By issuing staff credentials with strong authentication mechanisms, healthcare organizations and universities are effectively investing in their well-being and demonstrating that they take security seriously.

What Smart Cards Can Do for Your Campus

Smart credentials improve physical and logical access control, and help improve campus business functions. Selecting the right technology and laying the groundwork for deployment are the keys to success in upgrading your systems.

Written by: A member of the Allegion Healthcare Marketing Team

It's not easy to create and maintain a healthcare or educational environment that acts as an asset in delivering quality service. All too often, systems and technologies purchased to improve business objectives and processes can create more complexity than intended for the people using them. For example, there has been a significant increase in the number of card access control systems, which is a wise move because the use of credentials can offer increased security and data exchange. However, sometimes these systems have been added in a vacuum and not through collaboration with other departments. If each department is doing it this way, users of the systems could end up using a different credential for each of the functions they do throughout the day and feeling frustrated over the complexity.

Healthcare and university staff members and college students often use different credentials throughout their day to do basic functions. It could be entering the building, signing on to their computers, checking out supplies or paying for lunch. And if they work at or attend two or more facilities, the number of credentials they need to use multiplies. The time required each day to find the correct credential for each function can be frustrating and decrease productivity and customer satisfaction.

Fortunately, smart cards can provide one credential for a multitude of tasks. Additionally, they provide greater security, allow for fewer PIN codes and passwords, and simplify duties.

Smart Credentials Can Lead to Efficiencies
The use of smart credentials or smart cards can make staff more efficient and increase their job satisfaction. Besides access control, smart credentials can support various applications such as identification; parking access; time and attendance; logical access; supply check-out verification; charge privileges at various locations, including the cafeteria; document printing; and biometric template storage.

In addition to the functionality for multiple applications, smart credentials also increase the security of information kept on the card and stored in the facility. If applications require multiple forms of verification, the smart card securely stores other credential types, such as biometric templates, PIN codes and photos, right on the card, utilizing the enhanced storage and encryption of smart technology. It also
Access privileges to events such as concerts and sporting events can be managed with smart cards.

provides an extra level of security at the access point, protecting the information behind closed doors or on the secure network.

Issuing one smart credential also impacts administrative costs. Not only is the cost of a single credential lower than purchasing multiple forms of identification, but the reduced management and distribution time for one credential will have a significant impact on administrative costs.

Most important of all is protecting the safety of employees, patients, students and visitors. In today's environment, programs that foster increased facility security are on the forefront of every campus security director's mind. In comparison to door keys, magnetic stripe cards or proximity cards, the inherent security of smart credentials ensures that they are far more difficult to counterfeit. It is not possible to put a dollar amount on the potential damage that an organization could suffer by unauthorized individuals using authorized users' credentials. But, by issuing staff credentials with strong authentication mechanisms, healthcare organizations and universities are effectively investing in their well-being and demonstrating that they take security seriously.

**Smart Credentials Offer Quick Payback**

With all of this added security and functionality, one would expect the cost of smart card credentials to be much higher than the standard proximity card that is in use today. In fact, the price of smart credentials is comparable to proximity technology, so there is no reason to delay the deployment of smart cards, even if initially the only application will be physical access control.

Not only will campuses reduce the cost of purchasing a variety of credentials, they will save on the cost of managing multiple credentials. Plus, the hospital, university or district will be able to incorporate applications that were being delayed because of the cost of additional credentials. One card will do it all.

**How to Lay the Groundwork for Smart Credentials**

It is very important that campuses be prepared for smart credential deployment, even if the facility wants to continue using the proximity, magnetic stripe or keypad readers that are already installed. One way to start preparing for the migration to smart cards is to deploy multi-technology credential readers and electronic locks that combine the ability to read both proximity cards and smart cards in just one reader as new installations take place. This way, when the organization makes the transition to smart cards, it won't have to replace all of its current devices when the move happens. During the transition, current staff members will be able to use their current credentials and new employees can be issued and start using the new smart cards. This allows the institution to transition the rest of the staff on a reasonable timeline and according to budgets.

Also, choosing the right smart card can make all the difference when trying to use them with applications other than access control. Campus decision makers should look for platforms that are open format rather than proprietary. Open formats allow easy integration into other applications with minimal programming, speeding up the time of deployment, reducing the cost of implementation, and giving campus officials more freedom to get the most out of their investment.

**Be Smart about Your Next Choice of Credential**

Hospitals and universities can immediately begin budgeting for and deploying smart card technology in their facilities. Smart credentials will deliver increased security to staff, patients, students and visitors while providing campus employees with increased functionality and efficiencies. Deployment is easy, and migrating can be stress free when using the right solutions.
Smart Cards: What Are They Exactly?

Within a smart card, a microchip allows information to be stored and modified right on the credential. This means that information can be both read from and written to using compatible devices. This differs from the popular proximity credential because information on this card can only be read. The increased functionality of smart cards offers campuses greater flexibility in how credentials can be used.

While functionality is very important to the purchasing decision, increased information storage and transmission makes security one of the top reasons to choose the right credential when implementing a successful credential strategy. Some smart cards offer several different layers of security, including mutual authentication, which ensures that the reader and the card are allowed to talk with each other before any information is exchanged. Smart cards can also provide encryption.

Diversified keys, another component of some smart cards, can virtually ensure no one can read or access the holder's credential information without authorization. A message authentication code ensures complete and unmodified transfer of information, helping to protect data integrity and prevent outside attacks.