

Making the Business Case for Smart Credentials

Alexandra Brickl, Ingersoll Rand Security Technologies, Portfolio Marketing Specialist, Credentials and Readers

Today's security management team is becoming bewildered by the increased need for personnel safety and asset security while, at the same time, being asked to oversee keys, codes and various types of cards used in a multitude of applications that require a credential. What can organizations do to meet these conflicting desires in a cost-conscious manner?

Managers are learning that they get their best return-on-investment (ROI) with smart credentials. Within a smart credential, a microchip stores, protects and modifies information, providing many opportunities for information sharing and exchange.

They provide companies, schools, hospitals and other organizations with a more open and secure contactless solution than other card products. Not only can the smart credential provide added security and convenience over other cards, including proximity cards, it offers a complete array of applications

Increased Security at a Similar Investment

Secure access solutions available with smart credentials have important ROI implications. Most important is protecting the safety of employees and visitors. In today's environment, programs that foster increased facility security are on the forefront of every security director's mind. It is not possible to put a figure on the potential damage that an organization could suffer by unauthorized individuals using authorized users credentials. By issuing their staff credentials with strong authentication mechanisms, companies are effectively investing in their well being and demonstrating that they take security seriously.

At the core of an access control system is the need to stop unwanted individuals from gaining access to facilities. Companies require systems that minimize the prospect of equipment and intellectual theft. Such losses could prove costly both in terms of the dollar value of replacing the equipment and the loss of data and information (e.g. stored on laptops). Insurers are highly likely to raise their premiums in light of a major breach of security. The effect of equipment theft is also highly likely to impact staff productivity in the short term, due to a lack of equipment and potentially ensuing stress.

In comparison to door keys, magnetic stripe cards or proximity cards, the inherent security of smart credentials ensures that they are more difficult to duplicate. For instance, the new aptiQ™ smart card from Schlage, using MIFARE DESFire™ EV1, offers four different layers of security:

1. **Mutual authentication** ensures that the reader and the card are allowed to talk with each other before any information is exchanged.
2. **AES 128-bit encryption** is a key encryption technique that helps protect sensitive information.
3. **Diversified keys** virtually ensure no one can read or access the holder's credentials information without authorization.
4. **Message authentication code (MAC)** further protects each transaction between the credential and the reader. This security features ensures complete and unmodified transfer of information, helping to protect data integrity and prevent outside attacks.

By introducing smart credential-based authentication, a facility can immediately reduce the number of staff members needed to manage and control access to laboratories, data centers and other buildings that only authorized staff should enter, allocating these employees to areas that will create greater productivity. By demonstrating their reduced risk in terms of intruders gaining access to their facilities, organizations can affect marked savings on insurance premiums.

With the price of smart credentials being comparable to proximity cards, there is no reason not to deploy smart credentials immediately, even if the only application will be physical access control. A smart credential, for a comparable price, provides a much higher level of security than today's most popular card credential, the proximity card.

And, in those smart card programs introduced for password control, an organization immediately solves the problem of (forgotten) passwords, a nemesis for both users and administrators. The organization will reduce overhead costs simply by not having to administer passwords.

More Applications at a Reduced Investment

In addition to their increased security capabilities, smart credentials can be used to host multiple applications, letting organizations consolidate many services on one card, producing cost savings and increased efficiencies. From checking out parts at the factory depot and buying lunch at the company cafeteria to passing a biometric

verification for security at the data center, contactless smart credentials are convenient—one credential has the ability to provide many features –

- Identification
- Check out privileges
- Building access
- Cafeteria and vending machine purchases
- Charge privileges at organization stores
- Admission to corporate events
- And many more.

With limiting to only one the number of credentials each authorized recipient needs, organizations can put all the people needed to manage multiple credentials programs to better, more productive use.

Looking at the ROI Benefits of Smart Cards

More security at the same price and more applications at a lower price – it's really that simple why smart cards are quickly becoming the most popular choice for credentials.

-30-

455-111610