FOR IMMEDIATE RELEASE
September 15, 2014

The Physical Security Interoperability Alliance
Details Milestones Achieved in
Physical Logical Access Interoperability (PLAI) Specification

(SANTA CLARA, CA) The Physical Security Interoperability Alliance (PSIA) today announced it has achieved important new milestones within its Physical Logical Access Interoperability (PLAI) specification less than a year after forming a Working Group to develop it.

PLAI is being designed to enable employee identities and roles defined or revoked in an authoritative logical identity system to automatically propagate to one or more PLAI-compliant physical access control systems (PACS). PLAI synchronizes physical and logical identity management and access control and standardizes functions that typically have required custom programming to achieve. PLAI now can accomplish the following:

- Compatibility with PACS from multiple vendors.
- Enables initial registration of an employee from an authoritative source (IT or HR logical directory) to the PACS.
- Establishes role-based privileges at the authoritative source and propagates this logical privilege data throughout multiple PACS
- Propagates the credential information (both in the form of cards or upcoming mobile credentials) of an employee from one PACS to others, thus supporting enhanced access control at multiple facilities.
- Easily invokes and revokes physical access privileges in multiple PACS.

PLAI asserts roles defined by an authoritative source (HR or IT) so these roles do not need to be redefined in the PACS. The use of a single authoritative source by multiple PLAI-enabled PACS ensures the validity and synchronization of an employee's physical and logical identity data.

"The PLAI Working Group has achieved a great deal of important functionality that adds tremendous value to access control systems," said Mohammad Soleimani, chairman of the PSIA, head of the PLAI Working Group and CTO and executive vice president at Kastle Systems. "By being PLAI-compliant, access control vendors can offer security end users a streamlined, standard means of synchronizing physical and logical identities and their access privileges. The

PSIA is pleased to offer the industry a cost effective, intelligent solution to a perennial challenge."

"Mohammad has been instrumental in taking this from concept to an active working group in a very short time. The PLAI initiative was demonstrated as a proof-of-concept at ISC West earlier this year and now has a very dynamic group of physical security leaders developing implementations that could be rolled out commercially in the near future," said David Bunzel, executive director, the PSIA. "That's a testament to our members and their dedication and the PSIA's focus on solving significant industry issues."

The PLAI Working Group member companies are Allegion, Honeywell, Inovonics, Kastle Systems, Mercury Systems, Microsoft Global Security, STANLEY Security and UTC/Lenel.

###

Special Note: Bunzel, PSIA Chairman Mohammad Soleimani and PSIA Vice Chairman Joshua Jackson will be available for appointments to discuss PLAI capabilities at the annual ASIS conference and exhibits in Atlanta, September 29-October 2. To schedule an appointment, please contact Debbie Maguire, Executive Administrator for the PSIA, at dmaguire@psialliance.org.

# # #

PHYSICAL-LOGICAL IDENTITY INTEROPERABILITY ISSUE BACKGROUNDER

In most businesses, logical employee identities and physical access credentials are managed by two separate departments. The logical security, generally managed by the IT department and or Human Resources, is responsible for assigning "logical" access privileges to employees, such as computer login credentials and network and data access. The physical security department in turn manages the physical access credentials—identity badges and tokens, etc.—employees receive that permit access to various locations, from a data center to a regional or international office.

The Problem: These logical identity management system and the physical access control systems are usually completely separate. Maintaining physical and logical identity security data at two different places leads to gaps in the security model, is operationally inefficient, and provides little hope of securing either one. For example:

- Organizations are challenged to effectively manage employee credentials and limit security risks. This process now typically involves HR defining privileges and transferring this information to the security group, which manually inputs the information needed to issue a credential. With PLAI, this process is performed one time in HR and no longer needs a second data entry step that can introduce errors.

- Until recently, this process involved expensive custom programming, which enabled these systems to automatically share meaningful identity data, such as that an employee in Role X should only have physical access to Facility B. The systems based on such programming are expensive to maintain and upgrade.

- The resulting physical access credential is static and does not easily permit dynamic changes in privileges. This problem is compounded when employees' logical roles change, affecting physical access rights; when they travel to different company locations running different PACS; or they leave the company.

- Another issue is making sure the physical and logical security data are in sync. Maintaining two sets of user data can lead to loopholes in the security model, is inefficient, and increases security risks.

The PSIA's Solution: The PSIA introduced its Physical Logical Access Interoperability (PLAI) specification in 2013. This protocol will provide a means for organizations to transfer and dynamically update relevant employee data and privileges from the "logical" HR system to any Physical Access Control System (PACS) being operated at various company facilities. PLAI is a standards-based specification and leverages the LDAP v3 interface to support a number of logical identity directories, including Active Directory.

Features/Benefits of PLAI

- More efficient onboarding process for employees
- Instantaneous invoking and revoking of security privileges across disparate physical access control systems
- Ability to support logical privileges and physical access in multiple business locations and campuses
- Supports temporary access credentials when employees travel to remote sites. Syncs security access with different physical locations.
- Ability to minimize risk because all logical and physical access privileges are based on a single authoritative source (e.g., it is impossible for a PLAI-compliant PACS to contain two versions of an active employee's name because it is drawing the employee identities from the authoritative IT/HR source.)

The Physical Security Interoperability Alliance (PSIA), incorporated in March 2009, is the world's leading standards body addressing the need for interoperable systems and intelligence/data sharing in the security ecosystem and beyond. The international group has developed seven specifications to date that enable PSIA-compliant systems and products to interoperate on a plug-and-play basis to share information and intelligence. Such interoperability enhances the power of security systems, reduces product development time and lowers end users' total cost of ownership. PSIA members include leading manufacturers,

consultants, integrators and end users committed to the adoption of IP-based standards through a truly democratic standards-setting process.

Contact:
David Bunzel, Executive Director, PSIA, dbunzel@sccg.com
Debbie Maguire, Marketing Coordinator, PSIA, 650-938-6945, dmaguire@psialliance.org