WHITE PAPER

How to Connect Business Systems: A Breakdown of the First 5 Critical Steps

CONNECT ACCESS CONTROL, SECURE PRINT AND OTHER KEY SYSTEMS FOR BETTER AND MORE SECURE USER EXPERIENCES

The Connected Workplace
The Connected Workplace allows employers to verify an employee's identity once, and then grant access to multiple systems—leaving these trusted identities free to seamlessly access disparate systems. This cross-platform, identity aware understanding makes access more convenient and more secure.

Trusted Identity
A validated identity using biometrics or a credential provisioned onto a card, mobile or a wearable device

Years ago, the ability to use a credential like a smart card to gain access to a building was revolutionary. Today, credentials have evolved, allowing people to use their trusted identities to enter buildings, accurately record time & attendance, print securely and more—creating an ecosystem we call the Connected Workplace.

Organizations benefit from the increased convenience and security offered by connecting multiple systems and identities. Their employees enjoy faster movement throughout a building, the use of flexible workspaces, and the ease of cashless cafeterias and vending machines. This rise of the Connected Workplace has left many business systems manufacturers faced with an increasing number of requests for identity aware systems—but where to begin?

This white paper outlines the critical first five steps to making business systems identity aware, laying a clear and simple path for manufacturers to provide the best products and services to their customers. You'll discover key questions to ask and the most important considerations for ensuring the smooth installation and adoption of identity verification devices into business systems.

The number of identity aware systems has proliferated in recent years. Popular ways to expand the usage of identity cards include:

Time & Attendance
Clock in and out swiftly and securely while preventing "buddy punching"

Secure Printing
Securely print documents on demand to reduce cost and improve data security

Elevator/ Turnstile Control
Access restricted areas and reduce wait times

Parking Management
Quickly enter and exit parking facilities and grant access to visitors

Authenticate Network Users
Log on and off at flexible work stations, simplifying collaboration and movement with added security

Manage Meeting Rooms
Grant or revoke access to meeting rooms for visitors and staff

Step One: Evaluate current organizational needs and infrastructure

A thorough investigation of an organization's current capabilities is a vital first step. The ideal solution works seamlessly within a current system, without major overhauls or retrofitting. It's even better if identity aware solutions can be built into an organization's infrastructure from the beginning. When evaluating the current infrastructure, take care to consider:

Current trusted identity capabilities. How are current trusted identities used and managed? Readers access a database each time they are used, but organizations have different policies about which applications can connect to which databases. You may need to work with a customer's security officer to determine whether your business system will access one central database or if a new one must be created. Another option is to have users self-register, eventually creating a completely new database themselves. Identity aware solutions like HID's Seos® allow access to multiple applications using one card.

Available real estate for new readers. Is there enough space? Cards or biometrics need readers to validate identity. Consider how much physical space there is for the reader, how it will be mounted, and whether it can be inside or outside a device. For example, a printer may have room internally for a reader or chipset or may need a reader to sit as a separate unit nearby.

Connectivity. How will the reader communicate with the database? Each reader will authenticate a card, extract the control data and share that data with the unit being utilized. How will this communication occur, and what level of security does the communication need? What kind of hardware, software and communication protocols are needed? The popular choices today use USB, UART (Universal Asynchronous Receiver-Transmitter), Wiegand for connectivity and CCID (Chip Card Interface Device) and KBW (Keyboard Wedge) protocols for data transfer.

Materials used to house equipment. What space is available inside the device and/or the surrounding environment? Smart card technology works best in a free-air environment, without any additional housing to potentially block communication. If readers must be contained, plastic allows signals to pass through much more easily than metal. Custom retrofitting is possible but may limit performance. For biometrics, the enclosure materials matter less.

Step Two: Identify the desired user experience

Organizations expect technology to work conveniently *and* securely. Take the time to determine what employees and employers really need in order to provide the best solution. Common considerations include:

Speed. How quickly does a reader need to confirm identity? It depends on the use case. Extremely secure areas may need additional layers of verification, like full insertion of a card in addition to a fingerprint scan via biometric authenticator. In less secure and highly trafficked areas, like a lobby, employees may need to quickly pass through turnstiles and flash cards, use mobile phones from a short distance or tap wearables briefly as they go.

Read range. How close does the card have to be to the reader for each use case? Readers can verify cards or devices from a variety of distances, with varying levels of security. For example, some readers are designed to pick up employee locations as long as employees carry their credential somewhere on their person, eliminating the need to present an ID. Readers in highly secure areas may require a card to be inserted for a few moments while layers of data are transferred. Note that read range is often more about perception than reality—an employee may be impressed when granted access the second he touches his phone to the reader, but in reality, that reader picked up his phone's signal and began verification when he was several feet away.

IT administrator experience. Does the customer's organization have a robust and experienced IT team? Smaller companies may not have the manpower to create and manage new databases or install new chipsets. Larger companies may require remote update configuration, allowing them to update thousands of readers without sending thousands of techs into the field.

Step Three: Identify and access the current technology

Technology is constantly evolving, so its evaluation should include current capabilities as well as future plans. Since the goal is to work with what an organization is already using as much as possible, identity aware systems need to have future planning built into current models. Mobile access is particularly key—even if a company is not currently using mobile devices as a means for authentication, they likely will be soon. Most organizations use combinations of these common technologies:

RFID. Radio Frequency Identification is commonly used for cards and wearables, and is the most predominate and wide-ranging security option.

NFC. Near Field Communication supports access control for cards, mobile and wearables.

Mobile Access
With mobile access, an employee's smartphone or smartwatch becomes the gate key. By enabling access to systems and facilities through mobile devices, organizations are ensuring high levels of both security and convenience.

BLE. Bluetooth Low Energy is most often used for location and condition monitoring and is accessed by mobile and wearable devices.

Biometrics. Despite its complex integration, this is the most secure—and often the most convenient—option, with nothing to carry or wear.

Step Four: Determine the best reader form factor for the application

Identity aware systems vary greatly in levels of complexity, and organizations vary greatly in levels of capability. It's best to discuss technical abilities with the engineering manager or outsourced resource to determine whether a DIY or turnkey option is best.

Reader options include:

Reader chipset. A chipset or Secure Element (SE) processor is the least common denominator of all identity aware products and is part of every reader. Organizations with experienced tech teams design the Printed Circuit Boards (PCBs) for a business system to include the reader chipset. Biometric authentication is not supported in a reader chipset.

Reader core. This combination of chips and core components enables a reader (but not the antennas) to communicate over RFID, BLE, etc., but does not support biometrics. Reader core is preferred by manufacturers who want to design their custom antenna to fit with the available real estate.

Reader module. The reader module includes the chipset and antennas but must be housed inside the existing business system. Card and biometrics reader modules can be seamlessly integrated to make the system identity aware.

Desktop reader. This is an entirely separate piece usually placed on a desktop or mounted on the existing device. Desktop readers like HID Global's Omnikey® are nearly turnkey and require very little technical knowledge, but they do take up more space.

Step Five: Designing and integrating the reader with current devices

The most important thing to ensure throughout the selection and integration process is that the current device—the printer, elevator kiosk or timeclock working with the new reader—maintains its functionality. The new identity aware system should add convenience, not complexity. Some things to consider:

Backend communication. The database, reader and access card must understand each other.

Aesthetics. Ideally, the reader will appear to be part of the existing device, not haphazardly attached or awkwardly retrofitted.

Testing and ongoing support. Development toolkits come with test cards for a variety of systems, allowing administrators to check the system's user experience before going live. HID Global also offers continued support for OEMs, integrators and direct consumers through our Extended Access Technologies (EAT) portfolio of Professional Services.

Conclusion

Build on Today's Infrastructure for Tomorrow's Needs

The ability to use one trusted identity in multiple ways is convenient and user friendly. It also results in significant cost and frustration savings over the long term, including reducing human error. Best of all, integrating formerly disparate systems doesn't have to mean a total technology overhaul—the Connected Workplace can be built on existing infrastructure, paid as you go, and tailored to an organization's needs.

HID Global offers a diverse portfolio of readers and cards for every industry, with support and service at each step. For more information on the benefits of an identity aware business system, read our executive brief, *Experiencing the Connected Workplace*, click here, or visit our website.

2019-03-16-hid-eat-make-bus-syst-id-aware-wp-en

PLT-04344