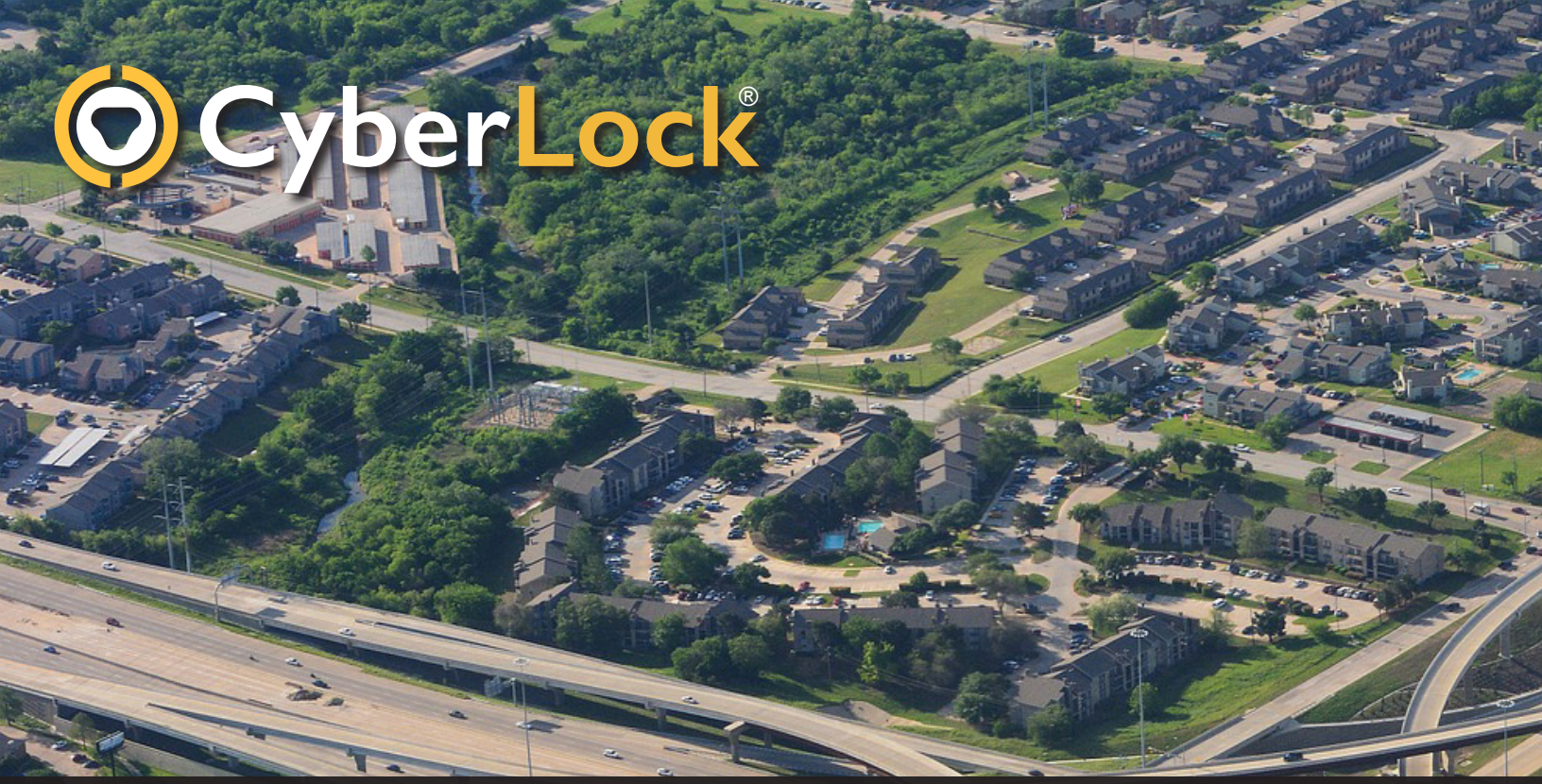
CyberLock®



Executive Brief:
Transportation Departments

How CyberLock Electronic Locks and Keys Represent the Best Solution for the Traffic Industry

Abstract:

Regional and local Departments of Transportation throughout the United States struggle to properly secure traffic cabinets, traffic lights and road communication equipment. The leading problem in transportation security is key duplication. For most traffic cabinet locks, a standard #2 key is issued to control access. #2 keys are extremely prevalent and easily duplicated. Additionally, there is limited variation in the cut of the key, a single key can open a variety of traffic cabinets accross the country. Transportation departments are tasked with finding a reliable security solution that eliminates the concerns and risks that the #2 keys pose. This document will cover key duplication concerns, identify which assets demand protection, and illustrate how key-centric solutions can improve security and accountability.

Concerned About #2 Keys in Circulation?

The #2 standard key, widely used to access traffic cabinets from many of the top manufacturers, is unfortunately one of the easiest mechanical keys to duplicate or purchase online. On any given day, an abundance of these #2 ‘skeleton’ keys are available for purchase. Further yet, new technologies now enable accurate duplication of any mechanical key, using only a smartphone app and a consumer-friendly 3D printer. Despite these concerns, the #2 mechanical key often represents the only form of security preventing access to critical roadside equipment; equipment that should only be accessible by trained, trusted individuals. The lack of control inherent in these mechanical key systems jeopardizes the security and safety of transportation infrastructure across the globe, from small towns to some of the largest cities.

What Needs to be Secured?

Traffic control boxes and digital signs are expensive pieces of equipment that are essential to the safe and smooth operation of roads and highways. Each traffic control box contains thousands of dollars in critical equipment, including networking devices, computers, expensive cabling and more. The security of this equipment is of the utmost importance.

Traffic Cabinets

Traffic control boxes not only control the flow of traffic, they also house equipment used to control operations of other public systems. With thousands of dollars in critical equipment inside, traffic boxes are attractive targets for thieves. Numerous detailed accounts shine light on the issue of theft in the traffic cabinet industry. Not only are traffic boxes subject to the theft of internal components, they are also subject to tampering. Whether malicious or not, tampering may create dangerous conditions for the public.

Roadside equipment is a frequent target of tampering, particularly speed monitors and digital signs. Messages displayed on digital signs are regularly altered by unauthorized individuals, with intentions ranging from helpful to malicious. A routine web search returns countless photographs and news stories illustrating unapproved changes that both DOT employees and members of the public have made to digital signs. Signs often get changed from important warnings, such as “Night Construction: Be Prepared to Stop,” to trivial messages, like “Marry Me Sally?” depriving drivers of critical information.

Not only is tampering potentially dangerous to motorists, it can be problematic for employees and engineers who service this equipment. Leaving their regular service route to resolve issues caused by tampering can delay scheduled maintenance.

Digital Road Signs

CL-TC1 & CL-TC2

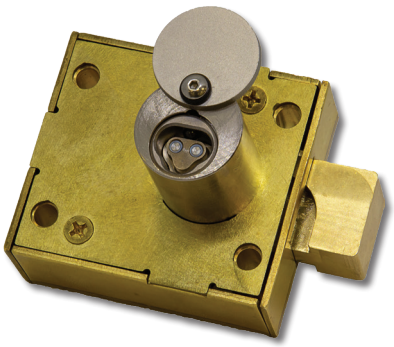
CyberLock is a key-centric access control system designed to increase security, accountability, and key control. Based on a unique design of electronic lock cylinders and programmable smart keys, CyberLock solves security problems that no other system can.

Traffic control administrators can quickly schedule and review access with the powerful CyberAudit-Web software. Permissions for each lock and key can be changed effortlessly, enabling precise control over access to every entry point. Email alerts and audit reports keep management informed of each employee's activities, including denied access attempts.

CyberLock has developed over 380 electronic cylinders designed to seamlessly retrofit into existing hardware. The CL-TC1's and CL-TC2's are cylinders designed specifically for the traffic industry. CL-TC2's are available in left or right configurations.

CL-TC1

CL-TC2L



CL-TC2R

CK-BLUE2 & CK-AIR2

CyberLock cylinders install without expensive hardwiring and contain no battery to service or replace. The battery from a CyberKey energizes the electronics within a CyberLock cylinder. Moreover, the stand-alone design of CyberLock cylinders means that secured access points are not susceptible to network or IoT attacks.

Although CyberLock cylinders are not networked, the Wi-Fi capabilities of the CK-AIR2 enable wireless updating of schedules, permissions, and access events when the key is connected to an authorized Wi-Fi network. This allows for near real-time audit reporting and access permission updates.

CK-AIR2

CK-BLUE2

The Bluetooth capabilities in the CyberKey Blue 2 allow users to update permissions in the field, even if they are outside of cellular range.

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, without the need to run power or network cables, 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.

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.

CyberLock®

1105 N.E. Circle Blvd., Corvallis, OR 97330
541-738-5500 • Fax 541-738-5501
www.cyberlock.com • sales@cyberlock.com
Designed, Manufactured, & Assembled in the USA