How a Standard Interface Enhances Visitor Management and Physical Access Control System Integrations

A white paper for corporate security system integrators

Mohammad Soleimani,
CTO Kastle Systems and Chairman PSIA
Sept 13 2016

Abstract

This white paper presents the use-case and solution for corporations that are integrating visitor management systems (VMS's) and physical access control systems (PACS's) as an integral part of their strategy for enhanced security across their facility and building perimeter.

In reflection to the state of the world today, the need for higher levels of security is being driven by threats to personnel, property, and company assets. As companies welcome many different types of visitors – business guests, employee relatives, delivery or repair personnel, or potential candidates for hire – on any given day, it is essential that they are processed in a swift, accurate, and courteous manner without compromising the security of the building and staff.

In an effort to handle access of authorized personnel within the organization and to improve security measures, many corporations are using a VMS to check-in/check-out and track visitors. In these corporate settings, integrating the VMS and PACS is essential in sharing visitor information across the facility. Doing so provides appropriate physical access, limits access to restricted areas, offers visitor tracking capabilities through the VMS, and overall assures enhanced security. Integrating these systems also facilitates efficiency in visitor processing and improved visitor service by eliminating the need to manually enter duplicate information in both the VMS and PACS.

Making it possible to integrate these systems with plug-and-play simplicity, the Physical Security Interoperability Alliance (PSIA) provides a standard interface that enables visitor information to be exchanged between the VMS and PACS: the Physical-Logical Access Interoperability (PLAI) specification. This paper describes the PLAI solution, its application and benefits in VMS PACS environments, and demonstrates how one client is implementing PLAI to allow physical access for regular visitors.

Scope of the Problem

In today's world, corporate security is of paramount importance. Most companies have deployed a PACS to manage building entry and door access. While some companies may still rely on employees to escort visitors during their visit and to gain physical access using the employees' credentials, an increasing number of corporations are now using a VMS.

Integrating the VMS and PACS is key for sharing visitor information across the facility and ensuring proper physical access permissions/restrictions; however, doing so presents its own set of challenges. The development of custom code and scripts may be required to bridge different vendor systems application program interfaces (APIs). This in-house development process can be costly to develop and cumbersome to maintain. It also lacks flexibility if one or more of the systems needs to be switched to a different vendor, and scalability in enterprise environments, where multiple PACS's are deployed increasing the cost and complexity of the system.

In other scenarios, where the VMS and PACS are not integrated at all, corporations are challenged with tedious management of disparate systems and need to fill in the gap with added business costs, labor, and operations. The absence of any system integration requires visitor information to be manually entered in both systems, creating work redundancy and potentially increasing visitor registration time. Similarly, when a visitor checks-out, their information must be resolved in both systems requiring duplication of effort.

These challenges common to VMS PACS integrations are overcome by the standardization and flexibility of PLAI enabling corporations to share visitor registration and access permissions between systems and ensure robust corporate security.

How PLAI Enhances VMS PACS Interoperability

PLAI makes it possible to integrate VMS and PACS systems over a well-defined HTTPS REpresentational State Transfer (REST) API and is adaptable when having to add or replace a VMS, PACS, or both. This standard interface is built with extensibility in mind, which makes not only adding features into the specification relatively easy, but also makes it so that users can customize and extend the features of PLAI if necessary.

Figure 1 shows how PLAI is implemented in a VMS-PACS environment to support bidirectional visitor information management over a REST API. In this scenario:

- The VMS is the authoritative source for visitor identities. Each visitor is uniquely identified by a 128-bit universally unique identifier (UUID).
- Visitor information is shared via the PLAI agent (REST client) with the PACS (REST server). Visitor information includes:
    - Name
    - Email address
    - Access rights (roles)
    - Visit duration
    - Credential format and details (i.e., barcode, mobile credential)
- Optionally, visitor information may include:
    - Visitor's company
    - Visitor's contact method
    - Visitor's point of contact
- The PACS (REST server) may also optionally share visitor location data (access grants, etc.) with the VMS.

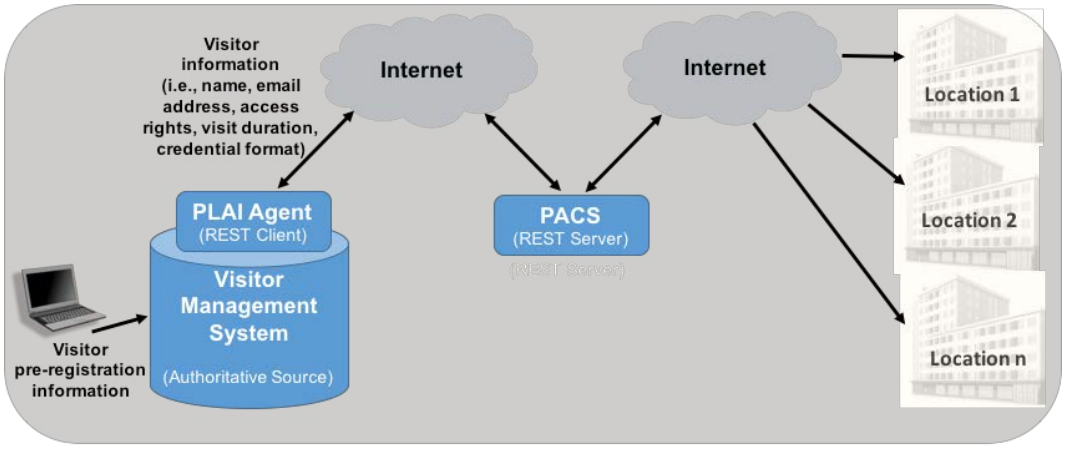

Figure 1. The PLAI agent provides visitor information to the PACS using the PLAI standard interface. Visitor pre-registration information is reconciled with the VMS upon visitor sign-in and access is permitted as configured.

In a VMS PACS implementation, the VMS specifies visitor roles for each visitor. For example,

company "ABC Co" may have roles such as "ABC Co Basic Visitor Access" and "ABC Co VIP Visitor Access." These roles are understood by the PACS to allow physical access to buildings, specific floors, or individual doors; entry is permitted or denied based on the user privileges for that role as provided from the authoritative source.

Additionally, email address information may be used to electronically notify employees upon visitor arrival, and also to send confirmation notices and provide the PACS interface with a method of contact for the visitor.

Solution Benefits

In VMS-PACS environments, PLAI offers benefits such as:

- Clearly-defined specifications for security device communications, which offers significant cost savings on API development and potentially more resources for the development of new features and enhancements.
- Plug-and-play integration, which delivers a streamlined solution in lieu of costly and labor-intensive custom code and scripts.
- Common-event language interoperability, which provides a unified view of security data and the ability to trigger automated responses or alerts in other systems.
- Backwards compatibility, which ensures scalability with compliant devices regardless of version level.
- Robust specifications, which support operating system or application software upgrades with transparency and eliminate custom interface maintenance expenses.[1]

From Concept to Commercial Implementation

More than 65 physical security manufacturers and systems integrators have been involved in advancing standards through the PSIA. Most of the leading access control companies are engaged in the development of the PLAI specification. Their focus is on promoting interoperability of IP-enabled security devices and systems and developing open specifications pertaining to networked physical security technology.[2]

PLAI has been demonstrated at ISC West (April 2016) and extensions to the specification are continually being evaluated within the PSIA PLAI Working Group to enhance its functionality. Other vendors actively involved in the development of PLAI include Tyco, Lenel, Honeywell, Kastle Systems, Stanley Security, and Gallagher.

A recent implementation of the PLAI VMS integration took place between Kastle Systems with Quantum Secure (now a part of HID Global) for the Department of Treasury. In order to facilitate ease of visitor management for employee visitors at the Treasury site hosted by Kastle's PACS, Quantum Secure implemented PLAI and provided VMS services to which Kastle built their API around. In this application, when a visitor in Quantum Secure's system requires access to a Kastle space, Quantum Secure communicates RESTfully to Kastle's PACS, and the visitor is granted entry within the access rights and time constraints that have been granted. Most importantly, this interface was implemented using the standardized PLAI API. Because government organizations at all levels are especially keen on reducing use of non-standard and proprietary APIs, the PLAI implementation was a natural fit.

The Irvine Company also implemented the PLAI VMS solution with Kastle. Irvine maintains stringent operational control of their facilities through sophisticated automation. In this application, when a guest is scheduled to visit an Irvine site managed by Kastle's PACS, Irvine utilizes PLAI to not only provide the basic visitor data, but they also take advantage of PLAI's extensibility to supply Kastle additional data elements such as the visitor's company name, the visitor's contact method, and the visitor's point of contact.

The adoption of the PLAI standard interface across VMS vendors will help to ensure ease of interoperability between systems, as well as successful, scalable, and low-maintenance integrations. Greater system interoperability correlates with gaining the most from security equipment in terms return on financial investment and functionality.

Summary

Stand-alone systems are quickly becoming obsolete as corporations drive the need for disparate systems to work together and technological advancements make it readily possible. Faced with the need to provide a high level of corporate security, maintain visitor service, and preserve corporate image, many companies are deploying a VMS and PACS, and the integration between these systems is becoming prevalent.

The demand for sophisticated security measures and sharing of credential information from one system to another in a seamless fashion depends upon adaptable and scalable interfaces. With PLAI, a flexible VMS-PACS system integration is possible. The PLAI solution offers all the benefits of a standards-based interface and is suitable for the integration needs of today and easily scalable to meet future needs as directed by growth and change.

To become a PSIA member, or for PLAI specification details and other documentation to help meet your integration needs, please visit the PSIA website: http://www.psialliance.org.

References

[1] PSIA Alliance, "Backgrounder: The PSIA Family of Specifications," PSIA Specifications and Documents. Retrieved from http://psialliance.org/SpecificationsOverview.html.

[2] PSIA Alliance, "Organization," PSIA About the Organization. Retrieved from http://www.psialliance.org/org.html.

Mohammad Soleimani *is CTO at Kastle Systems and chairman of PSIA. He may be contacted at msoleimani@kastle.com.*

Appendix – PLAI Specification XML Code Sample

The PLAI XML example that follows represents a visitor. (Note: This sample only shows basic VMS operation; if desired, additional data may be passed according to the PLAI specification.)

```
<CredentialHolderInfo version="1.0" xmlns="urn:psialliance-org"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:psialliance-org ACWG.xsd ">
  <ID>0</ID>
  <UID>{a3e23219-7ba6-42b3-9a9d-4d510cdbb5f9}</UID>
  <Name>Doe, John</Name>
  <GivenName>John</GivenName>
  <Surname>Doe</Surname>
  <State>Active</State>
  <RoleIDList>
       <RoleID ActiveFrom="2016-08-01T08:00:00" ActiveTill="2016-08-
01T15:00:00">
             <GUID>{7a29a7cb-3164-46d8-bc35-f6f78bb593a2}</GUID>
             <Name>ABC Co Visitors</Name>
       </RoleID></RoleIDList>
  <AttributeList>
       <Attribute>

       <Name>/psiaalliance.org/AreaControl.CredentialHolderAttribute/Email</Name
>
             <Value>jdoe@acme.org</Value>
       </Attribute></AttributeList>
</CredentialHolderInfo>
```

Credential information assigned at the VMS is also passed to the PACS for use. These credentials range from legacy 26-bit, 1-dimensional barcodes that are printed at the VMS upon visitor registration, to more modern 2-dimensional barcodes that may be presented on a visitor's smartphone. Because both the credential format and the encoding is passed from the VMS to the PACS via PLAI, these credentials may be used with a hardware-compatible PACS.

The PLAI XML example message that follows would succeed the previous example.

```
<CredentialInfo xmlns="urn:psialliance-org"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:psialliance-org ACWG.xsd ">
       <ID>0</ID>
       <AssignedToID>
             <GUID>{a3e23219-7ba6-42b3-9a9d-4d510cdbb5f9}</GUID>
       </AssignedToID>
       <State>Active</State>
       <ValidFrom>2016-08-01T08:00:00</ValidFrom>
       <ValidTo>2016-08-01T15:00:00</ValidTo>
       <IdentifierInfoList>
             <IdentifierInfo>
                   <Type>Card</Type>
                   <Value>{b97167e5-765b-4145-83a5-3d0697123e50}</Value>
                   <ValueEncoding>String</ValueEncoding>
                   <Format>
                         <Name>128-bit UUID 2D Barcode</Name></Format>
             </IdentifierInfo>
       </IdentifierInfoList>
</CredentialInfo>
```