



Physical Security Interoperability Alliance

Newsletter

May 2015

PSIA Demonstrates Expanded Feature Set of Physical-Logical Access Interoperability (PLAI) at ISC West 2015

The Physical Security Interoperability Alliance (PSIA) continued to build momentum in its efforts to develop specifications to support interoperability at ISC West 2015. The PSIA hosted a demo that was oversubscribed and featured expanded functionality of the organization's Physical Logical Access Interoperability (PLAI) profile. Building on previous PSIA demos, the ISC West event featured four PACS (Gallagher, Kastle Systems, Lenel, and STANLEY/Pacom), receiving credentials from a trusted source and synchronizing the information across the disparate systems. Additional new features included the use of mobile credentials and role-based identity management.



Capacity crowd at PLAI demo

Allegion provided the mobile credential capability for the demo, showing how an employee or contractor could be on-boarded in an organization and have his or her credentials enabled on a smart phone. "Implementing the PLAI profile in our aptiQmobile™ platform was accomplished in a matter of weeks. Seeing this functionality, with the other PACS systems, demonstrates the potential scope and capabilities of PLAI," said Brad Aikin, the Director of Product Management, for Allegion Electronic Locks Division.

Effective identity management is one of the more critical issues facing security directors today. This has become more complex with large companies relying on contractors to supplement their salaried workforce. Contractors are often on limited-term contracts. Being able to terminate access is essential to having a robust physical security plan. In addition, when companies make acquisitions, they often inherit different and incompatible PACs. PLAI addresses this by providing a common platform that allows different PACs systems to communicate and effectively synchronize identities.

"We became involved with the PSIA because we saw an effective standards-based solution for integration of the various parts of the physical security system. PLAI addresses a critical component-identity management. We not only employ a large number of contractors, but need to provide access for employees at facilities around the world. To

be able to quickly invoke and revoke access privileges will save considerable time and money for Microsoft," said Mike Faddis, a Director at Microsoft Global Security.

Microsoft has committed to include PLAI in its internal security system that will go live later this year. This will offer significant benefits to the company. One of the early benefits will be a means to integrate the security system of Nokia's mobile phone business, which was acquired in 2014. Microsoft not only added 25,000 employees in 50 different locations to its identity management system, but also had to integrate two different PACs systems. PLAI will make this a simple and cost-effective integration, allowing for a robust security operation.

The PLAI profile is part of the PSIA's Access Control Specification 3.0 and can be accessed at <http://www.psialliance.org/documents.html>. Conformance tools are available in beta-test form for PSIA member companies.



PSIA Announces New Working Group Chairs

At the recent PSIA Board meeting in Irvine, CA, members reaffirmed the appointments of two new working group Chairpersons. Ken Larson, President at Z9 Security, was named chairman of the PSIA Systems Working Group. Ken replaces Roger Richter, a long-time supporter and advocate for the open source work of the PSIA, who has moved on to another venture. We thank Roger for all the work he's done with the Systems

group and for his support over the years.

"Ken has made significant contributions to recent PSIA specifications and profiles. His understanding of physical security systems and products and the nuances of technical specification development, will prove invaluable to this role," said David Bunzel, Executive Director of the PSIA.

We also would like to announce the appointment of PSIA PLAI WG chairman Darren Bain, CTO of RightCrowd. Darren takes over for Mohammad Soleimani who was recently elected PSIA Chairman. Mohammad will continue to work closely with Darren and the PLAI work group as they move forward with their profile and test tools.

"We are excited to have Darren on board as the new PSIA PLAI Working Group Chair. He will be a great asset to the team with his extensive experience in transforming software products from conception to successful completion and delivery. I am looking forward to working together with him to continue to move the PLAI initiative forward," said Mohammad Soleimani, PSIA Chairman and Chief Technical Officer of Kastle Systems.



New Systems and Area Control Specs posted on PSIA website

*CSEC, CMEM, and Service Model updated;
PLAI profile part of Area Control 3.0*

This month, the PSIA Systems and Area Control Working Groups released their updated protocols and specifications. Both groups, over the last few months, have been diligently working to revise and enhance these documents.

CSEC, **CMEM**, and the **Service Model** specifications have all been updated to support multiple topologies. Each topology is a combination of Master-Slave vs Peer-to-Peer, and LAN vs Internet. These distinctions:

- Simplify implementation for Peer-to-Peer use cases, because many of the Master-Slave requirements no longer apply to them.
- Increase security requirements for Internet and IoT-style deployments

The event streaming requirements in CMEM have also been simplified to require only a single, XML-based event streaming mechanism. This also makes implementation easier.

The **Area Control 3.0** specification has been updated to:

- Clarify terminology
- Reflect the topologies distinction
- Improve consistency - between events and status, actions and status, and more
- Add the PLAI profile, and resources to support it: roles, card formats
- Increase possibilities to use UUIDs, for PLAI and other future applications.
- Make the resources and actions more closely match typical access control functionality in the industry
- Optimize for IoT applications and extensions

From the Executive Director

One of the impressive characteristics of the PSIA is the valuable support provided by its members. Yes, almost all of them support the PSIA with membership dues, but the contribution in time and talent is as much, if not more, important. Our member companies are enlightened enough to understand that contributions not only enhance their businesses, but also help advance our industry as a whole.



When the PSIA first started, its mission was to develop a common API for cameras. A couple of months into the process, Cisco decided to donate a specification it had been working on, which would address this and save considerable time in developing what ultimately became the PSIA's IP Media Device Spec. Quickly following this was a camera implementation by IQinVision, with the company agreeing to share the sample code, making for a very short and easy integration for other companies.

Later we had valuable technical contributions from Honeywell for our analytics spec, Hikvision for our Recording and Content Management (RaCM) spec, and GE Security for our Common Metadata and Event Model (CMEM) spec.

More recently we have been focused on Area Control. Valuable contributions have been made by Lenel, in access control; Inovonics, in intrusion; Kastle Systems, in identity management; and Allegion, in mobile credentials. Subsequently LifeSafety Power has made important contributions in power management.

While the technical contributions have been critical, we also have relied on strong leadership in the last year from STANLEY Security, ASSA Abloy, and Tyco.

In summary, the success of the PSIA is the result of broad industry efforts, featuring some of the best and brightest minds in security industry, and the support and commitment of the companies they work for. The PSIA wants to recognize and thank these companies for their support and the momentum it has provided for our open standards efforts.

Best regards,

David Bunzel
Executive Director, the PSIA

Be Social with Us!



Help us spread the word about the PSIA by re-tweeting our tweets, following our blog and forwarding this copy of our newsletter to peers you think would be interested in learning more about how the PSIA specifications are building true plug-and-play interoperability throughout the physical security industry and beyond.

About PSIA

The Physical Security Interoperability Alliance is a global consortium of physical security manufacturers and integrators focused on promoting the interoperability of IP-enabled security devices across every segment of the industry. PSIA supports license-free standards and specifications, which are vetted in an open and collaborative manner to the industry as a whole. Specifications are developed through member and industry participation in five active working groups: IP Video, Video Analytics, Recording and Content Management, Area Control and Systems. To date, more than 2100 industry professionals have downloaded PSIA's specifications.

[Visit our website at www.psialliance.org](http://www.psialliance.org)

Physical Security Interoperability Alliance (PSIA)

Debbie Maguire
PSIA Admin
dmaguire@psialliance.org

[Forward email](#)



This email was sent to dmaguire@psialliance.org by dmaguire@psialliance.org | [Update Profile/Email Address](#) | Rapid removal with [SafeUnsubscribe™](#) | [About our service provider](#).



PSIA | 65 Washington St. | #170 | Santa Clara | CA | 95050