



Physical-Logical Access Interoperability

Specification Language

Physical Security Interoperability Alliance
65 Washington Street, Suite 170
Santa Clara, CA 95050
Phone: +1.650-938-6945
Fax: +1.408-516-3950
info@psialliance.org

Background

The PSIA introduced its Physical Logical Access Interoperability (PLAI) specification in 2013. This protocol provides a means for organizations to transfer and dynamically update relevant employee data and privileges from the “logical” HR system to any Physical Access Control System (PACS), often being operated at different company facilities and sometimes disparate systems. PLAI is a standards-based specification which leverages the LDAP v3 interface to support a number of logical identity directories, including Active Directory.

Guidance to Manufacturers and Specifiers:

The language contained on the following pages is intended to be used within the text of an overall access control product specification. This document is not a standalone specification. If being inserted by a specifier in a project specification, the specifier should insure that the intended candidate access control specifications comply with PLAI. A current list of compliant manufacturers may be found at <https://psialliance.org/conforming-products/plai-conformant/>.

Primary Specification Areas (per CSI MasterFormat 2018)

- 28 05 45 Systems Integration and Unified Systems
- 28 10 00 Access Control
 - 28 12 00 Special Requirements for Access Control Systems
 - 28 13 00 Access Control Software and Database Management
 - 28 16 00 Access Control Interfaces
 - 28 17 00 Access Control Identification Management Systems

PART 1 General

1.01 Summary

- A The access control system shall be PLAI compliant, allowing the bidirectional transfer of data between PLAI compliant solutions for the purpose of harmonizing personnel, credentials, and related information.

1.02 Reference Standards

- A PSIA Physical-Logical Access Interoperability (PLAI) Latest Version

1.03 Abbreviations

- A HR – Human Resources
- B IT – Information Technology
- C LDAP – Lightweight Directory Access Protocol
- D PACS – Physical Access Control System
- E PLAI – Physical-Logical Access Interoperability
- F PSIA – Physical Security Interoperability Alliance

1.04 Definitions

- A PLAI - An interface designed to connect different systems that have a necessity to harmonize some or all of the following information in a secure, Internet connected environment:
 1. Identity
 2. Credential
 3. Streaming location information of a person
 4. Roles
- B PLAI Agent – A software agent, based on the PLAI specification, which facilitates the exchange of information among compliant systems.
- C PLAI Adapter– A software integration to products such as Physical Access Control, Biometric, or other system, which normalizes identity data to provide for exchange between disparate systems.

1.05 Qualifications

- A The Manufacturer's PACS product shall have successfully passed PLAI compliance testing and have had such test results reviewed and validated by PSIA. Compliant products will be posted on the PSIA website: <https://psialliance.org/conforming-products/plai-conformant/>

1.06 Submittals

- A PLAI compliance certification documentation
- B Written statement on provisioning of PLAI agent

PART 2 Product

2.01 Interoperability

- A The PACS shall be PLAI compliant and capable of communicating with an authoritative source of data for purposes of drawing employee identity information from that source harmonizing across all PLAI connected systems.
- B The PACS shall have the ability to support logical privileges and physical access in multiple business locations and campuses and to support temporary access credentials when employees travel to remote sites.
- C The PACS shall support instantaneous invoking and revoking of security privileges, both within the system and across every other disparate PACS within the organization which is PLAI compliant.