

Key Management – Threats and Solutions

Who has the keys?

Key management and control is a critical aspect of security systems for many institutions, buildings and campuses. There is a mistaken belief among some that the use of traditional mechanical keys is becoming less important with the proliferation and evolution of sophisticated access control technology. The fact is that traditional mechanical keys are more commonplace than ever, and today's security awareness dictates that the possession and location of these keys be tracked, monitored, and managed effectively. Casinos, convention centers, healthcare, residential and commercial property management, educational institutions, government, transportation/delivery, auto dealerships, and prisons are among the common users of good key management systems.

The need for and evolution of key management systems will be addressed, as well as the current state of technology, network architectures available, legal compliance needs, and cost-benefit analysis will be examined.

A typical key management system is characterized as:

- 1). Keys are secured in a locked (or unlocked) enclosure and each key is assigned a physical and logical location (or a hook as in the more primitive systems).
- 2). Each key or key bundle may be assigned to an individual whose security credentials permit the use of that key during that time period. Authority systems range from a guard identifying and issuing keys in primitive systems to automated locking, release, tracking and timing system in advanced systems.
- 3). Returned keys are logged in (electronically or in writing) providing management with a report of when and to whom the keys were issued and whether keys are available or remain out.

There are three basic key control system architectures:

1). Manual/Primitive - key possession is tracked and/or controlled by a sign out sheet and the oversight of administrative and/or security personnel. This method is labor intensive susceptible to human error; there is no way of generating an automatic report in case of key non-return.

2). Mechanical/Electronic - Metal to metal contact identification technologies have been available for over 20 years. These contact “chips” and similar systems rely upon electrical point-to-point contact points of the device attached to the key. Keys are fundamentally mechanical devices subject to abuse and frequent exposure to dirt and moisture (“the mud, the blood and the beer” to paraphrase Johnny Cash). These same mechanical devices are, for secure operations, dependent upon electrical contact points which are subject to failure and high maintenance due to the normal wear and dirt acquisition of the contacts.

3). RFID/Contactless - The newest form of key management systems is based on contactless RFID technology (similar to but more rugged than traditional Prox cards). An RFID tag is embedded into a non-destructible key fob, which is docked into a round port in the key board. RFID technology is maintenance-free and the contactless identification capability of the Fob can be used for additional purposes related to access and control efficiency. The first system of this type (<http://www.proxsafe-usa.com/>) was introduced by Deister Electronics USA, Inc.



Network Architectures:

Smart Key Management is essentially an Access Control System for assets. Such systems can be configured in three different topologies:

A. Stand Alone: Until 4-5 years ago nearly all such systems were configured stand alone. The system embeds an Access Database and log locally and operated without centralized oversight. Data and changes are periodically updated and uploaded by system management.

B. Networked: Multiple systems, often at multiple locations (from a few feet to halfway around the world apart) comprise a single overall key management and access system. Management is from a browser accessible server and the system resides on the local IT network with full Web Access capability. A single database governs and records events and authority for all locations. Networked systems must also have fallback for all systems to operate effectively in standalone mode should temporary failure of the network occur.

C. Integrated: Key management is really access control. From a logical and administrative standpoint, a key (or key bundle) is really a kind of door object. The most advanced systems have open protocols that may be integrated into classic Access Control to take advantage of single databases, single management and the overarching security needs of an organization.

Cost-Benefit:

Misplaced keys cost organizations in North America approximately \$35B annually in inefficiency, shrinkage, liability and lock replacement costs. Automated, electronic key management systems typically have a payback of less than 12 months when all of the risks and costs are analyzed.

Electronic Access Control has become a staple of the tools available to Security Directors within and outside of government to increase and manage security requirements within their arc of responsibility. Yet, relatively few of these same sophisticated executives have incorporated physical keys into their Threat Analysis. Great care is taken with access through doors to sensitive areas while some of the organizations highest risk areas are accessible by physical keys loosely managed with a sign-out list.

As increasing numbers of Security Directors assess the risk posed by uncontrolled physical keys and as more and more sophisticated Access Control systems (especially in response to such mandates as FIPS 201-1) integrate key control into the broader access control capability set, electronic key management is destined to achieve an equivalent ubiquity.

Summary:

Electronic contactless RFID key management systems offer efficiency, security, aesthetic beauty and are most cost-effective over time. As the most popular choice among users at many levels (facility management, security, IT, etc.), the RFID technology method of key management is destined to be the most obvious solution for a universal realm of applications in the future.