Top Questions to Ask When Investing in Wireless Locking and Access Control

BY JEFF CAHILL

Much has been made over the last decade about wireless locks and the effort by lock manufacturers to bring access control to the countless number of interior doors in a facility. However, many options available today offer wireless in name only; many costly wires are still required to power and connect wireless access points to make a lock wireless at the door.

Most facilities managers would agree that brass key control issues cause poor security and expensive rekeys due to lost, stolen, or duplicated keys, and these issues are more prevalent than ever. There are now thousands of 3D key printing kiosks in most hardware retail chains so that almost any key can be duplicated without authorization. Fortunately, a number of access control locking products are appearing on the market to combat the weaknesses of these traditional lock and key systems. The challenge for security managers is how to choose from a wide range of products and features that may seem confusing to security decision-makers when choosing a smart lock or wireless access system.

The most common dilemma and mistake in the decision-making process is deciding access control functionality—controlling user's time of access, getting audit trails, and immediate "e-rekey"—needed on interior doors, then keeping the existing key system because extending perimeter door access control systems to interior doors is cost prohibitive. Now, some cost-effective options may integrate with the expensive perimeter door system. Currently, virtually all users carry three credentials: an access card, a key, and a phone. Organizations which decide to do nothing will still have poor, outdated key control, and users will still carry three credentials. Organizations which choose affordable access control/smart locking systems can decrease the number of needed credentials and eliminate poor key control without affecting the perimeter access control systems.

The following questions should serve as a guideline for asking the right questions when investigating potential wireless locking solutions:

Is the wireless lock ANSI Grade 1 rated?

ANSI Grade 1 is the standard for any commercial, industrial, or institutional facility in the United States today. It makes no sense to invest in a product that features access control functionality, then install a low-cost smart lock that is easily defeated by simple picking or other vulnerabilities. Decision-makers should insist on Grade 1 protection as a starting point when developing the requirements for a new wireless system. Important features to consider related to this question of quality are:

- High security keyway for emergency key over-ride
- High security cylinders or pick-resistant pin segments in a 6- or 7-pin cylinder
- A clutch mechanism lever or other attack-resistant lever handle.

Will the wireless lock report tampering and key override?

Just like on-line electronic access control solutions, wireless locks are only as secure as the brass key override included with them. Understanding whether a wireless lock has a method of reporting tampering such as

entrance by a mechanical key, picking, etc., should be an important factor in any purchasing decision. For life safety reasons and protection against electronic failure, key override is an important feature. However, keys should not be used or distributed except in an emergency. Otherwise, security is no greater than a standard pin-tumbler lock system and compromises the security of any wireless lock. Decision-makers should make sure that the system can provide an audit trail by detecting each time the lock/door was accessed.

How secure is the credential?

Many card technologies that were available just a few years ago can easily be duplicated today. Decision-makers should ensure that the wireless lock system uses a credential technology that has not been hacked. This consideration may be the most important and yet least considered part of this list. Virtually all credentials can be hacked with a $30 equipment purchased on-line. Better choices are DESfire EV2, 3 or SEOS® credential technologies with multiple layers of encryption instead of easily hacked legacy credentials such as Mifare®, Mifare Classic®, HID standard prox, or iCLASS®.

How many communication protocols does the wireless lock use?

Most wireless locks can communicate via Bluetooth, RFID, Wi-Fi, or some other wireless protocol. Decision-makers should choose a system that only utilizes Bluetooth as a mobile credential. Mobile phones are typically a personal device of an employee who may deny use of their phone as a corporate credential, so secure RFID credentials—cards, fobs, etc.—should be provided as an option for such employees. Adding biometric access or PIN codes for dual authentication may be an added-cost option for consideration in higher security areas. For security reasons, PIN codes should be avoided as a single authorization device.

How is information retrieved from the wireless lock?

Understanding how to update wireless locks with new information and retrieve activity logs and audit trail information is a critical question to answer when considering a wireless lock deployment. Many wireless locks today require a heavy infrastructure investment in order to interact with them; some claim to be able to leverage the existing Wi-Fi network in a facility. The key here is understanding how often users can communicate and what is required in order to capture data that resides in the lock. Decision-makers should always ask: does data capture require traveling to the lock and, if so, will this "sneaker-net" option meet campus requirements? In addition, understanding if there are other options to communicate to the locks on demand—Mobile Credentials, Wi-Fi, Bluetooth Low Energy (BLE) bridges, Data-on-Card, etc.—and the cost of this added connectivity will be important in any final decision around a wireless lock investment.

continued on next page

PHOTO COURTESY PROXESS

What is the future capability of the wireless lock?

When technology advances so quickly, future proofing any investment made in wireless locks may prove challenging. So, understanding if there is any current or future capability of turning the off-line or wireless locks into on-line doors for real-time communication will be critically important. Asking if online doors are required and if they are compatible with the wireless locking system are important questions to get answered as part of the decision-making process.

Will the wireless lock work on all major door applications?

Every facility is unique, but most door openings and locking systems in any facility fall into four major categories: cylindrical, mortise, panic, and storefront. Any wireless lock solution being considered should have an effective and thorough way of addressing each of these types of applications. This capability is not always a given, so decision-makers should research these applications, especially when retrofitting existing openings to ensure a successful implementation. Any required auxiliary locks, such as gates, padlocks, cabinets locks, etc., should also be considered.

Is the wireless lock system scalable?

Many wireless locking systems are limited as to the number of users and the number of locks available, so the selected system should be scalable to campus needs. Decision-makers need to understand how the management software works and how easily doors and users can be added, changed, or deleted. Decision-makers should ask what fees may or may not be associated with adding additional locks and users over time before making a decision that has future ramifications.

How does the wireless lock consume power?

One of the limitations of a wireless locking system is power consumption. Wireless systems typically require battery-operated locks, and systems vary wildly in how power is consumed, affecting battery life and the frequency at which batteries need to be changed. Understanding cycle testing results and how often the batteries will need to be changed is important in decision making because this schedule can translate to added labor costs. For instance, Wi-Fi can talk to more devices in a system but typically uses up to twenty times the power requirements in comparison to BLE, so knowing the power draw for the number of times users need to connect or communicate to the lock is important.

What are the recurring charges or costs?

When desiring and comparing access control functionality with standard locks, price is usually the most important factor because almost all access control systems have some type of recurring cost connected to their features. Obviously, any such costs drive the cost comparison significantly higher when compared to a standard mechanical locking system. So, one of the most important questions is: What is the cost, and are there any ongoing or recurring costs associated with systems that are being compared?

While personal computers of all types have quickly and thoroughly replaced the typewriter over the past few decades, the locking industry is still using pin-tumbler lock technology invented by Linus Yale in 1861 as the industry standard. Each day, increased school shootings, terrorism, and threats demand a change toward increased security and the access control features wireless locks can provide for interior and perimeter doors. Wireless lock technology is ready to challenge the status quo as the next generation of security for all doors, not just the perimeter doors. Campus administrators need to be prepared for the coming revolution.

ABOUT THE AUTHOR: Jeff Cahill has spent over forty years in the locking hardware and access control industries, including twenty years with Best Locking Systems, was one of the founders of XceedID Corporation and is the founder and majority owner of Proxess, LLC, a wireless locking/access control platform.

COLLECT.
SORT.
TRANSPORT.

ROYAL®
BASKET TRUCKS
www.royal-basket.com
800.426.6447

ORGANIZE YOUR AUDITORIUMS & PERFORMING ARTS FACILITIES WITH FUNCTIONAL CART SOLUTIONS FROM ROYAL®. OUR CARTS ARE DESIGNED TO REDUCE CLEAN UP TIME, TRANSPORT LAUNDRY AND EQUIPMENT, AND KEEP YOUR FACILITIES LOOKING CLEAN AND PROFESSIONAL.

CHOOSE YOUR CART. **PICK YOUR COLOR.** **ADD YOUR LOGO.**

- 13 VINYL COLORS
- 7 MESH COLORS
- 9 POLY COLORS
- CUSTOM BRANDING & LABELING

CONTACT US TODAY! **WWW.ROYAL-BASKET.COM • 800.426.6447**