

## Wireless Electronic Access Control

### The Problems of Securing Your Parking Equipment with Mechanical Locks and Keys and How to Solve Them



Parking equipment typically is secured by mechanical locks and keys. There are a number of problems with mechanical locks and keys which shrink the revenues and increase the operating costs associated with parking equipment. These problems can all be solved by electronic access control, which new wireless technology has made practical for parking equipment.

#### The Problems of Shrinkage

“Shrinkage” from parking equipment is reported to be between 5-10% of cash taken in by the equipment. Securing the cash in parking equipment with mechanical locks and keys makes you vulnerable to theft by both insiders and outsiders:

- You don't know if and when a lock was opened.
- Perhaps more important than when equipment was accessed, is when unauthorized access was attempted, and you don't know that either.
- You can't control when a key is used - a key lets the holder open a lock anytime he or she desires, not when you desire.
- Most mechanical keys can be copied.
- Most mechanical locks can be picked.

The Problems of High Operating Costs

#### Mechanical locks and keys impose high operating costs:

- You and your staff have to manage a large number of keys,
- When a mechanical key is lost or stolen, the relevant lock or locks need to be re-keyed which costs time and money. When a master key is lost or stolen, the time and money can be extraordinary.
- Any mechanical lock can be easily vandalized – the key hole can be jammed with a paperclip, chewing gum, glue etc.

#### The Electronic Access Control Solution

If you can secure your parking equipment electronically, you've solved the problems of mechanical locks and keys:

- You know when equipment is accessed.
- You know when unauthorized access was attempted.
- You can limit access to specific days and time.
- No more key management.
- No more re-keying of locks.

- An electronic lock cannot be picked.
- An electronic lock has no key opening and therefore is pretty much impervious to vandalism.
- Electronic access control provides you an audit trail you can use to detect problems or investigate reported problems.
- Knowing who accessed what equipment, when, and when unauthorized access was attempted can help detect theft.

The mere fact that access is being monitored electronically, which is apparent to anyone looking at the parking equipment, is a powerful deterrent to theft.

#### The Impediment

Single-space meters lack the onsite power and network communications required by conventional electronic access control. Pay-on-foot machines and multi-space meters usually have onsite power and network communications but conventional electronic access control is often difficult, and sometimes completely impractical to retrofit with the various locking mechanisms in such equipment.

#### How Wireless Electronic Access Control Works for Parking Equipment

Wireless Technology Makes Electronic Access Control Practical for Parking Equipment. Wireless electronic access control requires neither onsite power nor network communications and can be easily retrofitted into almost any mechanical locking mechanism.

The cores of the mechanical locks are replaced with new electronic cores. There are now electronic cores available to replace almost any mechanical core, including those commonly used in parking equipment, and the procedure for swapping them out is simple, quick and usually can be done in the field.

The electronic cores require no onsite power because they are powered by battery powered keys when the key is



# Wireless Electronic Access Control

presented to the core. The locks, which are assigned to specific personnel, are programmed to accept specific keys within specific time frames for a specific period of time, and are programmed to open certain locks within these time frames.

When a key with the proper permissions is presented to the lock, the lock opens. When a key that isn't authorized to open the lock is presented, the lock rejects it.

Programming of the locks and keys is done by a designated administrator using either desktop or hosted software. It is a simple matter of registering each lock and each key, assigning keys to locks, setting schedules (what days and times should the key open the locks to which it is assigned), setting expirations (when should the key's permissions expire), and then assigning keys to personnel.

The administrator then uses the same software to monitor and control access, as well as automatically generate desired reports.

The communication link is the key. Each time a key is presented to a lock, it uploads access information (including denied access) from the lock, which will date back to when it was last opened. This information is downloaded to the administrator's system when the key is placed in a download station, usually located at some central dispatch point, or presented to the infrared port of a computer.

At the same time the access information is downloaded, the key is refreshed with any new permissions, which can include renewing the previous permissions, changing them, or disabling the key completely.

Downloading should be at regular intervals to keep the access information in the system current and enable permissions to be changed in a timely manner. Downloading can and should be enforced by setting the permissions of a key so they expire within a relatively short period of time, requiring them to be refreshed by downloading in order to keep working.

As a backup, in case a key is lost or stolen, the lock can store the last 1,100 events which can be uploaded by a special key.

Ideally the software for the system is hosted, as this allows the administrator and others to use the system from anywhere with an internet connection, and to use cell phones to upload information from the keys and refresh them.

## Conclusion

Wireless electronic access control is a powerful tool for securing and getting the most from your parking equipment. When the cost of wireless electronic access control is compared to the cost savings and the reduced shrinkage attributable from wireless electronic access control, the typical return on investment is over 30%. ■

Mike Hopkins is CEO of EZ-Assure. He can be reached at [mhopkins@ez-assure.com](mailto:mhopkins@ez-assure.com).