A smart way to sell healthcare facilities

Ann Geissler Timme, Healthcare Marketing Manager, Allegion

Hospitals and other healthcare facilities operate in a complex, ever-changing environment. Staying ahead of technology trends, creating a safe, secure, and yet welcoming environment and most importantly, providing the highest quality of patient care as possible are important goals of any healthcare organization.

Security integrators that can contribute to these goals will be seen as a valuable partner as initiatives are moved forward. One area that touches on many aspects of a healthcare facility’s operation is the credential/ID strategy.

Think about this, a hospital’s employee wears a lanyard with a magnetic stripe ID badge with a barcode printed on it. In addition, she must remember two different PIN codes for offline keypad locks, carry keys for cabinets and a proximity card to access the institution’s other facility. She finds it frustrating to find and use the correct credential for the function she needs to accomplish – whether moving through the facility, using the time and attendance system, logging into the Electronic Medical Records (EMR) or diagnostic imaging review workstations, or accessing supply closets. Integrators are in a great position to help their healthcare customers implement a more efficient, secure credential strategy.

If we review the typical healthcare facility access control system, in all too many cases, its components were installed in stages by various departments and using different manufacturers’ equipment. As a result, the system is comprised of different brands and disparate products, many of which do not interface with each other, causing physicians and employees to use different credentials throughout their workday.

But what if there was one credential that could do it all...one credential that could be used with most systems in the facility? One credential for the staff to carry and easily accomplish multiple tasks? One credential that was secure enough to meet even the toughest standards? One credential that meets their business objectives? Smart cards can do just that.

What smart credentials can do for a healthcare facility

Besides making access control more convenient, smart cards can be use for time and attendance, logical access, cashless vending and cafeteria payments, and checking out scrubs and medical equipment just to name a few. Right now, it’s likely that a different credential type is being used with each system. And different departments are managing those credentials. Smart cards make it possible to consolidate all of those functions onto one credential, creating an efficient environment where staff would have only one credential to use throughout their day.

Issuing one smart credential also impacts administrative costs. Emphasize that not only is the cost of a single credential lower than purchasing multiple forms of ID, but the reduced management and distribution time for one credential will have a significant impact on productivity.
In addition to the advantages of their functionality for multiple applications, it is important for integrators to show healthcare security administrators how smart credentials also increase the security of information kept on the card and stored in the facility. In comparison to door keys, magnetic stripe cards or proximity cards, the encrypted security of smart credentials ensures that they are far harder to counterfeit. It is not possible to put a dollar amount on the potential damage that a healthcare organization could suffer by unauthorized individuals gaining access to restricted areas of the facility or private patient records. By issuing their staff credentials with strong authentication mechanisms, healthcare organizations are effectively investing in their wellbeing and demonstrating that they take security seriously.

For higher-security applications that require multiple forms of verification, the smart card also has an advantage as it securely stores other credential types such as biometric templates, PIN codes and photos right on the smart card. This provides an extra level of security at the access point, protecting the information behind closed doors or on the secure network without added inconvenience to the user.

You will get kudos from IT

When presenting a smart card solution, be prepared for representatives from the IT department to take notice. As in many other industries, more and more healthcare security system decisions are being made with input from the IT department. And we’re seeing increased convergence of physical and logical security team structures in light of recent widespread adoption of EMR and other hospital systems.

IT professionals want strong authentication credentials, the level of security provided by smart cards. Contrary to proximity cards and their readers, smart cards go through a challenge and response sequence to initiate conversations with the network. Communications are encrypted using industry standard encryption techniques. By welcoming their involvement and showing ability to speak their language and answer their questions, you will gain additional layers of approval within the IT organization.

Another partnership that may also prove valuable is collaborating with hospital IT systems integrators. Healthcare providers are already working with this segment of integration experts in their implementation of EMR and other technologies.

Just as you are expert in physical security integration and have strong relationships with your customers, building relationships with an IT systems integrator could broaden both companies’ customer bases and build your combined reputations as innovative service providers.

Not all smart cards are created equally

While functionality is very important to the purchasing decision, increased information storage and transmission makes data security one of the top reasons to choose the right credential when implementing a successful credential strategy. The IT department, specifically, will be very involved in what type of smart cards and readers are specified for this reason. While all smart cards are more secure than other credential technologies, one stands far above the rest.

Smart cards utilizing MIFARE DESFire™ EV1 technology, such as aptiQ™ from Allegion 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 using MIFARE DESFire EV1 will also provide –

- AES 128-bit encryption, a key encryption technique that helps protect sensitive information.
- Diversified keys which virtually ensure no one can read or access the credential’s information without authorization.
- Message Authentication Code (MAC) which 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.

Also, choosing the right smart card credential can make all the difference when trying to use them with applications other than access control. Look for platforms that are open format rather than those designed for proprietary systems. Open formats allow easy integration into other applications with minimal programming, speeding up the time of deployment, reducing the cost of implementation, and giving your customer more freedom to get the most out of their investment.
How to lay the groundwork for smart credentials

It is very important that healthcare organizations be prepared for smart credential deployment, even if the facility wants to continue to use the proximity, magnetic stripe or keypad readers that are already installed. One way to help them 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 using a single device as new installations take place. This way, when the organization makes the transition to smart cards, they won’t have to replace all of their current devices when the move takes place. 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 card credentials. This allows them to transition the rest of the staff on a reasonable timeline and according to budgets.

By helping your healthcare customer set a sound credential strategy and consolidating the number of credentials in use at their facility, you will help them make their employees more efficient and satisfied in their job which, in turn, creates a more secure and productive environment in which supports everyone’s number 1 goal – quality patient care.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit allegion.com.