Prioritizing Security in the Mergers & Acquisitions Process

A Cost-Effective way to Integrate Disparate PACS Systems

By Glenn Trest-Nokia

Summary

The merging of two companies is a process-laden activity. Critical business functions, sales activities, engineering, and human resources are often the first priorities. Overlooked in M&A activities are the early on requirements for building physical access. The Physical Security Interoperability Alliance (PSIA) provides a standard interface that enables passing of personal data between PACS: the Physical-Logical Access Interoperability (PLAI) specification. This paper describes the PLAI solution and its application and benefits for merging disparate PACS environments during Mergers & Acquisitions (M&A).

This paper reviews the potential cost savings from implementation of PLAI over traditional access control management in a company merger. The case study examined the pre-closing to Day 1 activities. Executives and M&A key stakeholders are treated as visitors during pre-closing. Credentialing beyond the typical visitor process is not needed. Day 1 changes that requirement and the process becomes more complex. Top executives and key players, such as Human Resources, IT, and Corporate Security require access to all facilities by an unencumbered method, usually an issued access card with unrestricted access. Due diligence prior to closing, often overlooks this immediate need, as well as the soon-to-follow requirement to grant all employees access to the merging company's facilities.

Comparing the processes of traditional implementation to PLAI starts with the process required for merger access management. How to grant access is the first activity. Companies must first compare the processes and policies and find commonalities. Differences are analyzed and best practices are implemented. A successful integration requires a common process at all locations. Secondary to the process analysis, is branding requirements. Existing brands are identified and a determination is made if an existing brand is used or a new brand is required. Of course, this is a dependency only if branded identification cards are used.

It is critical to plan during pre-close for this process. Funding for materials, time management, and branding should be considered. Traditionally, corporate security teams consider compatibility of systems from the merging companies and make costly investments in rebadging, dual badging, or rip-and-replace to gain interoperability with access controls. For example, to give access, employees will be issued two badges – one for each company, as they often operate with different software platforms. Duplicate badge numbers, facility codes, or other badge conflicts result in numerous man-hours to support. PLAI eliminates the man-hours and cost associated with these activities by normalizing data allowing data sharing which is now understood between disparate systems.

The Case Study

In 2016, Nokia purchased Alcatel-Lucent and merged the two global telecom companies. The activities for Day 1 were most prevalent in the United States. Nokia relied on a Lenel physical access control system (PACS), where Alcatel-Lucent exclusively used an AMAG PACS. These two systems are not interoperable. It was important to have credentialing available on Day 1 allowing employees from each organization access to the two companies' buildings. Due diligence activities began in advance of the closing and Day 1. Corporate security teams worked to determine the requirements for access sustainability.

The compatibility process began with a PACs system inventory. It was critical to understand the software configurations including system version, patches, and database structure. The first challenge was discovered, with two different physical access control (PACS) software systems at each company– Lenel and AMAG.

The PACs hardware was examined next. The challenge was to determine access compatibility with card readers and access cards. Both companies were using HID Wiegand card readers. However, the card formatting was different. One used a 27 bit card and the other a 35 bit card. To enable the cards on the disparate systems, manual programming was required.

The final step of the due diligence was a thorough examination of the cardholder data within both systems. With employees and external contractor staff, approximately 18,000 cardholder badges existed. These card holders were managed by eight different badging locations. Both companies had established policies for badging in place, but they engaged much different rules for access. One company relied on general access to all locations in North America, while the other relied on "as-needed" access away from the employee's home location.

Data accuracy was very good on both sides, but only one of the companies relied on an authoritative Active Directory to manage the on-boarding and off-boarding activities of the PACs. The company without connectivity to the Active Directory relied on a manual process for on-boarding and off-boarding, coordinated with its HR department.

The system due diligence determined limited options for badging. A decision was made to program both access cards to the opposing systems. Rebranding of the Alcatel-Lucent cards was accomplished by using an adhesive laminate, but programming required manual data input of the 18,000 cardholders. A matrix of criticality was applied to determine the waves of programming, but eventually all cardholders required a level of manual programming.

With no combined authoritative source, Nokia relied on PAC database reliability and/or interaction with cardholders for data. Names, card numbers, and company identification numbers were used for PACs authorization. Nokia experienced data failures which resulted in card conflicts and unauthorized users. This was only remedied with end-user involvement, which leads to concerns about Corporate Security's quality standards.

Cost Analysis of Traditional Implementation verses PLAI

Nokia estimates it spent about $10 USD on new cards, card supplies, and labor hours to reissue access cards and program the access cards to the two systems. The estimated cost was $180,000 USD. There were many hours of labor required to rebrand and reissue access cards, but with the implementation of PLAI, the labor hours would have been greatly reduced, resulting in significant cost reductions. The automation of card holder data transfer and automatic card assignment to a basic level of use would result in a high-quality and transparent implementation of card access with two merging companies. Nokia estimated a cost savings close to 40% or $72,000 USD if PLAI was used.

Summary

The ability for disparate PACs to interface data is critical in Merger and Acquisition scenarios. Automation and digitization of data should be demanded of all PACs to enable uninhibited transfer of data between linked systems. Using one of the PACs, PLAI can recognize the data as authoritative, therefore creating a source of trusted data. PLAI offers many enhancements to the traditional manual entry approach including:

- More efficient onboarding process for employees
- Instantaneous invoking and revoking of security privileges across disparate physical access control systems
- Ability to support logical privileges and physical access in multiple business locations and campuses
- Supports temporary access credentials when employees travel to remote sites. Syncs security access with different physical locations.
- Ability to minimize risk because all logical and physical access privileges are based on a single authoritative source (e.g. it is impossible for a PLAI-compliant PACS to contain two versions of an active employee's name because it is drawing the employee identities from the sole authoritative IT/HR source.)