WHITE PAPER

UNDERSTANDING KEY SYSTEMS AND THEIR IMPORTANCE TO END-USER PHYSICAL SECURITY PROGRAMS
INTRODUCTION
Key systems are a crucial part of a physical security program, and must be properly designed and managed in order to provide the necessary controls and a solid foundation to an overall security program. Left alone and unmanaged, a key system opens an organization to the potential for loss and liability.

An electronic physical access control system verifies individuals’ identities and provides access based on a company’s security policies and procedures, which govern how access privileges are granted within an organization. The management (or enrollment), issuance and termination of these credentials is a critical component in providing the right individual with the right level of access and in making sure that no individual has unauthorized access to any part of a facility.

In order for access control systems to properly function, some manner of restraint must be employed to prevent an unauthorized individual from gaining access to a restricted area. In most cases, this restraint is a locking mechanism (i.e., lock) that can be opened by using a mechanical key. The management of this secondary credential (the key) is critically important because it provides any individual with access to restricted areas. Many times, security personnel are unable to verify the identity of the individual key holder.

Managing electronic credentials (cards) and mechanical credentials (keys) is vitally important; the management of the card and key must be linked to a uniform security policy with a centralized key (credential) control authority. If proper controls are not instituted, security efforts will be compromised; the ability to properly manage a key system sets the standard for the entire physical security program. To properly manage keys and key systems, it is important to understand the fundamentals associated with key system policies, design and management. This information helps to improve a key system and physical security program that reduces the potential risk of loss and liability.

Your security starts with locks and keys, and your key system is your first line of defense. It is a critical component in protecting your facility against loss while increasing accountability and limiting risk. With mechanical key systems, security is derived from the management and protection of physical keys and the key system policies you create to enable that management and protection.

KEY SYSTEM POLICIES
The key system policy and its stated principles will express the desired goals and outcomes and will function as a guide for the security team to respond quickly and effectively to all decisions involving key control. Well-written key system (or key control) policies guide the behaviors and actions of the individuals who issue and use the keys for a facility and play an essential part in increasing the safety and security of any facility.

When determining a key system policy, there needs to be a balance between the needs of security and the needs of the individual. It can range from an open, accommodating environment to one with strict and limiting access controls.

A well-documented key system policy will seek to address the following:
- Taking action when a key or master key is lost or stolen
- Distributing, replacing, tracking or returning keys
- Handling requests for additional, new and replacement keys
- Managing temporary and contract employees
- Identifying the key control authority and the authority’s responsibilities
- Keeping records
- Creating an authorization process to obtain keys
- Taking steps to re-key the facility
- Enacting disciplinary actions for individuals that violate the policy

As an example, The University of Massachusetts, Amherst answers the first and last questions in this way, “If a Master Key is lost or stolen, it should be reported to the Residence Director immediately. A lost Master Key will result in disciplinary action, which could include job termination, as well as all costs related to securing the Cluster with new keys.”[1]

If an end-user maintains its own key system, the key system policy should address these additional areas:
- Storing of key blanks
- Procuring key blanks
- Processing the auditing of key blanks, miss-cut keys, returned keys and active keys
- Storing, managing and protecting key codes

A key system policy will inevitably be a customized document that reflects a company’s specific security needs and culture and should be drafted by those in the organization that have a vested interest in securing the facility, maintaining compliances, lowering risk, and supporting and maintaining the company’s culture. This will achieve the balance and appropriate processes that are so critical to the long-term success of your key system.
KEY SYSTEM DESIGN

A well-designed key system can do more than just secure doors. It can control traffic, protect people and assets, enforce compliances, and manage access rights. Poorly designed key systems are usually complicated, unmanageable and inconvenient for the security team and employees.

The process for creating a well-designed key system starts with identifying all the doors that require a key. This would typically be followed by identifying the security level for each opening. In this situation, consider the risk or liability associated with each opening and the assets, personnel, information, and/or certifications or compliance that would be required of any individual who would need access to the space behind each door and then assign the appropriate key-locking technology.

Keyed cylinders and cores are available in multiple configurations, and because locks come in many shapes, sizes and cylinder types, it can sometimes present a challenge to the end-user to have a uniform key system, particularly if the facility has several different brands of locking hardware. In some cases, creating a well-designed key system could require the replacement of some locksets or working with a brand of locking cylinders that provides multiple configurations using the same keyway (pathway into the cylinder) or key profile.

The long-term viability of any key system is dependent upon the ability to prevent keys from being duplicated without knowledge. Having "Do Not Duplicate" stamped on a key affords no protection because there is nothing legally enforceable to prohibit anyone from duplicating the key. It has been estimated that unauthorized key duplication accounts for as much as 40 percent of unexplained illegal entries, resulting in billions of dollars in losses to businesses each year. The ability to control who can duplicate keys is critical to key system success, and the only way to make sure that keys cannot be copied is to invest in a patented key system.

Patents reinforce key systems with legally binding agreements that restrict the availability of key blanks and enforce processes for only authorized individuals to obtain key blanks. Patents are only in force for a period of 17 years, and the choice for any patented key system must consider the patent expiration date. An expired patent does not mean that a facility is unprotected, only that there exists a potential for key blanks to become available. Therefore, the choice of a patented key system should also consider the popularity (distribution) of the specific key selection.

In the discussion of patented key systems, it is important to understand where patents fit in the range of available keyed cylinder technologies (and restriction) because in some cases a patented system is not warranted. Keyed cylinders are available with differing levels of restriction, and the choice of a key system technology should consider the risk and liability associated with any opening where access control is maintained with a key.

The following table illustrates the different types of cylinder mechanisms and technologies:

<table>
<thead>
<tr>
<th>Cylinder Mechanism</th>
<th>Restrictiveness Level</th>
<th>Key Blank Availability</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conventional</td>
<td>1</td>
<td>Open and available through a wide variety of sources</td>
<td>A majority of key systems fall into this category and there is no secondary locking mechanism</td>
</tr>
<tr>
<td>Restricted</td>
<td>2</td>
<td>May be contract controlled and/or available through limited sources</td>
<td>Some of the key systems that fall into this category may have expired patents and a secondary locking mechanism</td>
</tr>
<tr>
<td>Patented</td>
<td>3</td>
<td>Contract controlled, restricted availability</td>
<td>Patent technology will normally include secondary locking mechanisms</td>
</tr>
<tr>
<td>Patented High Security</td>
<td>4</td>
<td>Contract controlled, restricted availability</td>
<td>Meets UL437 security rating</td>
</tr>
<tr>
<td>eCylinder</td>
<td>5</td>
<td>Contract controlled, restricted availability</td>
<td>Electronic key communicates with an electronic cylinder, can include a mechanical feature for a hi-low hybrid</td>
</tr>
</tbody>
</table>

Table 1: Different types of cylinder mechanisms and technologies
After selecting the cylinder technology, it is time to design the master key system. A good rule here is that “simple is better,” providing a secure and easily controlled, manageable system. Consider working with a key system design consultant that can provide good recommendations that meet the objectives described in the key system policy. Consider the following at the beginning of the key system design:

- Decide who is assigned the master key. Be judicious with any master key, especially the grand master as this is the key that could open all locks in a facility. A re-key for a stolen or lost master key could be extremely expensive, and it is best if only a few individuals have it. It is sometimes recommended that a grand master is never cut nor issued.
- Determine if every employee should be assigned a key. This is not always necessary if electronic access control at key control points is used and most employees work in cubicles and not offices.
- Address high employee turnover. In this situation, consider using interchangeable cores as this will allow for the quick replacement of cylinders when employees leave with a key.

Master key systems are also described as having levels where each level is part of a hierarchy with the top level master key generally opening every door. Again the principle is to keep it simple because more levels will open up the key system to potential unauthorized or unintended change keys. There are methods for creating larger master key systems that would eliminate the risk of unintended change keys. A key system design consultant can determine how many levels would be required based on your specific needs.

**Figure 1: Three-level master key system structure**

![Diagram of three-level master key system structure]

There are a variety of other steps that can be followed in completing the design of a master key system including grouping of doors into categories, departments or geographies; the use of building plans to determine what doors are associated with the different categories; the assigning of key symbols; and understanding what requirements are needed for system expansion.

The “keep-it-simple” rule applies throughout all facets of key system design, and is a critical factor for the long-term success and ongoing management of a key system.

**KEY SYSTEM MANAGEMENT**

Before a key system is built and installed, it is important to understand how it will be managed. Establishing a policy before a key system is in place is critical because policies need to be enforced from the beginning as any lapse in enforcement could jeopardize the integrity of the key system.

Determining whom is the key control authority and that person’s responsibilities should be the first step; it is recommended that this individual understands the company’s key system and overall physical security program. This person is responsible for the daily activity and interaction with employees and key system and would oversee the issuance, tracking, and cutting of keys as well as the storage and procurement of key blanks and other materials. It is also recommended that this individual be responsible for (or responsible to the individual who is) issuing credentials for the electronic access control system. The two should be linked to make sure that integrity of the overall physical security program is maintained.

Keeping track of keys can be a difficult practice. The more keys available, the more opportunities there are for someone to lose them or for them to get into someone else’s hands. The most likely scenario is that keys get lost in the facility where they are used, and that the person finding them can identify exactly which doors they access. In 2011, a teacher at Menlo-Atherton High School in the San Francisco Bay Area lost a master key and according to Principal Matthew Zito, “In this case, the keys were most likely lost on campus. As far as I’m concerned, they are lost in that the person or persons who have them most likely know what they have.”

Effective management of key systems can be enhanced by the use of software that tracks issued, lost or stolen keys, and any other event or incident involving a key system. Without consistency in the credential management process, someone with an authorized key having access to an unauthorized area of the facility could be a realistic scenario. Options are available that could prevent such a situation from occurring and include:

- Designing a physical security system to eliminate the need for most individuals to carry keys
- Keeping all keys for a facility on site in an electronic access controlled key storage unit that provides auditable tracking of those keys.

In an office environment where most employees work in cubicles, it is entirely plausible to eliminate the need for keys for most individuals and should be strongly considered as an option. It still may require that a facility is re-keyed anyway because the use of existing and older unrestricted keyed cylinders would continue to create vulnerability in the security program, particularly if the keys had been previously issued. Electronic access controlled key storage units are a popular option to maintain control over a key system and allow individuals on site to have access to only the key(s) required for that day. These units can be tied into an existing electronic access control system and operate off the same credentials.
MECHANICAL AND ELECTRONIC ACCESS CONTROL
A physical security program will inevitably have both electronic and keyed access control points working together to control access to and within a facility. Most end-users may feel that these are the only two options available, one of which is expensive. A variety of access control options are available, such as conventional keyed security and high-end electronic controller panel-based systems.

One option is the use of eCylinders, which can combine mechanical patented cylinder technology with an electronically controlled cylinder and proximity card capability in a single solution. This option would provide loss and liability control, which improves regulatory compliance. Additionally, there are several offline and online locking options that integrate with an electronic access control system.

It is advisable to conduct a security vulnerability assessment of the facilities. As technology changes or as systems age or patents expire, security may be vulnerable and need to be updated. A security program should include a process for improving all aspects with access control platforms both mechanical and electronic. This will make sure that the needed protection is provided for employees and assets over the long term.

SUMMARY
A key system is critically important to the overall security program, and poorly designed and managed systems introduce vulnerability throughout a facility. There are several options available to you when it comes to key system design and management and it is important to understand what differentiates one solution from the others.

- Understand how each technology is able to fulfill various security objectives and try not to focus on any single solution. Sometimes a combination of solutions (e.g., eCylinder and mechanical cylinder) may be the right choice.
- Work with consultants that have experience with video surveillance, electronic access control and intrusion as this is an important consideration when designing a key system to work in conjunction with an overall security program.
- Work with a consultant that can help design or update the security policy by providing recommendations; no outside firm or consultant should ever write the policy. Policies and programs needs to reflect security needs and objectives and the company's culture.
- Decide if security and facilities each have a role in managing the security program; it is important that both are governed by the company's security policy particularly when it comes to issuing and managing keys and credentials.

REFERENCES
Interactive Master Key System Design Guide, Assa Abloy, 2008
Guide to Developing and Managing Key Control Policies and Principles, Medeco, 2005
Facts and Fiction About Duplicating Keys, Assa Abloy
[1] University of Massachusetts at Amherst website, 2012