Understanding
Key Control Systems
and Best Practices

**MORSE
WATCHMANS**
think inside the box.

Abstract

Key control and asset management technology is seeing significant growth across a broad range of applications, and for good reason. It's a reliable and cost effective method of improving building security by ensuring that facility keys are properly managed with regard to access, storage and tracking. Key management systems can reinforce access control policies that are already in place and can also help to reduce the costs associated with lost keys or unmanaged access.

Another factor impacting the growth of key control technology is that facilities, both new and existing, will likely continue using conventional key/lock systems as these devices are exceptionally cost-effective. It therefore makes sense from a cost as well as a time standpoint to maintain these key/lock systems while increasing the level of security they offer – and key management systems are the perfect solution to this need. They provide an immediate improvement to safety and security, are much more accessible in terms of managing costs, and are extremely easy to implement.

The effective implementation of a key control and asset management system can be achieved through best practices to realize decreased operational and financial risk and provide the best value from the application. This white paper presents several best practices for deploying key control and asset management solutions.

What You Need to Know about the Technology

Key control and management systems are defined as an orderly and secure solution for addressing controlled usage and safekeeping of mechanical keys and/or plastic card keys. The tamper-proof systems are designed so that only authorized users – using pre-programmed PIN codes, access cards or biometrics – can access keys, while on-board advanced technology automatically records all access activity.

Today's key control and management systems have become a higher-level management tool for effectively addressing the safety and security of building occupants and the security of the building assets. Knowing the identity of authorized key holders, which keys they have in their possession or have access to, and when they were used are all essential pieces of information that help ensure a safe and secure environment. Furthermore, technological developments and open protocols have made it possible to integrate key control with access control and other security systems as part of a facility's networked security system. Now, a user who has taken a specific key can be denied egress from the facility until the key has been returned – and selected management can be alerted via email or SMS text if a key has not been returned on time.

A basic system typically consists of a computerized key storage cabinet, a key locking mechanism and a tracking system. From this basic package, several options and design variations can be added to customize the solution and help protect the investment as needs grow and change. For networked installations, management soft-ware can also be included in the system. Permission levels can be established for each user and data can be monitored from any desktop connected to the network. When the system is networked, changes such as additions or deletions are synchronized throughout the enterprise for faster, more effective control. Additionally, the software can run activity reports, sort based on different criteria and view and print reports, among other uses.

Vital documents, cash, employee badging/access control cards, data drives and even small electronic gear can also be controlled and secured using asset management lockers or keycard modules that can be integrated into a key control system. Asset locker systems are identical in function to key control systems; users can access items only from the lockers/modules for which they have been pre-authorized and any activity such as removing or returning items or opening lockers/modules is automatically recorded in an audit trail.

Key management systems have become an operational necessity in environments such as correctional institutions, hospitals, car dealerships, property management, casinos and educational facilities, to name just a few examples. Key management is also a critical function for anyone overseeing security at conference centers, government agencies, control rooms, automotive businesses and corporate buildings. However, key control can and should also be applied to businesses of all sizes because of the measurable benefits of enhanced security and convenience, as well as increased staff productivity and accountability.

Read more about key control solutions for **city and municipal government facilities**, **control rooms/data centers**, and **correctional facilities**.

"A basic system typically consists of a computerized key storage cabinet, a key locking mechanism and a tracking system."

Getting Started

Implementing a key control and management system is a straightforward process that involves a few basic steps: take inventory of the facility to identify all access points and installed locks; ascertain the operational needs of employees as well as of others who may need access to the facility (e.g., service repair or cleaning crew); and establish a policy with easy to follow procedures for effective key control and management.

The first step is to catalog every access point and every piece of door hardware. This process is followed by management assessing which individuals have keys, which keys they have and which doors they access. Without this preliminary audit, it's almost impossible to know what size and type of key cabinets will best fit your needs and where the key control systems should be located.

System growth should also be factored in at this stage of planning. What may seem adequate today may become insufficient in a year or two. The ability to add on the exact components you need, or change modules where and when you need, helps protect your investment. This way you will avoid having to rip and replace an entire key control and asset management system because the current system cannot accommodate lockers for securing cell phones or other valuable items, or does not integrate with a new access control system.

Next, review operational needs to understand how the facility works on a day-to-day basis, so that use of a key control and management system is efficiently optimized. For example, would system users benefit from a second-language interface, or auditory prompts that cue users on correct key removal and return procedures? Assessing these and other requirements in the planning stages will help ensure that daily operations are disrupted as little as possible and the implementation is a success. Whether the facility is a hospital, dormitory, hotel or office building, having a comprehensive grasp of daily activity will help in implementing a key control system and will also help in minimizing the trade-off between security and convenience.

> Read more about key control solutions for **hotels**.

If a networked key control system is planned, a review of the network topology will reveal any configuration and performance alterations that may need to be applied. Compatibility with other security systems should also be reviewed to maximize interoperability for more comprehensive integrated operations.

A simple but strong set of guidelines for administration and use of the key control system will help to define areas of responsibility and enable better control of the keys.

Designing and Customizing the System

Configuring a key control solution is as easy as identifying needs and then building the system with modular components that meet those needs. Users select a cabinet size, and if more than one cabinet is required, the arrangement can be linear (side by side) or stacked. Cabinet doors may be solid steel or they may be see-through (e.g., polycarbonate) designs.

Choices for modules to fill the cabinets may include a selection of key storage modules, credit card modules or simply blank modules (to be filled at a later time). The combination of modules is entirely up to the user, pro-

viding the ability to customize and also change the system to meet growth or other specific needs.

Custom modules and lockers that can accommodate plastic card keys or other valuable items may also be included in the system. Lockers, available in various configurations, can be used for storing credit cards, small firearms, cell phones, 2-way radios, laptop computers, tablets, cash trays and so on, and can be managed as efficiently as keys in key control systems. Items can be returned to any open locker for convenience, and systems can be set up as personal storage spaces for one or multiple users.

Key control and asset management systems can also be configured with additional security features to help enhance the integrity of the system. For example, where protection of asset lockers itself is mission-critical, installation of a remote access device provides an addi-tional layer of protection by enabling the locker system to be placed in a secure room. A second individual's PIN input and verification are then required in order for an authorized employee to access the contents of a locker.

Access to the key and asset cabinets can also be customized, with options including a built-in keypad, biometrics such as a fingerprint reader and a magnetic or proximity card reader. Systems that integrate card readers for access can often utilize the access control cards that are already in use throughout the organization, making the system implementation easier and more convenient. Changes to an individual's access authorization can be made instantly by program administrators. The optional user interfaces can be integrated directly into the cabinet for easy accessibility or they may be separate. In either design, users can access only the stored items that they have been authorized to remove or return.

Company Support

Another important point for consideration is the level of vendor support the user can expect when implementing a key management system. While all parties hope there will never be any problems during or after the installation, issues can and do arise. For example, what happens if there is a problem after the user updates the system software? Given the mission critical role key management systems

play in businesses, end users should check whether the vendor offers any phone/tech support, warrantees or other resources prior to purchasing the system.

System Integration

A key control and asset management solution can usually be integrated with the existing physical security system without costly upgrades or overhauls. Today's key control solutions feature open protocols to enable connectivity to access control, IP video surveillance, intrusion and fire alarm systems, and other systems provided by a range of integration partners for multiple levels of security and control. For example, with a turnstile-type access control system networked to the key control system, a user who has taken a specific key can be denied egress from the facility until the key has been returned, or may be allowed access to another area of the facility when holding a specified asset.

Open protocols also allow the system to be networked and integrated with other key technologies to streamline processes and eliminate redundancies across common points. Employees can be entered into the access control system, for example, with their credentials, profile information, access group, etc. instantly transferred to other systems. The system can also pass data about transactions and alarms back to the access control system for greater integration.

Software Add Ons

One of the enabling factors for successful key control implementation is the ability to manage all programming, remote functions and reports for the system with a software-driven solution. Similar in concept to popular access control systems, the PC-based package of key management software helps make day-to-day operations and activities easier and more fluid. Users can be added from a global list and all specific settings (added or modified) will be automatically synchronized across the system. Profiles can be assigned for improved user control, and administrative access levels have various options to be tailored to specific needs such as reports only or alarms only.

Built-in schedulers can be programmed to automatically download all data to a secure PC as required by the user. With this capability, management can better sort and analyze information to maintain maximum control of access and security issues.

Read more about **integrating key control** with existing access control systems.

Scheduled email reports, detailing what keys are in or out and who has/had them, keeps security management informed and up to date. If an incident occurs, management can query the system for specific details, such as a listing of all transactions between certain times; and when doing a follow up investigation, management can request a report for the hour preceding the incident. Or, immediately following an incident, a report can be generated showing which keys are back in the system and which keys are still out and who last accessed them. Together with the audit data from an access control system, a key control system's customizable reports provide a strong evidence trail. Given the ease of generating custom reports, users are strongly encouraged to leverage the wealth of data available to identify opportunities for greater process efficiency (e.g., rotating users across less-used key cabinets in a facility to reduce bottlenecks at certain times of the day).

Mobile Applications

Advanced communication capabilities enable key control systems to be monitored and administered remotely from a smartphone or tablet as well as from a desktop. Apps for automated key control systems enable users to maintain control of keys no matter their location. At any time, an authorized user can see real time transactions and information about keys that are in use and any keys that are overdue, as well as where and when alarms may have been triggered or overall system status. For investigative purposes, managers can even review key usage to determine who may have last accessed a key for a vehicle that was found to be damaged. Having this information available on a mobile device is like having a remote office.

Notifications and events are automatically sent to authorized personnel, allowing them complete control of the system. They can cancel an alarm and even, if necessary, remotely disable user privileges. These features, along with multiple others, provide the mobile user with a greater level of convenience and control when it comes to key control management. For situations that demand rapid response (or just for greater peace of mind), such functionality should not be ignored.

Mobile applications are quickly becoming a preferred platform for security managers accessing key control data and even to perform transactions. The result is improved safety and integrity of the facility.

Technology Updates

User Features — Along with the introduction of mobile apps, today's electronic key management systems are continually updated with new features that make it easier and more efficient for everyone to use. Some of these may include illuminated key slots to locate keys and random return capability (i.e., return keys/assets to any open slot in the cabinet or in the system); large touchscreens on the front panel with buttons and an easier to use interface with step by step instructions or audio prompts. Keys available for access can be called up on the touchscreen along with information about the location of a specified key, what keys have not been returned and when the key will become overdue. Notifications advise users when an overdue key has been returned.

Other new user enhancements include the ability to replace keys from key tracking software using a specialized reader device and reports can now be saved/viewed as a PDF, or saved as a CSV file. Data encryption and firewall protection updates help protect sensitive information on the network.

RFID — Another recent innovation in key control systems is RFID asset management locker systems which use RFID technology to track assets placed in or removed from the lockers. Similar in concept to an automated key control and management system, RFID asset management locker systems use the integrated RF antenna rather than a key fob to automatically record all user access activity. Designed for optimum security, a locker will not open until the system verifies that the user has permission to access the contents of that specific locker. And because the system automatically records all activity, custom reports can be run and delivered automatically to management on a scheduled or as-needed basis.

Application Examples

Educational Facilities — A robust key control and management system can provide an additional layer of security and information for first responders in an educational environment. For example, badges can be pre-

configured and distributed to designated first responders and, in the event of an incident, when they reach the scene they simply scan the badge into the system and the critical emergency keys will be released. It's also important to remember that in addition to traditional first responders such as fire, law enforcement and EMS (emergency medical services) personnel, there is a wider circle of school staff and departments that play an integral role in emergency situations. Key control systems that are strategically located, networked and easy to use/manage add to an individual's ability to efficiently cope with an emergency.

Read more about key control solutions for **education**.

Many schools (both public and private) today at all levels are battling budget cuts to their operational expenditures, and key control systems may help reduce costs. For example, services by janitorial or maintenance staff might be shared among several schools in a district rather than be dedicated to a single school, or teaching/support staff may be assigned to more than one school.

In these instances, instead of issuing duplicate sets of keys to several employees (and potentially creating a security vulnerability), a single set of keys can be stored in a key control system that is located in the building for which the keys are used. Using their pre-authorized PIN codes,

visiting staff can quickly and easily access needed keys without having to go looking for them or interrupt another individual to dispense the needed key. All access activity is recorded and any changes to authorizations can be made quickly and easily by the system administrator.

Casinos — To effectively manage casino assets, key control systems store, control and track keys that are used for access to all the most sensitive and highly secured areas of the casino where money and chips are held, including the slot department and cages. Customized features and advanced technology in key control systems also make it easier for casinos to comply with gaming commission regulations pertaining to key control and management. For example, to meet gaming regulations that require the three man rule to access sensitive or restricted key sets, the key control system can be programmed to recognize these keys or key sets and only open the cabinet door and release them once the three required logins are completed and the credentials verified. These measures ensure that no one person acting alone can access a sensitive or restricted key and that these keys never leave the property.

Gaming requirements do vary from state to state, as well as from tribe to tribe. The key control and management system chosen for deployment in a casino environment should be flexible, so that it can accommodate any of the above regulations and much more. It should also be modular and scalable, so the number of keys and the scope of features can change and grow along with the business. Finally, it should be easy to use, as training time can be costly and many employees will need to be able to access the system.

Fleet Management / Car Dealerships — The benefits of adding a key bank system to a dealership operation are many. Management controls who accesses vehicle keys, who enters the system, who takes a key and why it is removed and how long the key is out. No more missing keys. No more mystery damage or mileage.

Read more about key control solutions for **fleet management** and for **automotive dealerships**.

In applications for automated key control and management systems used in fleet operations or dealerships, software is available to track key usage so that management knows at any given time who has accessed keys and when. Dealerships that network their key control systems can experience additional benefits in managing vehicle usage. For example, scheduling can be used to ensure that drivers can't simply grab the newest car on the lot while older cars sit unused. Additionally, networked systems allow keys to be returned to any fleet key cabinet in the system. This makes it easier to track a vehicle that has been returned to a location different from where it was picked up. The system software will record the location and time so anyone looking for that vehicle will know where it – and its keys – is currently located. This benefit allows vehicles to be moved around and located as needed.

Conclusion

By following these best practices for key control and asset management systems, users may experience decreased operational and financial risk and achieve best value from the application. They can also be assured that new and innovative features will continue to be added, increasing the value of their investment. From the enterprise to the SMB, these systems offer a simple yet highly effective solution.