BY RAY COULOMBE

PSIA Primer

While ONVIF has become the de facto standard in video, PSIA is trying to leverage a foothold in access control

As a follow-up to my previous column on ONVIF (www.securityinfowatch.com/12084509), our attention now shifts to another effort to drive system interoperability — the PSIA, short for the Physical Security Interoperability Alliance (www.psialliance.org), which was founded in 2008 by more than 20 companies including Cisco, Honeywell, GE (now UTC) and Tyco. Although neither ONVIF nor PSIA have the power of a true standards-making organization, I believe that either would claim success if their efforts became de-facto standards and widely adopted by both manufacturers and specifiers.

The PSIA has created a security ecosystem, relying on seven complementary specifications, which enable systems and devices to interoperate and exchange information. Three of these — the Service Model; PSIA Common Metadata & Event Model; and the PSIA Common Security Model — provide a framework for functional specifications, including the IP Media Device spec (video), Recording and Content Management spec (storage), Video Analytics spec, and Area Control (access control, intrusion, power management) spec.

Focus on Access

While early on, both organizations focused on video, ONVIF has evolved to have a strong international coalition of companies who, today, are mainly video-centric. The PSIA, on the other hand, has emerged to have access control as its primary focus, embodied in its functional specification for Area Control. Its leadership contends that most of the significant North American PACS (Physical Access Control System) manufacturers are now participating in this effort.

I asked David Bunzel, PSIA Executive Director, about the need for interoperability of access control systems since, unlike cameras, there seems to be less of a requirement for "mix and match" — particularly since many hardware panels can be repurposed with a change in access control software. Bunzel explained that the idea is to provide actionable intelligence coming back to a dashboard from disparate systems, with the ability to share data among systems. This suggests a larger, enterprise focus.

> "Clearly, the industry recognizes that **common physical-logical credentialing** is a necessary component for next-generation access control systems — and the PSIA expects to be a key driver in this regard."

Imagine a scenario where a company grows by merger or acquisition and wants to avoid a forklift replacement or extensive modification of acquired systems. If both the incumbent and the acquired system meet the PSIA specification, the barriers to a lower-cost implementation may be easier to overcome. An integral part of this enterprise scenario is identity management, which PSIA also claims to be addressing.

PLAI: A Step Forward for Identity Management

The PSIA has achieved industry attention in the last year because of its Physical Logical Access Interoperability (PLAI) profile, which is part of its Area Control specification. PLAI is a dynamic identity management protocol, designed to have Lightweight Directory Access Protocol (LDAP) as a single authoritative source for identities using role-based access control (RBAC) — for more on PLAI, please check out an exclusive *SD&I* 1-on-1 interview with Bunzel at www.securityinfowatch.com/12056742.

The National Institute of Standards and Technology (NIST) has mandated that all access occurs through roles, and permissions are connected only to roles, not directly to users (CINCITS 359-2012 is the current standard for RBAC, approved by ANSI in 2012). In IT terms, this is in lieu of Access Control Lists (ACLs), where permissions are assigned to individual users, much like today's physical access control world.

In RBAC, roles can be easily created, changed, or discontinued as the needs of the enterprise evolve, without having to individually update the privileges for every user. NIST lists RBAC's

advantages as: More efficient access control policy maintenance and certification, and provisioning by network and systems administrators — resulting in a reduction in new employee downtime, and enhanced organizational productivity and system security.

Originally intended for the logical domain, using a working standardized framework in the melding of the physical and logical domains makes good sense, as the above benefits could certainly be imparted to the physical world. Clearly, the industry recognizes that common physical-logical credentialing is a necessary component for next-generation access control systems — and the PSIA expects to be a key driver in this regard.

Expansion and Competition

The PSIA is also moving to include areas adjacent to access control, such as power management, an integral part of many access control systems. Vendors Altronix and LifeSafety Power are participants in the initial stage of this effort. Other areas of emerging interest are battery-powered locks and the Internet of Things (IoT).

Additionally, the PSIA interfaces to different systems employ the Representational State Transfer (REST) mechanism, popular for web interface and cloud applications because of its simplicity and ease of implementation. Some would argue that this is a superior approach to ONVIF's use of SOAP, which is more verbose, but adds security and reliability.

So, while ONVIF has dominated the "de facto standards" of IP surveillance video, PSIA has clearly staked its future on access control, the physical-logical evolution of access control and adjacent areas. Unlike ONVIF, we are not yet seeing "PSIA compliance" splashed throughout manufacturers' product literature or websites, and PSIA compliance has not become a key consultant spec item.

Can ONVIF push its advantage into access control, given its broad membership and the increasing integration of video and access? ONVIF approved its access control standard in Dec. 2013. While the push for RBAC is a sensible and worthwhile strategy, time will tell if PSIA compliance becomes ingrained into the industry's psyche.

Next month, I will focus on The Security Industry Association's OSDP interoperability efforts in my next column. ■

» **Ray Coulombe** is Founder and Managing Director of SecuritySpecifiers.com and RepsForSecurity.com. Reach him at ray@SecuritySpecifiers.com, or follow him on Twitter, @RayCoulombe.