How a Standard Interface is the Key to Harmonizing Identity Data for a Plug-and-Play Integration Solution

A white paper for corporate security system integrators

Mohammad Soleimani
Kastle Systems
July 2016

Abstract

This white paper presents the use-cases and plug-and-play solution for enterprise and tenant-building environments where expanding corporations are challenged to manage multiple, often disparate logical access control systems, physical access control systems (PACS's), and vendors.

The need to extend corporate headquarters across multiple locations or campuses, or to lease office space in other buildings as a tenant, are typically signs of business success and growth. Integration business drivers may include:

- Company acquisitions or mergers.
- An increase in the number of personnel.
- Derived extensions of products or services.
- A domestic, or even global, need for remote sales offices, manufacturing facilities, and customer service locations.

However, as organizations expand beyond the primary corporate location, they face the task of integrating logical computer-based identities (which control access to the network) with physical identities (which control access to facilities and physical assets) across multiple PACS.

To meet this need, the Physical Security Interoperability Alliance (PSIA) created a specification that enables the harmonization of data across multi-PACS environments using a standard interface: the Physical-Logical Access Interoperability (PLAI) specification. This paper describes the PLAI solution, its application and benefits in multi-PACS environments, and demonstrates how one client implemented PLAI to solve the challenges they encountered in security system integration on a global scale.

A System Integration Problem

In order to unlock the system barriers where seamless sharing of identity and credential data between PACS's is key, corporations are often subject to complex integrations with cumbersome and expensive approaches. Moreover, the departments that manage physical and logical systems within an organization may not be the same, or even in-sync with each other. These divisions make it even more difficult to manage and integrate logical access control systems and PACS's.

Nevertheless, growing businesses must ensure robust corporate security (both physical and logical) as well as employee access to company buildings, office suites, or restricted areas.

To counteract these obstacles, some companies may choose to standardize on a single-vendor. While this approach eliminates the need for heterogeneous interfaces, it lacks the adaptability and scalability for changing security needs and future prospects. Similarly inefficient, the "do-it-yourself" method of integrating the application program interfaces (APIs) in-house is costly to develop and maintain.

These hurdles, common to multi-PACS's integrations, are fully overcome by the normalization of identity and credential information and its data sharing across systems through the PLAI standard interface.

A PLAI Interoperability Solution

PLAI relies on the widely adopted Lightweight Directory Access Protocol version 3 (LDAPv3)

protocol to unify logical and physical identities and uses Role-Based Access Control (RBAC) to provide access privileges to PACS at the enterprise level.[1] PLAI is built with extensibility in mind, which makes not only adding additional features into the specification relatively easy, but also makes it so that users can customize and extend the features of PLAI if needed.

Use Case 1: Enterprise Environment Multi PACS's Integration

Figure 1 shows how PLAI is implemented in a multi-PACS environment to support dynamic identity management and to communicate with each PACS over a well-defined HTTPS REpresentational State Transfer (REST) API.

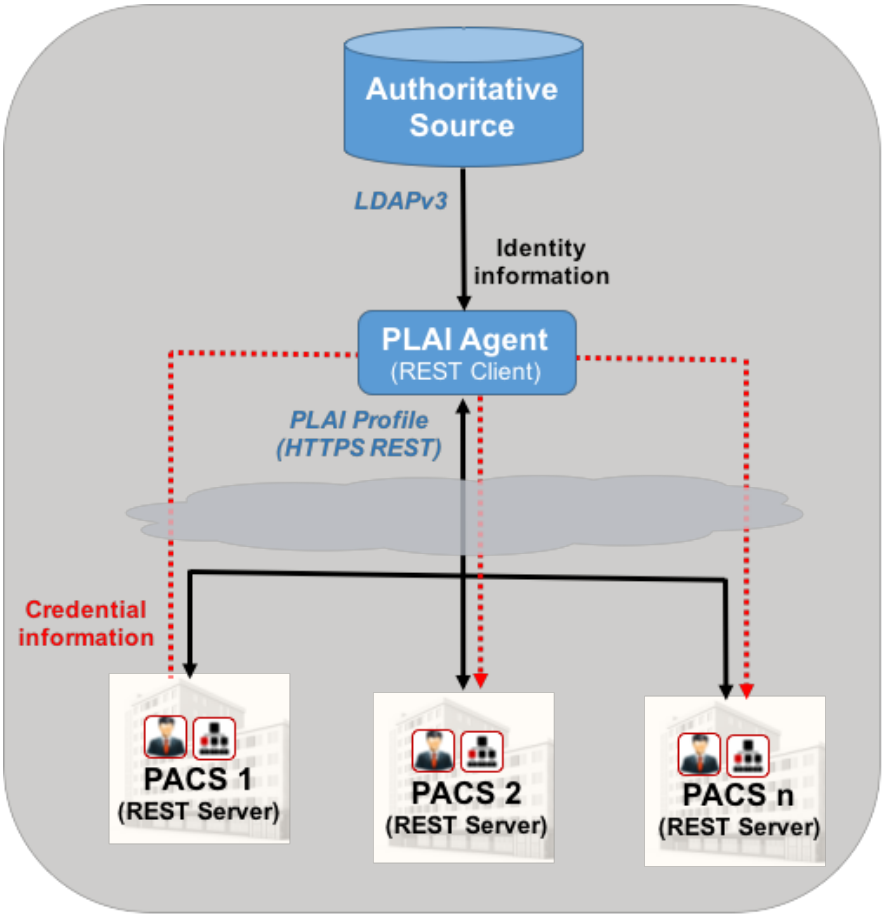

Figure 1. Physical-Logical Access Interoperability (PLAI) provides dynamic identity management and harmonizes data between the logical access control system (authoritative source) and multiple PACS's.

In this scenario, a PLAI agent (REST client) using LDAPv3 provides access to an authoritative source (typically an HR management system, or an IT system such as Microsoft Active Directory) that is populated with each identity uniquely identified by a 128-bit universally unique identifier (UUID):

- First, these IT-assigned identities are passed to each PACS via the PLAI agent.
- Next, an identity is assigned a credential number by the "home" PACS (PACS 1 in this figure) for the credential holder.

- Lastly, the credential number is passed to all other PACS's via the PLAI agent.

The bidirectional flow of credential information allows individual access at the physical level and the identity to be shared across all PLAI-compliant PACS's. Moreover, RBAC allows for mapping logical identities and their privileges to physical identities.[2]

Roles that are already used within the authoritative source, such as a primary employee role (e.g., "IT employee", "HR", or "Executive" role) may be mapped 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 (i.e., access directory group membership).

Use Case 2: Tenant-Building Environment PACS's Integration

The robustness of the PLAI standard interface and the adaptability of this approach in a multi-PACS environment also lends itself as the integration solution in tenant-building, security system management application as shown in Figure 2.

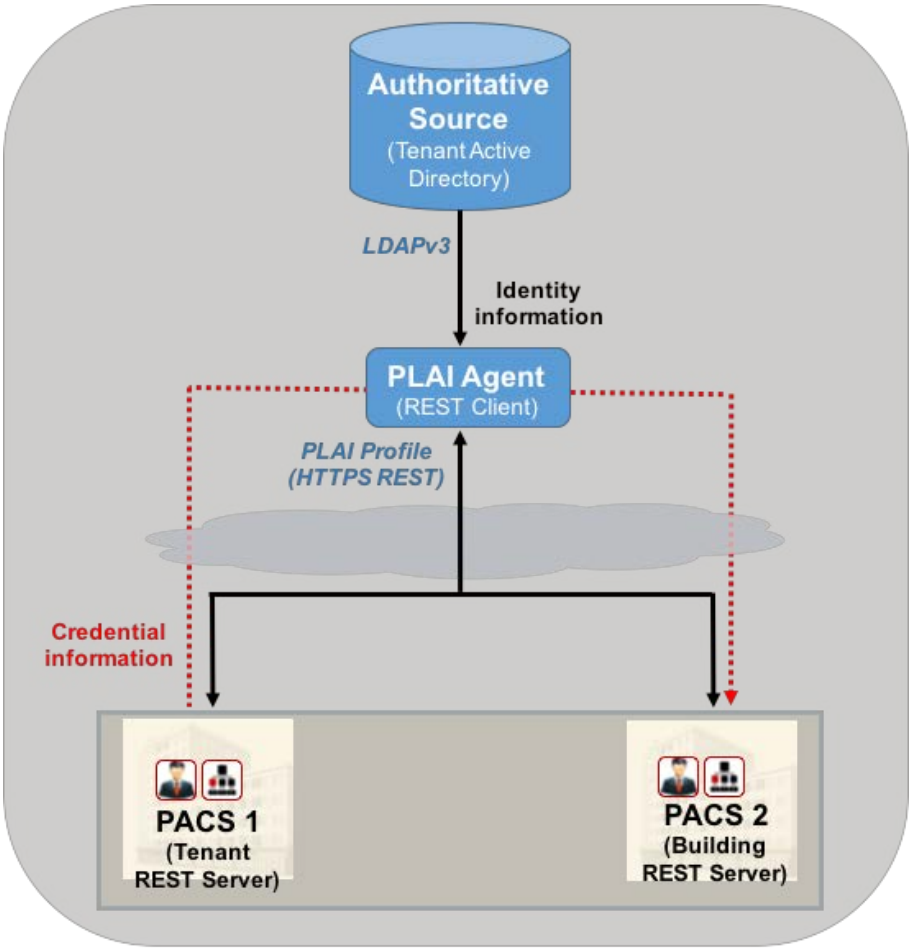

Figure 2. The PLAI agent serves as a bridge between the tenant and building PACS's and synchronizes identities and credentials in applications where a tenant is renting office space in a building.

Where a tenant (PACS 1 in Figure 2) is renting office space from a building (PACS 2 in Figure

2), the PLAI agent serves as the bridge between the PACS of the tenant and building, and provides a way to gracefully synchronize identities and credentials. With PLAI, all of the tenant identities are effectively shared with the building PACS. Doing so enables employee access not only to the tenant rental space, but also to the building perimeter accesses (i.e., exterior entrances, parking garage, and so on).

Provided that both (tenant and building) PACS's are PLAI-compliant, the advantages of the PLAI solution in this application include:

- The tenant maintains their preferred security system and gains building access transparently via PLAI as identities and credentials are passed to the host building PACS.
- The need to manually enter/update/remove tenant information into the host building PACS is eliminated.
- The need to replace the existing tenant PACS is avoided.
- The building is assured the provision of cost-effective perimeter security measures to the tenant through the automation of data synchronization with PLAI.
- The building security is enhanced overall when a tenant employee is terminated and perimeter access is consequently also dynamically revoked.

Solution Benefits

Whereas IT management systems are deploying a logical authoritative source or other trusted source solution, 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.[3]

Implementation Example

Why Microsoft Global Security Pledged a PLAI Implementation

Several organizations are bringing standardization and normalization of data into the enterprise world by implementing the PLAI specification into their environments. One such example is Microsoft Global Security.

Microsoft Global Security, a PSIA board member, has been a participant in the organization's standards and interoperability activities for several years. When Microsoft acquired Nokia's phone business in 2013, they faced the challenge of scaling 25,000 additional identities, which included employees and contractors, across a global company footprint. With this acquisition, Microsoft needed to share identity information from an authoritative source (Active Directory) to the acquired PACS's and guarantee appropriate physical access privileges for traveling employees across various sites.

To ensure uncompromised network and physical access for some 250,000 employees in more than 100 countries, Microsoft Global Security committed to PLAI for seamless identity and credential information sharing. And to help implement PLAI, Microsoft established a working partnership with RightCrowd Software.[4]

Formed in 2004, RightCrowd's mission was to develop software that solved identity integration problems by unifying PACS systems with HR and IT management systems. Currently working with Microsoft to make the PLAI solution standardized across its physical security domain, RightCrowd is utilizing its expertise in systems integration and its ability to harmonize data in multi-PACS environments with PLAI. By doing so, RightCrowd strives to meet Microsoft's needs today and support future industry applications through the PLAI standard interface.

Summary

In an enterprise environment, PLAI leverages identity and credential data sharing across PLAI-compliant PACS's and provides a way to secure identity in a physical security system by standardizing the approach for connecting to an authoritative source. The PLAI solution eliminates the need to manually integrate the authoritative source and PACS or to develop custom software.

Enterprises where the PACS's recognize employee identity across disparate systems gain efficiency in the process of hiring and terminating personnel, and also in revoking access privileges for contract employees with short duration work assignments. In these cases, PLAI also eliminates the need to replace PACS's, or integrate systems through an otherwise laborious process, whether manual or through software development in these applications.[5]

PLAI is the key for harmonizing identity data in multi-PACS environments such as:

- For companies with different PACS vendors (common in business acquisitions or in organizations with regional or international presence), and where employee access to multiple facilities is required, PLAI ensures a plug-and-play integration.
- For a tenant-building application, the PLAI interface offers uncompromised building security at minimal expense and effort.

With PLAI, implementing an integration solution in multi-PACS environments and managing corporate security access needs through the harmonization of data offers a quick, cost-efficient, and scalable approach.

Moving Forward

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.[6]

PLAI has recently 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.

To become a 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, "Physical/Logical Access Interoperability," PSIA Specifications and Documents. Retrieved from http://psialliance.org/documents/PSIAPhysicalLogicalAccessInteroperability.pdf.
[2] M. Soleimani, T. Weil, and E. Coyne, "Behind Closed Doors: Let's PLAI," *IT Professional*, IEEE Computer Society, vol. 17, issue 3. May-June 2015, pp. 64-67.
[3] PSIA Alliance, "Backgrounder: The PSIA Family of Specifications," PSIA Specifications and Documents. Retrieved from http://psialliance.org/SpecificationsOverview.html.
[4] "Managing identities across the security continuum," *Security Buyer*, 31 Oct. 2014. Retrieved from http://www.securitybuyer.com/?p=3629.
[5] P. Rothman, "Examining the Impact of PLAI," *Security InfoWatch*, 7 April 2015. Interview with D. Bunzel, PSIA Executive Director. Retrieved from http://www.securityinfowatch.com/article/12056742/examining-the-impact-of-plai.
[6] 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

Credential Holder XML

The below PLAI specification XML sample shows the structure and parameters for the credential holder information.

```
<?xml version="1.0"?>
<CredentialHolderInfo version="1.0" xmlns="urn:psialliance-org">
  <ID>0</ID>
  <UID>{984bc251-c288-435d-bb13-2123b1590551}</UID>
  <Name>One, AD</Name>
  <GivenName>AD</GivenName>
  <Surname>One</Surname>
  <State>Active</State>
  <RoleIDList>
    <RoleID>
      <GUID>{0750113c-00a6-4c5e-adf2-cced50e3dedd}</GUID>
    </RoleID>
    <RoleID>
      <GUID>{e2730892-2a19-4b90-b904-0fef3801e245}</GUID>
    </RoleID>
    <RoleID>
      <GUID>{7ce118bd-4851-4b3f-b705-bf2e8521a783}</GUID>
    </RoleID>
    <RoleID>
      <GUID>{cdeafdb2-bc11-4cde-9d37-40eefcd77893}</GUID>
    </RoleID>
  </RoleIDList>
  <AttributeList>
    <Attribute>
```

```
      <Name>/psialliance.org/AreaControl.CredentialHolderAttribute/Email</Name>
      <Value>adone@xyz.testing</Value>
    </Attribute>
  </AttributeList>
</CredentialHolderInfo>
```

Metadata Event

The below PLAI metadata event XML sample shows a credential being assigned to a credential holder.

```
<?xml version="1.0" encoding="utf-8"?>

<AreaControlEvent xmlns="urn:psialliance-org">
<MetadataHeader>
       <MetaVersion>1</MetaVersion>
       <MetaID>/psialliance.org/AreaControl.Credential/assigned.assigned/{3ba84fdf-
129a-4ee2-b357-2ef7217e6e0c}</MetaID>
       <MetaSourceID>{661da097-ba20-4416-a465 b33318179235}</MetaSourceID>
       <MetaSourceLocalID>0</MetaSourceLocalID>
       <MetaTime>2015-07-06T03:32:03.757Z</MetaTime>
       <MetaPriority>4</MetaPriority>
</MetadataHeader>
<EventData>
       <CredentialInfoList>
              <CredentialInfo>
                     <ID>0</ID>
                     <UID>{3ba84fdf-129a-4ee2-b357-2ef7217e6e0c}</UID>
                     <SourceUID>{661da097-ba20-4416-a465
                     b33318179235}</SourceUID>
                     <AssignedToID><GUID>{b944c772-5c15-4b9f-94c8-d01c41b0b2dd}</GUID>
</AssignedToID>
                     <State>Active</State>
                     <IdentifierInfoList>
                            <IdentifierInfo>
                                   <Type>Card</Type>
                                   <Value>3</Value>
                                   <ValueEncoding>Decimal</ValueEncoding>
                                  <Format><Name>26 bit</Name></Format>
                                   <CardComponentList>
                                          <IdentifierCardComponentInfo>
                                                 <Type>FacilityCode</Type>
                                                 <Value>123</Value>
                                                 <ValueEncoding>Decimal</ValueEncoding>
                                          </IdentifierCardComponentInfo>
                                          <IdentifierCardComponentInfo>
                                                 <Type>CardNum</Type>
                                                 <Value>3</Value>
                                                 <ValueEncoding>Decimal</ValueEncoding>
                                          </IdentifierCardComponentInfo>
                                   </CardComponentList>
                            </IdentifierInfo>
                     </IdentifierInfoList>
              </CredentialInfo>
       </CredentialInfoList>
</EventData>
</AreaControlEvent>
```