Physical Security Interoperability Alliance
Minutes: 10/15/2013 – 10/16/13, PLAI Working Group
Meeting Location:
Kastle Systems
6402 Arlington Blvd
Falls Church VA 22044

Attendance:

				Onsite	By Phone
1	Rajeev	Dubey	Brivo	X	
1	Jim	Sheahan	Brivo	X	
2	Brandon	Arcement	HID		X
3	Neelandra	Bhandari	Honeywell		X
4	Jeffrey	Longo	Kastle	X	
4	Mohammad	Soleimani	Kastle	X	
4	Praveen	Jha	Kastle/Global Logic		
5	James	Stroud	Microsoft	X	
5	Shayne	Bates	Microsoft	X	
6	Nick	Woosley	Stanley	X	
6	Josh	Jackson	Stanley	X	
7	Tarik	Hadzik	UTC/Lenel		X
7	Yuri	Novozhenets	UTC/Lenel		X
7	Vijay	Lakamtaju	UTC/Lenel	X	

Mohammad Soleimani (CTO Kastle Systems) reviewed the goals of the Physical-Logical Access Interoperability WG (PLAI), including the four different levels of integration.

- Lowest level, based on LDAP, would be interoperability of an *Identity*
- Second tier is functional *role* integration. The role is defined by IT, the role to permission group is done by PACS.
- Third tier is Mobile Credentials. Standard would remain technology agnostic (Bluetooth 2.0, 4.0, NFC, etc).
- Fourth tier is Dynamic Attributes, where things that are changed real-time can be sent back from a PACS back to LDAP. Example: Don't allow an employee to use WiFi if they haven't even used their credentials and logged into a location via PACS.

We are catching up to ANSI 359 and role based access management (RBAC). Trying to create an industry standard so that we can go across PACS.

ABAC (Attribute based access control) – gives a lot of flexibility, but brings a lot of complexity.

We are going to create a standard and protocol as well, so that it can be tested against.

We have a goal of 6 months to get something out the door.

Group discussed how the “IT” side can really be anything that speaks LDAP v3 – HR, IT, or another

Vijay asked what are we missing by specifying LDAPv3? Mohammad asked for specific examples. Banner (higher end software) was brought up as possible example. Stanley has written custom integration. James (Microsoft) noted that in an open standards-based integration, Banner would simply be a directory and the integration would be via LDAP.

Shayne noted how Microsoft is excited about these standards for IPSec. Vjay noted how if we tie LDAP to physical security, an attack on LDAP could have consequences on the physical security system. However, with the integration, attacks could be mitigated by only allowing access to IT resources when certain physical circumstances permit.

Why the middle tier between the authoritative source and the PACS systems? The middle tier provides a buffer to prevent all location data from overwhelming the authoritative source. Also, there will be a need to synchronize the data between PACS and the source. It also allows for future capabilities such as analytics.

Tarik questioned if an identity can truly come from authoritative source vs. PACS. Some biometrics are attributes of identity and come from PACS. Mohammad noted that there must be harmonization of the identity, which must come from the authoritative source.

Is mobile in the authoritative source, or an attribute in the PACS system? It is imperative that the resulting system allow for interoperability.

Parking lot items for afternoon session:

- PACS originated attributes.
- Who generates mobile credentials? Carriers will want a say – and a price.

Vijay requested scope clarification. Is it any LDAP-based system that we are talking about integrating PACS to? At the base level, we are talking about the syncing of UIDs (Identifiers) – RFC4122 defines UUID. Active Directory uses GUID. UUID is preferable for identifying uniqueness. Which companies support it via LDAP? PIV-I uses GUID/UUID. We want to ensure that we can support at least UUID (128 bit). Oracle’s PeopleSoft LDAP as well.

RFC 4511 defines LDAPv3.

Recommended practice is use UUID. This was specified in the draft document.

The association between the Roles and the permission groups would lie in the PACS. Tarik asked how much of the permission groups should be allowed

Discussed whether or not multiple separate authoritative sources (LDAP databases) would be in scope. If they are not synchronized and are truly independent, then no, that is out of scope for this phase. We need to have only one source of the UUID. Must define specific LDAP queries for scope definition.

CSEC specifications were also included in the draft for device management, including certificate and device ownership. Should we consider Federated AD? LDAP?

Mohammad has proposed PSIA fund a sample implementation development. Anyone that would like to use it are free to use it, or they can make their own and seek certification.

Credentials need to be classified into types:

- Ensure compatibility (with compatible hardware)
- Required identifier types are on portals
- Include mobile identifier
- We need to add a field to identifiers to allow for specification of format (type technology). This would be something like iClass, etc.

ACTION ITEMS

Asks from other groups:

- Area Control Group:
  - Add Roles (without hierarchy currently. Little benefit shown so far in studies)
  - Add Format to Credential/Identifier Type
  - Add extensible attributes, including base attributes such as disability, citizenship, clearance, etc.
- System Group:
  - New CSEC profile
- **Lenel (UTC)** and **Honeywell** will take this on

LDAP v3 Interface

- Subset of protocol: command/response
- **Microsoft** (Shayne) is going to work on getting expertise involved from Microsoft for LDAP. **Stanley** will also contribute.

Complete resource definition for PACS interface. There is a northbound, southbound, and GUI for reconciliation and parameterization– **Kastle** will work on this

Should certain attributes flow down from Authoritative source? Such as citizenship? Safety qualifications? Disability? Other dynamic attributes? Yes – as attributes of person/credentialholder. These attributes would take effect on the permissions. However, these attributes are not required, whereas Roles are required in phase 2 integration.

Wednesdays at 11-12pm: weekly status meeting.


PSIA