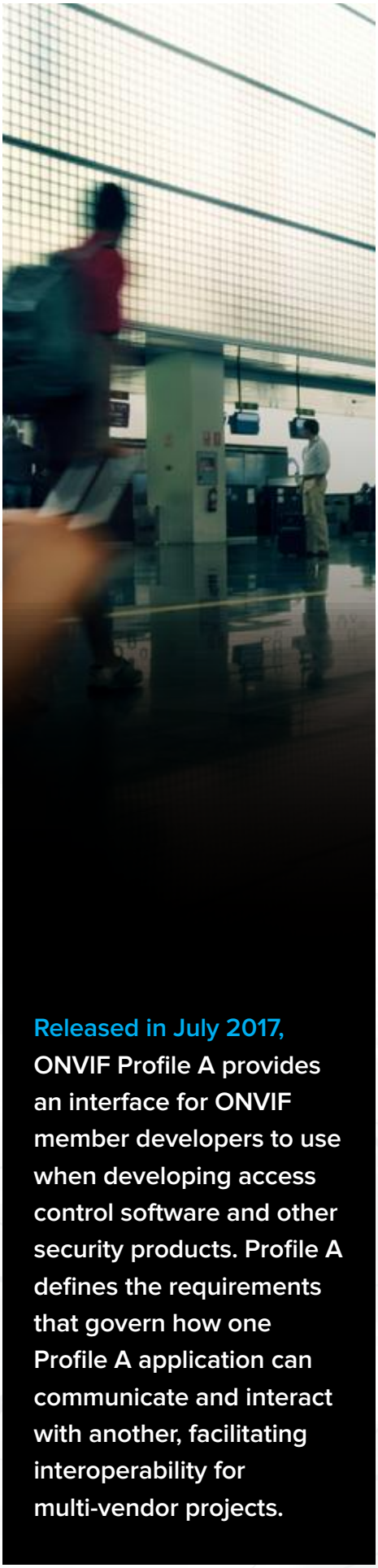
As a result of the proprietary nature of the access control market, customers often have remained confined to deploying single-supplier access control systems and felt forced to buy access control panels from a particular manufacturer in order to maintain their current investments in legacy card readers, door controllers and card technology. But the industry is changing as the development of standards-based applications grows, and end users and system integrators alike are recognizing the value of open standards, such as the interoperability standards created by ONVIF.

Released in July 2017, ONVIF Profile A provides an interface for ONVIF member developers to use when developing access control software and other security products. Profile A defines the requirements that govern how one Profile A application can communicate and interact with another, facilitating interoperability for multi-vendor projects.

The open device driver used in Profile A conformant access control panels allows end users to integrate control panels and management software from different manufacturers. This gives end users the ability to make choices on specific hardware for their access control systems and, even more importantly, means that if you want to install another supplier's access control management software in the future, you don't have to rip and replace existing access control hardware in order to do so. The common interoperability of ONVIF Profile A provides the bridge between the legacy hardware and new software if both are Profile A conformant.

The Tipping Point is Now

In contrast to the video surveillance market, access control technology has historically been slow to change in large part because of the high upfront costs to acquire and install a



Released in July 2017, ONVIF Profile A provides an interface for ONVIF member developers to use when developing access control software and other security products. Profile A defines the requirements that govern how one Profile A application can communicate and interact with another, facilitating interoperability for multi-vendor projects.

system and the longevity of the equipment — commonly between 12 and 20 years. End users and their need for open network-based infrastructures are driving recent changes in this market, as the line between physical security and IT continues to blur. Physical security systems are now often managed by IT departments and IT directors are rightfully demanding open architecture approaches (like IP networks) rather than the proprietary and sometimes duplicative design of traditional security systems.

The drive to an open architecture approach has proliferated across many related industries, and today we see lighting, HVAC and other functions residing on the network as well, offering businesses the option to minimize operating costs and to better control and monitor their facilities. This trend of hosting everything on an IP network clears a path for an Internet of Things, which in many respects is already here.

The network can already transfer pieces of data from one system or device and correlate it with other data in analytics software programs, ultimately providing usable, actionable information to end users, aggregated from such several systems as video, audio, intrusion, voice and other systems. Multiple network-based systems make things like intelligent building automation a reality, delivering costs savings, keeping people and assets safer and using less energy.

Profile A: A High Return on Investment

Middle and smaller market manufacturers will likely find Profile A the most beneficial because Profile A essentially levels the playing field between large and small manufacturers, eliminating the need for proprietary protocols between suppliers for communications between different components of a system. End users can, for example, choose specialized, high-end access controllers and panels from one manufacturer to use with Profile A conformant access control software that is perhaps lesser known, but that provides what the end user needs when it comes to management and reporting.

Another segment of the security market that will benefit from Profile A is the middle market business that is growing and acquiring other smaller companies. As manufacturers continue to adopt Profile A into their products, Profile A conformant access control componentry will mean that a business doesn't have to rip and replace the Profile A conformant access control devices in the facilities that they've acquired. Instead, they can deploy and use their own preferred management software in the newly acquired facilities using existing hardware. This can offer a huge cost savings for businesses.

It's also important to note that Profile A and other access control standards, such as the Security Industry Association's Open Supervised Device Protocol (OSDP) that allows access control readers to interface with control panels or other security management systems, aren't competing with one another, but rather are complementary. ONVIF Profile A and OSDP can coexist within the same access control ecosystem and can both provide benefits. This synergy between ONVIF Profile A and other standard interfaces allows end users to implement technology that is driven by their specific needs, rather than by a single standard or proprietary brand approach.

A Long-Term Commitment to Access Control Interoperability

With the development and release of Profile A, ONVIF is making a long-term commitment to open access control systems in particular. The development of Profile A took two years and the work of many ONVIF member company representatives from all over the world to develop a standard that can take the physical security market into the next decade.

One thing that ONVIF and Anixter have in common is our view that standards are created to be tools that let customers make educated decisions, with the freedom to choose the hardware and software of their choice, regardless of manufacturer. When end users can just think "It works," and move on with their day, that's when we know ONVIF has done a good job in developing a practical solution.