Backgrounder: Physical-Logical Access Interoperability Working Group

The Basics:

- The Physical-Logical Access Interoperability Working Group formed during 2013. It has not yet issued a formal specification.

- Many security end users want to synchronize the identities used by their logical and physical security access control systems but cannot justify the costs of proprietary solutions that require custom programming and disruptive new work flows.

- The Physical-Logical Access Interoperability specification now under development will provide a standard way for enterprises to ensure the logical and physical access privileges associated with an employee's role are always in synch. That synchronicity then makes it much easier and cost effective to create solutions such as confirming an employee is physically present before permitting access to an application or database as well as solutions for easily managing physical and logical access privileges when employees travel.

- Logical and physical identities typically reside in separate and different systems. Employee roles in a company determine their access privileges, or policies, which typically are created and stored in the enterprise network directory. Synchronizing these access privileges between logical directory and physical access control systems involves proprietary, error-prone, time-consuming and expensive manual processes.

- The new PSIA specification will build on standards already used in the logical identity and access management world, including Role-Based Access Control (RBAC-RPE) and Lightweight Directory Access Protocol (LDAP) to enable vendors and users to more easily map logical identities and their role-based privileges to physical identities.

Practical Application

- Easier mapping of logical-physical identities and their privileges would make it cost effective to ensure persons are physically present before allowing them to log into applications and databases, an effective measure against cyber security breaches. It would also streamline management of group privileges. The Access Interoperability group also hopes to extend physical-logical access synchronization to mobile devices used as credentials.

- Security end users could link physical and logical identities without having to build and maintain custom interfaces between physical security and logical systems. The PSIA specification will enable security end users and/or integrators to unify identities cost effectively and without requiring them to restructure physical or logical security ecosystems.

- For more information about use cases for this specification, please visit http://www.psialliance.org/documents/PSIAPhysicalLogicalAccessInteroperability.pdf

Specification Basics

- The PSIA specifications make plug-and-play interoperability possible for systems, applications and devices across and beyond the security ecosystem. All PSIA-compliant systems and devices, from cameras to physical security information management systems, have a common way to describe alarms, events, actions, etc.

- Because all the systems “express” themselves in a common way, it’s easy for the integrator or end user to set up “if-then” triggers in the rules engines usually built into security systems and applications.