Physical Logical Access Interoperability (PLAI)

Frequently Asked Questions

WHY should I get involved?

&

HOW can I be PLAI compliant?

Updated June 2020

Introduction

The PSIA has been very successful in demonstrating the reality of the standards that we have developed. Through PLAI demonstrations and presentations, the industry has seen how to share identities and credentials across multiple PACS, with concepts like roles and locations also impacting on the access that cardholders have and/or the systems that they can also interact with.

There are a number of key participants at the industry events where PLAI has been presented and these vendors, integrators, consultants, and enterprise customers have a range of questions – from "How does it work?" (in different scenarios), through to "What's in it for me?". The intent of this document is to provide the answers for these questions.

Questions and Responses

1. **How does a PACS vendor become PLAI compliant?**
   a. After implementing PLAI, the PACS vendor must use the test tools associated with the PLAI profile. If the vendor successfully passes the test, a compliance certificate will be sent to the PSIA for review. Once this has been validated, member companies will be able to have their product/company referenced on the PSIA website as being PLAI compliant.

2. **How do I know which PACS are PLAI compliant?**
   a. The PSIA site will reference all products which have passed the test tools and therefore are compliant with the PSIA specifications, including PLAI.

3. **Where can I get access to the PLAI agent?**
   a. Commercial PLAI agents are publicly available from two sources: Cruatech and Johnson Controls. Other vendors may develop PLAI agents and make them available to their customers.

4. **What sort of licensing is involved in having the existing PLAI agent available?**
   a. The PSIA has a downloadable file which has documents providing information needed to develop and test a PLAI adapter.

5. **As a PACS vendor, will customers be demanding that I am PLAI compliant?**
   a. We believe so. PLAI compliance will be necessary to achieve the full benefits of the profile and interoperability with other PACS and other downstream systems. PLAI compliance also has benefits in normalizing data between different systems.

6. **When will PLAI be available?**
   a. It is now…. At https://psialliance.org/all-about-plai/

7. **Where can I find out/read more?**
   a. The PSIA site has information about the specifications and profiles including PLAI. technical information and the specs themselves can be found at this link: https://psialliance.org/legacy-specs/.

8. **What are the benefits for my organization?**
   a. The benefit for an organization in implementing PLAI is to control access to assets physical or logical with the same consistent approach to ensure assets are protected across the enterprise security continuum.

   b. Making access interoperable, whether that is access to a building or computer data, and enabling ubiquity of access across the continuum, allows for cost reduction and efficiencies. It makes sense to remove the cost duplication of managing two identities because each end of the security continuum previously did their own separate thing.

   c. Because the PLAI approach uses standards and interoperability, it means that PLAI can transform the physical-logical identity landscape by using LDAP to connect to a logical authoritative source to push relevant directory information to physical access control systems. Besides being powerful, the resultant business efficiencies justify the reason to invest, and the enhanced and synchronized logical-physical security framework adds powerful new enterprise-wide security capabilities, while removing cost, and simplifying our overall and coordinated identity strategy. In addition, it has significant value in eliminating conflicts in a security ecosystem. There is one trusted source, so duplication of records is unlikely.

9. **What if I have only one PACS?**
   a. PLAI is an interface designed to connect different systems which have a necessity to harmonize some or all of the following information in a secure, network connected environment.
      i. Identity
      ii. Credential
      iii. Streaming location information of a person
      iv. Roles

   Even in a single PACS environment, there are many other systems that can benefit from these information areas. For example, intelligent package management, energy management systems, hoteling systems, and logical access control systems that rely on information from physical location of a person, etc. can all benefit from being connected through PLAI

10. **What if I have multiple PACS and some PACS that are PLAI-compliant but some are not?**
    a. Obviously, those that have PLAI-compliant interface would benefit from easier integration and the ones that do not will have to continue to process the information exchange as they would do today and only be interoperable if custom integrations are implemented.

11. **In a multiple PACS customer scenario, who provides and owns the agent?**
    a. A PLAI agent is based on a set of specifications and any company can build a product which meets these specifications. It is up to customers to acquire the PLAI agent. It could be provided by one of the PACS vendors (for example Johnson Controls or Kastle Systems) or from a third-party vendor (for example Cruatech).

12. **Do I have to use AD as the source of authority?**
    a. Any LDAP v3 interface can be used as a source of authority

13. **Is the AD interface out of the box or is there an integration project required?**
    a. Typically, there is some configuration mapping that is necessary. A well designed PLAI agent would most likely accommodate changes to these configurations settings to take place in one session with the customer.

14. Is there a user interface I have to install and use to make this happen?
   a. The PLAI agent will need to provide a user interface.

15. What business value am I, as a consultant or integrator to the security industry, going to provide to customers by adopting PLAI compliant PACS and this architecture?
   a. Ease of integration and interoperability of various PACS and other systems for the end customer. Significant cost savings with reduced coding requirements, removal of redundant manual data entry of employee records in multiple systems and the benefits of being able to avoid the data in these systems from conflicting in the future.

16. Where can I find out more technical detail about PLAI?
   a. The website provides a host of information on PSIA/PLAI, implementation guides, test tools and other information to assist you. https://psialliance.org/all-about-plai/.

17. Is there an implementation guide for completing the PLAI adaptor?
   a. Yes – this can be found on the PLAI website. https://psialliance.org/all-about-plai/.

18. As a consultant to the industry, is there a PLAI specification available that I can use for my documentation/specification use?
   a. Yes. There is an A&E Specification on the PSIA site. This will provide information which can be included in RFQs and related proposals specifying PLAI in a security environment.

19. What do I need to do to start implementing a PLAI adaptor within my PACS system?
   a. The downloaded file contains the information needed.
   b. Some of the key areas to cover are:
      i. The current specs, and an understanding of the PLAI profile (while PLAI is part of the Area Control spec, it is in the process of being converted to a unique PLAI specification which is expected to be available in July 2018
      ii. Current XSD's
      iii. Development tools and libraries for building a REST web service - e.g. Java, .Net. The adaptor may be implemented outside of the PACS system, in which case the PACS ideally has a suitable API for accessing credentials, holders, events, etc.
      iv. It is worth noting that PLAI imposes certain data storage requirements like UUIDs, so if those properties are not already available within the PACS, the properties may need to be added to the PACS, or, the adaptor needs its own place to store them
   c. See the implementation guide for more detailed instruction

20. How does my IT department need to get involved in implementing PLAI?
   a. The "logical" identity leaders should be involved in the discussion early in the process to make sure that they are aligned with their physical identity team and solution provider.

21. What test tools are available?
   d. PSIA provide a set of PLAI compliance testing tools. Test tools are available to any company, but in order to have a compliant product, you must be a PSIA member.

22. How long does the implementation normally take? For a test system? To be production ready?
   a. Example test system implementation is 4-6 weeks. Production-ready is estimated at an additional 4-6 weeks.

23. **What is the difference between PSIA Standards and SIA Open Supervised Device Protocol (OSDP)?**
    a. OSDP is driving standards between the Physical Access Control System (PACS) and its attached devices. The Physical Security Interoperability Alliance (PSIA) is defining the standards of how to provide roles, personnel, and credentials from an authoritative source which can cross PACS systems. PSIA and OSDP will work very well together in driving open standards which will drive from the management of personnel all the way to the edge devices where OSDP will provide for the ability to have the same device managing the personnel records pushed from the PSIA across disparate PACS manufactures that will protect the edge investment made by customers.

24. **Does my whole access control environment—readers, panels, etc. —need to be PSIA compliant before PLAI will work for us?**
    a. No the PSIA has structured the PLAI specification to integrate with the logical and physical software solutions to allow customers to quickly implement critical functionality that is most important to their organization without having to replace hardware to make PLAI operational. If there is a requirement to use one card across multiple PACS and the card formats are not compatible, the readers may need to be updated or changed to support this.

25. **What about the access level knowledge? How the system will know what particular doors will be granted to access in each Access Control system?**
    a. The management of access control for the particular doors will be managed by each local PACS. The Role properties of the PLAI profile provide the capability for membership of AD groups to be mapped to specific access within a PACS.

26. **What is the business proposition for my company? Sell the PLAI agent, sell a PLAI adaptor component?**
    a. For a PACS vendor, there is the opportunity to offer a customer a product that complies with the PLAI specification. Where a customer requires that their PACS environments comply with PLAI it will be important that your product provides the capability. Even for a customer who has only your PACS product, they may be using PLAI to interface with other systems including Active Directory as a source of truth, or downstream systems that relay on location information etc. It may be that a PACS vendor can also look at an opportunity to sell their PLAI compatible products at an additional premium or as a value-added feature to their PACS.
    b. For a technology vendor, there are a number of opportunities to offer customers PLAI capabilities. Customers may need a PLAI agent, they may need a loosely-coupled PLAI interface built to make their PACS PLAI-compliant, or they may need downstream systems integrated via PLAI

27. **Why would I do this when it seems to dilute my opportunity to expand my PACS within customer sites?**
    a. Customers who have other PACS within their infrastructure may see the cost of a changeover as being prohibitive – therefore other PACS within their environment may not be swapped out in the near future. Equally, it is important that your PACS offer PLAI compatibility to ensure it is maintained as a part of their ongoing infrastructure with other PACS in place. PLAI compatibility also extends the capabilities that your PACS can be a part of with other systems that the customer is looking to use location information or roles for.