Traffic Cabinets
It should go without saying that the mechanical locks that come standard on these ITS cabinets simply aren’t adequate to protect the critical infrastructure housed within. Departments of Transportation at both the state and municipality level should consider a more robust solution to ensure the security of these vital systems.

In today’s connected world, Intelligent Traffic System (ITS) cabinets that can be found at virtually every intersection are vulnerable to an entire gamut of risk from seemingly harmless vandalism to more malicious physical and cyber-attacks. Used to store and protect complex equipment that controls traffic signals and digital road signage, they are critical for road and highway safety.

With hundreds of thousands of ITS cabinets throughout the country and the potential safety risk of an attack, properly securing these cabinets is an absolute must. Unauthorized entry into an ITS cabinet not only provides access to control connected intersections but could also allow access to the entire network of traffic controllers and camera feeds. In addition, each cabinet has active network connections to state and municipal agencies, putting them at serious risk of cyber attack.

Despite the fact that physical access to traffic infrastructure can have an immediate and widespread impact, the majority of cabinets are secured with a physical key that could easily be obtained and duplicated.

**Solution**

It should go without saying that the mechanical locks that come standard on these ITS cabinets simply aren’t adequate to protect the critical infrastructure housed within.

Departments of Transportation at both the state and municipality level should consider a more robust solution to ensure the security of these vital systems.

---

**Problems in Traffic Control**

**Key Control**
Standard #2 key commonly used, uncontrolled and easily available on the market.

**Traffic Signal Boxes**
Contains Intelligent Traffic System (ITS) controls, city and state network access and more.

**Traffic Signals**
Tampering of traffic signals can cause significant traffic disruption and loss of life.

**Roadside Equipment**
Speed monitors, digital signage and other roadside equipment is exposed to tampering.

**Accountability**
Currently there is little to no accountability on the majority of our cities’ traffic and ITS infrastructure.

---

**Challenge**

In today’s connected world, Intelligent Traffic System (ITS) cabinets that can be found at virtually every intersection are vulnerable to an entire gamut of risk from seemingly harmless vandalism to more malicious physical and cyber-attacks. Used to store and protect complex equipment that controls traffic signals and digital road signage, they are critical for road and highway safety.

With hundreds of thousands of ITS cabinets throughout the country and the potential safety risk of an attack, properly securing these cabinets is an absolute must. Unauthorized entry into an ITS cabinet not only provides access to control connected intersections but could also allow access to the entire network of traffic controllers and camera feeds. In addition, each cabinet has active network connections to state and municipal agencies, putting them at serious risk of cyber attack.

Despite the fact that physical access to traffic infrastructure can have an immediate and widespread impact, the majority of cabinets are secured with a physical key that could easily be obtained and duplicated.
ASSA ABLOY Intelligent Key Solutions such as Medeco XT offer a fast, easy and affordable way to upgrade the security of traffic cabinets. Installed in minutes, Intelligent Key Systems eliminate the need for wiring and other expensive infrastructure. They offer a powerful feature set at a much lower cost than traditional electronic access control (EAC) when live monitoring and door alarm features are not required.

- Electronically programmed credentials can open specific locks on a designated schedule by user and can be expired or revoked to meet security needs
- Audit information, recorded in both the lock and key, shows a time-and-date stamped record of every event (authorized and unauthorized)
- Attack-resistant design and tamper-proof features protect against forced entry
- A great add-on to online locks where an uncontrolled mechanical key override is causing a security risk

Intelligent Key Solutions

Intelligent Keys eliminate complex components and wiring to enable easy, affordable access control in mission critical applications.

Advantages of Intelligent Keys

- Easy installation
- Key control
- No wiring required
- Audit trail
- Easy maintenance
- Retrofit capability for almost any opening
- Flexibility for use in remote locations
- Visual data analytics
ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience.