Physical Security Interoperability Alliance

Second PLAI White Paper Released- Cybersecurity
PLAI becomes a critical component in fighting cybercrime

The PSIA has released its second in a series of white papers relating to its Physical Logical Access Interoperability (PLAI) specification. PLAI offers a standards-based approach to normalize data and synchronize logical and physical identities and credentials across one or more systems. This white paper discusses an interesting use case, which supports an important aspect of cybersecurity-preventing changes to critical systems unless a person is physically present in a facility.

Particularly challenging in preventing cybercrimes is the fast pace at which security risks are evolving. Protecting networks, computers, programs, and data from damage or unauthorized access requires a combination of continuously advancing technologies, processes, and practices.

PLAI has the ability to address one aspect of this problem by integrating a PACS with a logical system/event consumer which performs verification checks on any combination of credentials, passcodes, or pins, biometrics, and also passes the user's location. Doing so ensures that the individual who is requesting access to perform a high-security task is actually on-site and intends to execute the operation. The ability to perform the additional location verification heightens multi-factor security measures and provides a critical safeguard in the defense against remote or overseas hackers.

High-security PACS integration solutions using PLAI provide a standardized approach for connecting to a logical system/event consumer and boast "3+1" factor authentication checks for:

*   What you have (credentials)
*   What you know (passcode or pin)
*   What you are (biometric, such as fingerprint or iris scan)
*   +1 = Where you are (current location)

As the need for cybersecurity continues to grow, this heightened measure of security to protect critical infrastructure is an important shield to counteract cybercrime.

PLAI is an open standard, which relies on other common industry specification such as Lightweight Directory Access Protocol version 3 (LDAPv3), the widely adopted protocol, to unify logical and physical identities and uses Role-Based Access Control (RBAC) to provide access privileges to PACS at the enterprise level. The benefits of PLAI include significant costs savings on API development, plug-and-play integration without needing custom code solutions, and the ability to minimize custom interface maintenance costs when application software is upgraded.

A white paper for corporate security system integrators related to PLAI's application in cybersecurity has been released and is posted to the following link providing more detail on this use case.

PSIA

Executive Director's letter December 2016

The physical security industry has seen some dramatic changes since the inception of the PSIA in early 2008. At that time a group of 25 industry executives met in Dallas to discuss the possibility of standards to support the security industry. Our initial objective was creating a common API for security cameras. The pioneering efforts of the PSIA influenced the industry and this objective is now a reality with most security cameras having a standards-based API incorporated into their system.

In 2010, the PSIA commenced efforts to support standards for the access control industry. A year later the PSIA's Access Control specification was introduced to the market. Subsequent efforts allowed the introduction of profiles supporting a variety of use cases, with dynamic identity management being addressed by the Physical Logical Access Interoperability (PLAI) spec, which was introduced in 2013.

Since this time PLAI has received a significant amount of attention, both within the PSIA and from the industry. The initial use case focused on how to normalize data and allow disparate PACS systems to synchronize data. Additional use cases were announced to address cybersecurity, building management, visitor management, building automation, and intelligent locking devices.

It is impressive that the vendors have come together to support these standards. We are seeing increased support from integrators and end-users. The PSIA's Integrator Advisory Council (IAC) is now actively educating and advocating standards and PLAI in the market.

2017 will see additional focus on education in the market. The PSIA will be introducing a series of videos to help the customers understand the various use cases of PLAI. We also plan to announce an End User Advisory Council, which will have representation from enterprise customers who recognize the need and value for standards in the market.

In 2017 we expect to see significant momentum for commercial implementations of PLAI in the market. Join us in this important effort!

Best wishes to you in the holiday season!

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
Physical Security Interoperability Alliance (PSIA)

Debbie Maguire
PSIA Admin
dmaguire@psialliance.org