ISG
Identification Systems Group

Integrated Identity Management

Recommendations for integrating identity management solutions with other applications like access control, HR/SIS and more

White Paper Summary

This white paper covers the issues faced by organizations wanting to improve their identity management systems and the key considerations to note for integrating with other applications.

If you have any questions after reading this white paper, please contact us.

Introduction

In security related publications you will hear about the importance of:

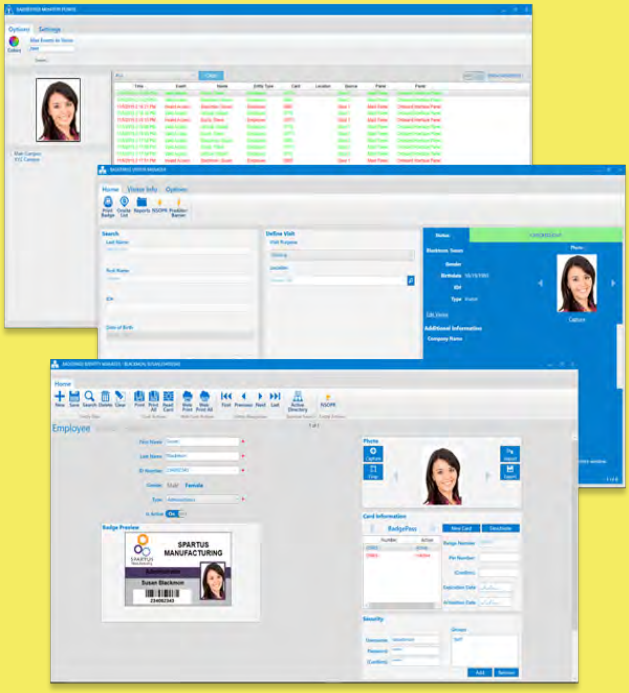
- Convergence of Physical & Logical Security
- Identity & Access Management (IAM)
- Enterprise ID
- Physical Security Information Management (PSIM)
- Logical Access Management Systems (LACS)

We all recognize that in today's world, there is a growing need for increased security. Current trends in identification security include Contactless and Contact Smart Cards, biometrics, vulnerability of information, government and industry group mandates and recommendations, and the convergence of physical and logical security. You need to make the right decisions, but operate within a finite budget.

Most industry experts are saying similar things. A lack of effective identity and access management poses significant risks not only to compliance, but also an organization's overall security.

These risks include:

- **Privilege creep.** Privileges are granted as needed when an employee duties increase, but the access level escalation is not revoked when no longer needed.
- **Credential overflow.** Cards not de-activated when an employee leaves



Why Integrate Physical & Logical Security, a whitepaper by Cisco, John Carney, 2011

This paper describes the importance of integrating physical and logical security under a single governing body or department. A lack of integration creates the following challenges:

- No single system to identify a person's identity because each functional security department controls its own identity database
- Increased potential for theft
- Lack of IT management and application of best practices applied to physical security device, or a lack of best practices applied consistently across departments
- Lack of physical monitoring of logical security devices that can detect tampering; that is, unauthorized access to a logical security device console

Some benefits of integration:

- Provides information on who entered the building
- Eliminates tailgating since the network cannot be accessed without the person swiping his/her badge
- Allows for a more productive work environment by making it easier for the employee to authenticate by using an integrated solution

"In an open, trusting and tech savvy environment, the best access control system may be predicated upon a line to system access. If you failed to badge into the building, you don't get access to the systems. The collateral benefits abound: building management systems, incident awareness, and who is in the affected building."
Edward Erickson, Senior Director of Safety & Security, Cisco

The Value of Converged Access Control, a whitepaper from HID Global, 2014

Truly converged access control consists of one security policy, one credential and one audit log. This approach enables enterprises to:

- Deliver Convenience – Replaces on-time passwords tokens and key fobs, negating the need for users to carry multiple devices.
- Improve Security – Enables strong authentication throughout the IT infrastructure and at the door.
- Reduce Costs – Eliminates the need to invest in multiple access solutions.

The Case for Convergence, a whitepaper from Identiv, 2014

Similarities between PACS and LACS, both systems are based on similar concepts and theories of operation.

1. A high confidence credential. Where authenticating to the door or a desktop, organizations want confidence in the credential being used.
2. Unique identification of individuals. The back-end systems authenticating the users must associate the user credential with the correct user account.
3. Limit access to authorized only individuals. Organizations don't want unauthorized persons wandering around their buildings (PACS) and they don't want them wandering around their network and files either (LACS).
4. Auditing of system activity. The PACS system creates logs in its database, whereas the LACS system does so in the network logs and/or Security Information & Event Management (SIEM) systems.

Issues Faced

Many organizations have a variety of ID and security technologies reside on one credential. Examples are barcode, magnetic stripe, Proximity, and Contactless. They also have a variety of applications that require ID information, including Access Control, Time & Attendance, Parking, Cafeteria, Housing and Active Directory, among others. This can raise many questions and red flags, like:

- Can you issue a credential in one step?
- Will the credential be active in all systems that require identification data? If not, how do you accomplish this?
- How is information shared among security applications?

- Can you coordinate getting information to the various systems and issue the various card technologies like Proximity, Magnetic Stripe and Contactless?
- How do you transition to different card technologies over time without complete card and reader replacement?
- When someone loses their ID credential and needs a replacement, how do you deactivate the old ID and issue a new one, all in one step? The replacement card may have a new Proximity card number, or ID number + Lost Card Code.
- How do you store a photo in your ERP/HR system? Most of these systems have a field for photo; however, it is rarely populated.
- How do you get database information into security applications like Visitor Manager and

avoid the hassle of manual data entry? An example is the list of employees to be seen by visitors.

- Where do you store identity information that is not suited for ERP system, such as Visitors, Guests & Recruits?
- How do you prevent card numbers and serial numbers from being duplicated in your access control system?

Key Points for Identity Management

The key features of Secure Identity Management are:

- A single point of enrollment and ID issuance
- Ability to add data needed for applications to the ID card at time of issuance
- Ability to send data needed for applications to the various systems, such as HR, Network Directory, Door Access Control, Time/Attendance, Parking, Housing, Cafeteria, etc.
- Automatic deactivation of ID in all security systems when it is lost or stolen
- Good communication between various departments, such as HR, Security and IT.

How to Get Started

Creating a plan is not impossible, you just need a team effort.

- Create a list of ID applications you currently have, and those you want to add in the future.
- Create a list of data each application needs.
- Gain buy-in from other departments.
- Speak to various vendors involved.

Below is an example of a list of applications and possible data elements.

Application Databases	Data That May Be Needed for Any App
Human Resources/ Student Information	Name
ID Badging	Photo
Network Directory	ID Number
Door Access Control	Door Access Control Card Number
Time & Attendance	Barcode Number
Parking	Magnetic Stripe Number

Housing	Lost Card Code Number
Cafeterial & Other Payment	Department, Title, Building, Room
	Date of Birth
	Active/Deactive Flag

Security Identity Platform

Unlike other expensive and complex identity management solutions, the BadgePass Secure Identity Platform from Identification Systems Group is reasonably priced and easy to understand. Identity management data is stored in a powerful SQL database. The provided synchronization tools and powerful event notification service allow for realtime or scheduled messaging and cross-platform communication, creating a world where one identity works with many applications. The Active Directory Plug-In™ provides the ability to synchronize BadgePass entities with your exiting Active Directory™ Users.

Issuance of ID Credentials

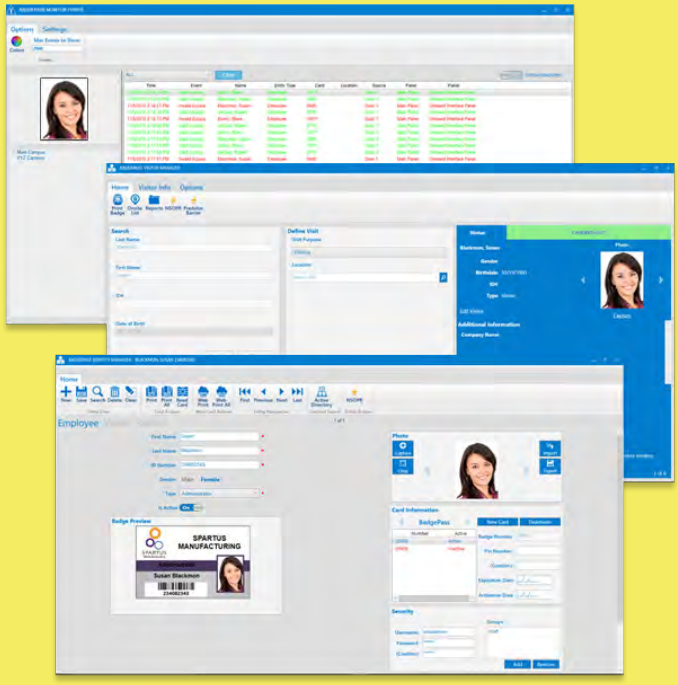
We all understand the importance of recognizing members of the team and identifying visitors and guests. To take ID security to the next level, credentials must be ready to use when issued. That means the various card technologies must be read (e.g. Proximity or Contactless Number) and written (bar-code, magnetic stripe, contactless) during the issuance process. The resulting data is sent to the needed databases.

Card issuance systems from Identification Systems Group automate the credential issuance process and will revolutionize the way you think of secure identity.

Contactless Card Technology

The world is moving to Contactless Card technology, and for good reason. However, there are a wide variety of card products to choose, and some can be very expensive. What is best for you?

The ISG offers a variety of proven contactless card technologies from premiere card manufacturers, including popular brands such as HID and Identiv. Discussion of your specific needs with your local ISG dealer would be recommended to be certain that you are able to get the exact cards for your current and future needs.



Benefits

The benefits of enacting a solid game plan are strong, yet simple.

- Greatly improved security
- Increased efficiency
- Affordability

Considerations

Some of the topics of discussion when considering a system include:

√ **Cost.** Does the cost justify the benefit?

√ **Card Technology.** What card do you want and need?

√ **Card Durability.** If you invest in a technology card, you want it to stand the test of time. What features and options should you consider to ensure it lasts?

√ **Security of system, data and supplies.**

√ **Use of Biometrics.** Adding a second factor, such as biometrics, to certain high security areas (IT, Research Lab, etc) can greatly increase your organization's security.

√ **Logical Access.** Do you want to use your credential to log-on to workstations?

√ **Public Key Infrastructure (PKI).** When considering PKI, storing the digital certificate on a Contact Smart Card is usually recommended, as it provides for portability.

About the Author

Tom Stiles is the Executive Director of the Identification Systems Group (ISG), which is an association of 30 identification solutions dealers serving across the US and Canada. He has served in various aspects of the ID and security industries for more than 40 years.

About the ISG

The Identification Systems Group (ISG) is a nationwide network of local experts in identification, security, tracking and card personalization technologies, providing high quality, cost-effective solutions backed by local support and the strength of our Professional Services Certification program. Each member company works together to provide seamless support and collaboration in the identification and issuance industries across the USA and Canada.

Identification Systems Group
888-964-6482
info@identificationsystemsgroup.com
www.identificationsystemsgroup.com

Your Local ISG Dealer