For Immediate Release
September 29, 2014

Microsoft Global Security Commits
To Physical-Logical Access & Interoperability Spec
From the Physical Security Interoperability Alliance

Summary: Three years into a substantial Standards and Interoperability effort, Microsoft Global Security is moving to implement the PSIA's PLAI identity specification and announces a new partnership to help implement more efficient management of identities on the physical and logical security continuum.

Three years ago, at the ASIS International security convention in Orlando, FL., Microsoft Global Security did the rounds, visiting standards and interoperability groups to discuss and encourage meaningful progress, as they charted their way to the cloud for Microsoft's physical security technology functions.

Microsoft's CSO Mike Howard is himself involved in a trifecta of industry activities, which includes chairing the International Security Management Association (ISMA) while serving on the Security Industry Association (SIA) Board, and participating in ASIS International activities as a member. Microsoft Global Security's proactive stance of engaging in industry activities is complemented by its overall standards and interoperability activities, such as those with the Physical Security Interoperability Alliance (PSIA), of which it is a board member.

In 2012, acting on his CSO's mandate, Brian Tuskan, Senior Director at Microsoft Global Security, challenged his technology team, led by Mike Faddis, to devise a ten-year technology plan that would move most of the two-dozen security functions to the cloud.

Faddis and his team noted that the significant future growth of IP-based security technologies could be hampered by lack of standards. "That impact," says Faddis, "scales to millions of dollars of inefficiencies if left unattended. Besides encouraging standards and interoperability groups to move forward and also talk to each other, I sent the clear message that in the future, my team would place increasing emphasis on standards and interoperability as part of the purchase decision. Vendors who ignore that advice lay the path for emergent new partnerships to become established and flourish."

The Security Continuum

But linking both the logical and physical environments is not a simple exercise. Many technologies, most proprietary, already exist with differing ways and huge cost at scale, to achieve that goal. Enter the role of standards and interoperability.

The logical *information security* discipline of keeping data confidential, maintaining its integrity and making it available when needed is commonly shortened to "InfoSec." Similarly, *Physical Security* is sometimes referred to as "PhySec." In a simplified sense, one deals with logical or virtual assets of value and the other with managing the risk associated with things physical and tangible such as buildings and people. They have often been stove piped and separate disciplines until more recent times, and there are many opportunities for common interaction between the two.

Ultimately, there is recognition that security controls for things tangible or intangible, such as buildings or data, exist on the same security continuum. Once this is understood, controlling access, to assets physical or logical, can have the same, consistent disciplines applied across the security continuum.

"This is the next frontier," claims Faddis. "Making access interoperable, whether that is access to a building or computer data, and enabling ubiquity of access across the continuum requires partnerships, standards and expert engagement. In my own experience as a practitioner in both the InfoSec and PhySec disciplines, it makes little sense to be burdened with the cost duplication of managing two identities because each end of the security continuum did their own separate thing."

Deon Chatterton, Sr. Manager, Security Technologies and Services at Cisco Systems, has also been a participant in PSIA activities and says, "The advent of the Internet of Things will, of necessity, require a more seamless interoperability between systems, and devices, and manufacturers. I believe that the activities, efforts and results of PSIA thus far will be of great value in helping the physical security industry continue its move toward standards based interoperability. Everyone wins through cooperation with standards."

Last year, a significant investment of time was made by PSIA members to develop a discussion document and strategy that was detailed in a document entitled Physical-Logical Access Interoperability. Mohammad Soleimani, recently elected Chairman of the PSIA and CTO at Kastle Systems, also chaired the working group that subsequently developed the PLAI specification. Soleimani says "The PSIA's intention, right from the outset, was to construct a PLAI specification which was relevant and accessible to anyone in the physical or logical identity space. We paid particular attention to the feedback from end user organizations, who are often struggling with the cost burden of managing several identity structures that do not interoperate."

Now, after several months of workgroup cycles with the PSIA's Physical-Logical Access Interoperability (PLAI) workgroup, a completed specification has been submitted and circulated. Test tools are being built and proof of concept example code being shared.

Plan for Implementation

As Global Security considered how to use its technology budget judiciously to enable PLAI functionality at Microsoft, a business decision by the Corporation to acquire Nokia's phone business, and integrate it with Microsoft had created the need for scale up by adding 25,000 additional identities.

"We know that some of the technology is not yet created that will enable our future functions of security," says Faddis, "so with our roadmap in hand to enhance identity efficiency across the security continuum, we needed to ensure a careful choice of partner for this project. Not only to meet our business and security needs, but also meet the commitment I made to partner with companies who are committed to standards and interoperability." With that in mind Faddis has recently formed a working partnership with RightCrowd Software.

RightCrowd, with its headquarters based in Brisbane, Australia, expanded into the US some time ago with a North American team, and has offices in Seattle, WA. Peter Hill, RightCrowd's CEO says, "We are very pleased to be working with Mike and his team at Microsoft Global Security. Our company's expertise is delivering practical solutions which solve difficult identity integration problems, and we do this across all three HR, Physical and Logical security domains. In Microsoft's case, when we discovered their vision to work with industry using a standards and interoperability platform, we examined the proposition closely and reached the same conclusion, which was that we could contribute and add value from our experience."

PLAI has the opportunity to transform the physical-logical identity landscape. Using LDAP to connect to a logical authoritative source to push relevant directory information to physical access control systems is very powerful. The business efficiency reasons justify the initial reason to invest, and the enhanced and synchronized logical-physical security framework adds powerful new security capabilities.

"Having coordinated capabilities across the security continuum is key," says the PSIA's Executive Director David Bunzel. "The PSIA has been focused on the entire security ecosystem from its inception, and will now define greater and more efficient functionality in the logical and physical security space. We are doing this in a manner that maintains interoperability with previous specifications and builds on the PSIA area control specification. We are also thrilled to have the experience of RightCrowd as a new member applicant, which continues to expand our increasingly diverse constituency."

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