

# Electronify\* Access to Your Parking Equipment

BY MIKE HOPKINS

*\*Electronify: conversion of a device to being electronically based. Typically, this is the conversion of a mechanical device; for example, a mechanical watch to a digital watch. (Geoffrey McDonald)*

**P**ARKING EQUIPMENT TRADITIONALLY has been secured by mechanical locks and keys. A number of problems are associated with trying to control access this way. Electronic access control solves these problems, but conventional wired systems just haven't been a practical solution for parking equipment. This has changed with new wireless technologies, which allow you to "electronify" any lock in any piece of parking equipment, giving you all the benefits of electronic access control.

## The Problems of Mechanical Locks and Keys

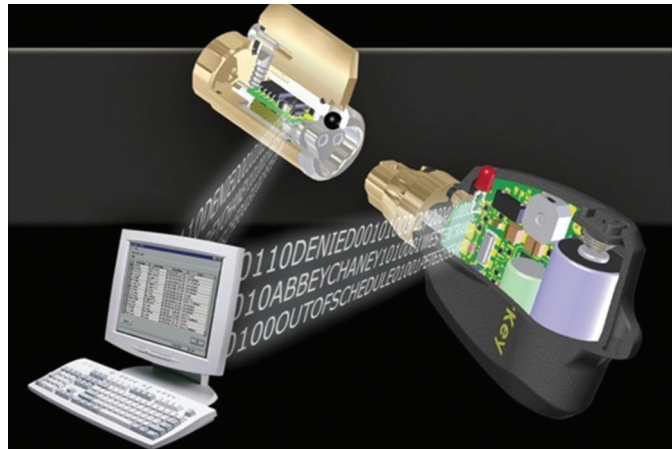
The fundamental problem with mechanical locks and keys is that you can't really control access. Why not? First, you have no way of knowing if and when a lock was opened. Second, you don't know if and when someone tried but failed to open a lock. Third, most mechanical keys can be copied. Fourth, most mechanical locks can be picked.

If you can't really control access to your parking equipment, you can't really protect the contents – most important, cash. This is a huge risk given that shrinkage in parking revenues is commonly reported to be 5% to 10%.

.....  
**The fundamental problem with mechanical locks and keys is that you can't really control access.**  
.....

Apart from putting your parking revenues at risk, mechanical locks and keys have high associated operating costs. You have to manage a large number of keys. You have to re-key a lock if a key is lost or stolen. If you are unfortunate enough to lose or have stolen a master key, that means re-keying all your locks.

Finally, mechanical locks are easy to vandalize. The need for a key hole means they can be disabled by inserting some foreign object or covering it with a superglue, requiring repair and even replacement, in addition to lost revenues while out of service.



## Benefits to Electronifying:

- You know when your equipment is accessed.
- You know when unauthorized access is attempted.
- You can limit access to specific days and times.
- You don't have to manage many keys. Electronic locks and keys allow each person to carry only one key that has all the permissions required for whatever locks they are authorized to open.
- No more re-keying locks. When an electronic key is lost or stolen, it can simply be killed and no lock is compromised.
- Electronic keys can't be copied, picked or vandalized (no key hole).
- You have an audit trail you can use to detect or investigate problems.
- You not only control access, but you also can record cash in equipment at the time it is accessed so that cash turned in can be reconciled with that removed from the equipment.

## Conventional Electronic Access Control

If you can secure your parking equipment electronically, you've solved the problems of mechanical locks and keys. However, single-space meters lack the on-site power and network communications required by conventional electronic access control. Pay-on-foot machines and multi-space meters usually have on-site 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 to Wirelessly Electronify Access

Wireless electronic access control requires neither on-site power nor network communications, and it can be easily retrofitted into almost any mechanical locking mechanism. Here's how it works:

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

The electronic cores require no on-site power because they are battery-powered keys when the key is presented to the core. Different manufacturers make different size keys, and while some are unwieldy, there are reasonably sized ones available.

The locks are programmed to accept specific keys within specific time frames for a specific period of time. The keys are programmed to open specific locks within specific time frames for a specific period of time, and are assigned to specific personnel.

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.

The programming of the locks and keys is done by a designated administrator using either desktop or hosted software. 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 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 a smart phone, PDA or 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 killing the key completely. Downloading should be at regular intervals to keep the access information in the system current and to enable permissions to be changed in a timely manner.

## A Compelling ROI

When you compare the cost of wireless electronic access control for your parking equipment to the cost savings and the reduced shrinkage you can expect from the investment, the typical return on investment is more than 30%.

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

**PT**