CyberLock®

Innovative Solutions
Traffic Control Security

CyberLock®

Security Challenges in the Traffic Industry

The traffic control industry faces some unique security challenges. Securing traffic control boxes, digital signs, traffic lights and other infrastructure can be extremely challenging and cost prohibitive. Making sure that the public does not change settings on digital signs or remove expensive copper from traffic control boxes is of the utmost importance. Additionally, ensuring that traffic boxes are getting serviced regularly and that emergency personnel can access them is highly critical.

CyberLock is virtually tailor made for the traffic control industry. CyberLock has designed locks that easily retrofit into existing traffic box hardware. CyberLock cylinders and CyberKey smart keys track every access attempt, whether successful or not.

CyberLock Features

Physical Security
Unlike mechanical locks, CyberLock cylinders have a unique, sealed design that negates standard lock picking techniques. Additionally, CyberLock cylinders are designed to withstand a variety of harsh environmental conditions, making them the ideal solution for outdoor applications.

Control and Schedule Access
Using the CyberAudit software, permissions for each lock and key can be changed effortlessly, enabling precise control over access to all entry points. CyberKey smart keys are programmed with a schedule to open one, several, or all locks in the system.

Increase Accountability
Every time a CyberKey meets a CyberLock, a time-stamped access record is stored in both the lock and the key, providing system administrators with full visibility of all access attempts, whether successful or not.

Easy Installation
Over 380 CyberLock cylinders have been designed to retrofit into a variety of access points, including traffic control boxes, gates, equipment and more. CyberLock cylinders retrofit directly into existing hardware, making installation quick and seamless.

Key Control
When a key is lost or stolen, CyberLock cylinders can be programmed to deny access to the lost or stolen key. Additionally, CyberKey smart keys can be scheduled with an expiration date, meaning when the key expires it will deny access until updated.

Eliminate Duplication Concerns
CyberLock employs unique access codes that electronically bind both the cylinder and key to one system, meaning CyberKey smart keys are not susceptible to mechanical duplication like standard #2 keys, the most commonly used key in the traffic industry.

Georgia Department of Transportation

The mission of the Georgia Department of Transportation (GDOT) is to deliver a transportation system focused on innovation, safety, sustainability and mobility. In furtherance of this mission, GDOT developed a set of goals to guide the agency. These goals include investing in citizen and employee safety, efficiently safeguarding existing resources, and investing to improve reliability. However, GDOT faced challenges in meeting these goals due to shortcomings of their access control system.

Challenge: Finding a Cost Effective Solution to Monitor Subcontractor Activity

With dozens of hub buildings and field equipment needing to be secured, GDOT found it hard to manage access to their assets. Oftentimes they needed to allow subcontractors into restricted areas for a limited amount of time. To do this, GDOT would have to issue a key to a subcontractor and ensure the key was returned within the prescribed time. Additionally, various traffic control meters and overhead digital signs were in need of a security solution that ensured the general public was not changing text or turning signals off completely.

GDOT initially used standard #2 keys, the most commonly used key in traffic control applications in the United States. Standard #2 keys are easily lost and/or duplicated, which caused key control problems for GDOT.

Solution: CyberLock

To combat the issues they were facing, GDOT turned to the CyberLock access control solution. CyberLock gave GDOT the ability to issue a CyberKey to a subcontractor. The CyberKey can be scheduled to open specific locks for a specific amount of time. Additionally, CyberKey smart keys are designed to prevent unauthorized duplication of the key ID code, meaning each CyberKey is unique and traceable. This solution gave GDOT peace of mind knowing that subcontractors could not have unlimited access to restricted areas. GDOT was able to easily retrofit their existing lock hardware with CyberLock cylinders without any hard-wiring. Additionally, without the need to hard-wire each access point, GDOT was able to deploy CyberLock while staying within their budget. They secured 28 hub buildings, various ramp meters, along with several digital traffic signs over freeways and interstates.

GDOT uses their CyberLock system daily to issue keys and track miscellaneous key holders' activity. According to Brian Jackson, their system administrator, "CyberLock fits the bill very well" and they are "very pleased" with the CyberLock system.

How it Works: A Simple Step-by-Step Process

Step 1
Replace existing mechanical cylinders with a programmed CyberLock cylinder. Each CyberLock is an electronic version of a standard mechanical lock cylinder. Installation is as simple as removing the original cylinder and replacing it with a CyberLock cylinder. Installation requires neither wiring nor batteries, making it quick and easy.

Step 2
Assign a CyberKey to a user. Keys are programmed with access privileges for each user. A standard key holds a list of locks the user may open, with a schedule of days and times when access is allowed. For instance, the key can be programmed to allow access from 8 A.M. to 6 P.M. on weekdays and 10 A.M. to 4 P.M. on Saturdays or it can allow access to key holding emergency personnel at all times.

Step 3
Access locks. When a CyberKey meets a CyberLock, the cylinder is energized and an information exchange occurs to determine if the key has access to that specific cylinder. The event and time is stored in both the lock and key. Lock cylinders and keys also record when an unauthorized attempt to open a lock occurred.

Step 4
Download audit trails and update keys via communicator devices. Expiring keys regularly ensures users frequently update their keys. When validating keys, the system downloads the audit trail and uploads new access privileges to the key. An expired key will not work until it is updated.

Step 5
View audit trail. The CyberLock system is managed centrally through CyberAudit software. Customized audit reports and notifications on suspicious activities can be automatically generated via email.

◉ CyberLock®

CyberLock, Inc. is the leading supplier of key-centric access control systems. It is part of the Videx family of companies with roots dating back to 2000 when the first CyberLock branded electronic locks and smart keys were introduced to the market.

Videx, Inc. has been designing and manufacturing innovative electronics since the company was founded in Corvallis, Oregon in 1979. Early products included display enhancement modules for Apple computers. In 1985, Videx entered the data collection industry with its first portable bar code scanner. Over the years, additional data collectors have been introduced, utilizing touch memory button and RFID tag technologies.

In 2013 CyberLock, Inc. was spun off as an independent company but maintains strong ties to Videx. The two companies continue to collaborate on future innovations.