DECREASE SECURITY THREATS WITH ENHANCED SMART CARD TECHNOLOGY

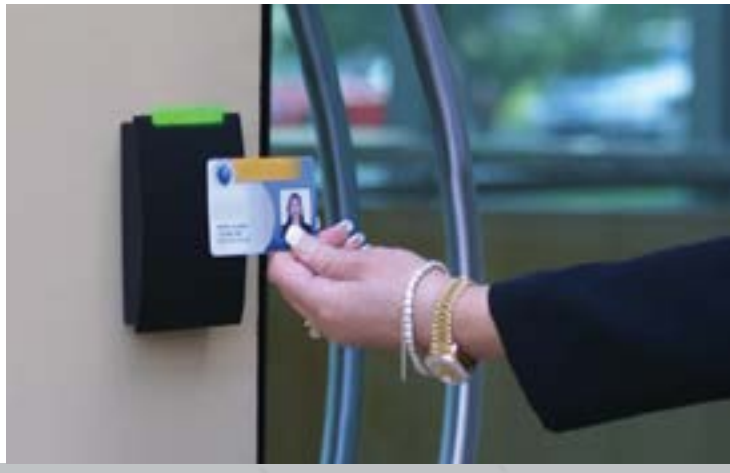
Security101®

Security in numbers.
Service that counts.

DECREASE SECURITY THREATS WITH ENHANCED SMART CARD TECHNOLOGY

For certain government organizations, physical security measures must keep pace with evolving political climates in order to protect valuable assets, confidential information, and public officials. While many have made security upgrades to video surveillance and alarm systems, it's important to also consider the new technologies within the realm of access control, such as the rising trend of smart card usage and smart devices versus using more traditional access cards or even mechanical keys and locks.

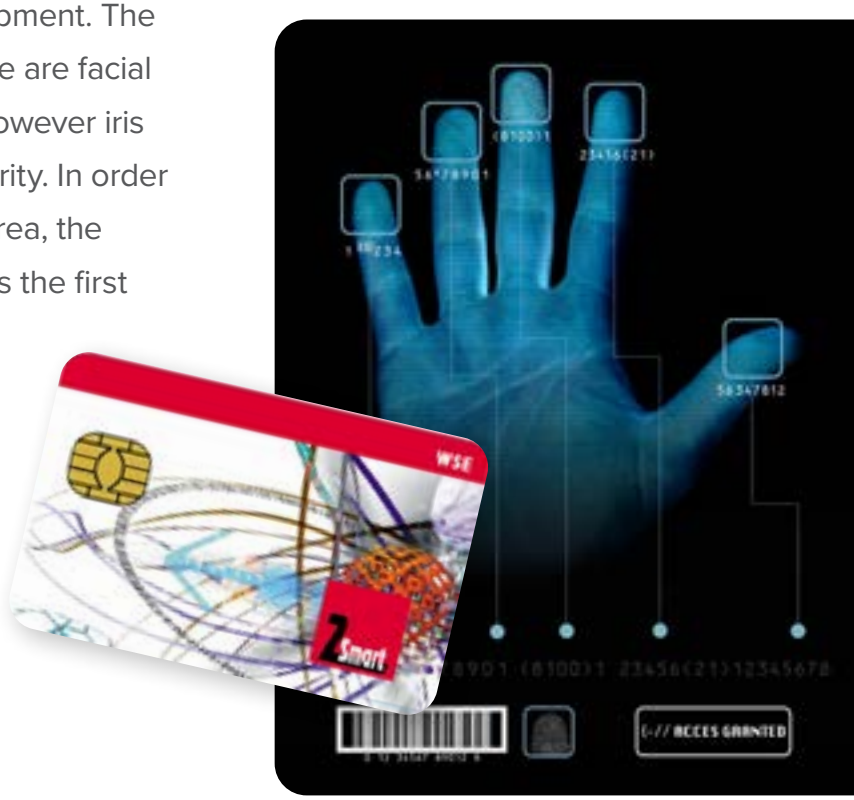
Migrating from traditional mechanical locks to smart cards as part of an access control system is a wise move for government institutions that require staff to typically carry keys in order to gain access to offices or certain departments. One lost set of keys can sometimes involve changing all the locks and rekeying all the keys, which results in an unexpected cost of time and resources. Magnetic stripe cards are a slight improvement, but over time they can wear and be prone to damage, causing users to replace their IDs more often and the administration to spend more maintenance on keeping the card readers functional. Proximity cards that use a low frequency 125 KHz RFID transmitter are a little more convenient since they are contact-free and fast, but the credential within the card is technically a generic serial number that can be cloned very easily with an inexpensive device available on the internet. Smart cards, however, require a two-way exchange of information between the 13.56 MHz chip on the card and the card reader. This mutual verification works as a "secure handshake" because the exchanged information is encrypted, decreasing their overall vulnerability.



The switch to a sophisticated electronic smart

card-based access control system is ideal for a medium to large sized government organization with dozens of users and a variety of “access zones” that correspond to different departments. Utilizing an integrated managed access software interface, system administrators are easily able to determine which areas each card can access. For example: an employee can have access to multiple areas but is restricted from others; custodial workers can have access to all areas but only during off hours; an intern may have access to a small number of areas and only for the duration of the internship. The software also is able to provide an audit trail of users’ access, improving visibility and accountability. And perhaps most importantly, the management software can enable instantaneous, facility-wide lockdown of zones and offices in case of emergencies.

For government entities that require an added layer of secure access, implementing two-factor authentication tactics by integrating biometric technology with smart cards is popular option thanks to considerable advances in biometric processing abilities and equipment. The most common biometric credentials in use are facial and fingerprint recognition technology, however iris and palm recognition is gaining in popularity. In order to be granted access to an ultra-secure area, the user must present his or her smart card as the first credential, and then the biometric data credential afterward. This is especially useful for when an individual without access tries to use a lost or stolen card to gain unauthorized access; since the credentials do not match up, no access is granted and a security breach is prevented.



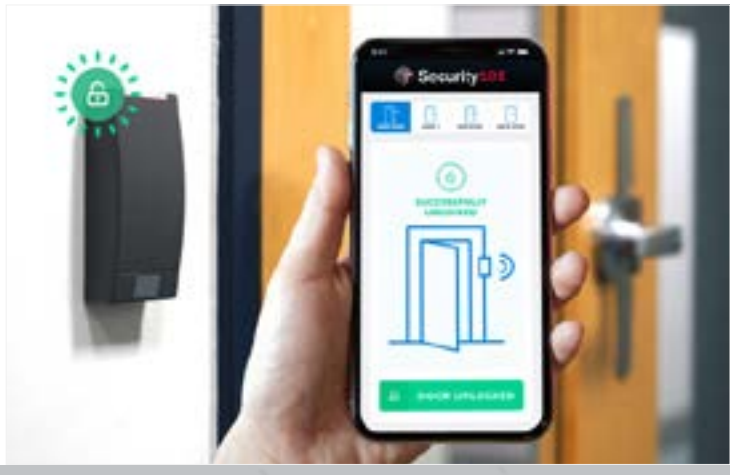
One last benefit of smart card technology is its multi-purpose use. If embedded with a contact chip on the front face of the card, such as the ones on EMV credit cards, employees can load a sum of money onto their smart card and use it for cashless payments. This is especially handy for paying for food in the cafeteria or items from vending machines and even on transit systems.

Governmental organizations with strict security needs should consider an upgrade to newer technologies to safeguard against unknowable threats to sensitive areas of operations. The ideal access control system is unobtrusive, user-friendly, and employs state of the art technology as it seamlessly scans the needed credentials to reliably control access to anywhere throughout the facility.

STREAMLINE YOUR ACCESS CONTROL SYSTEM BY INTEGRATING MOBILE CREDENTIALING.

In today's digital age with the prevelance of smartphones, streaming and everything trending towards mobile, it's no surprise that a recent study by Gartner suggests that 20% of organizations will use smartphones in place of traditional physical access cards over the course of the next year.

Now you can eliminate the need for keycards and heighten the integrity of your organizations security by using your smartphone and mobile credentials to open your office doors. Mobile credentialing provides convenient features that naturally compliment an end users lifestyle with ease making it a modern, secure and smarter choice for your organization.



Mobile credentialing is:

More Secure

Mobile phones are one of the most secure devices and cannot be cloned like a keycard.

Also, you can enable 2FA (Two Factor Authentication) so that a user needs biometrics to unlock their phone via thumbprint or FaceID in order to use their mobile credential.

Convenient

Employees no longer have to carry their keycard with them, their smartphone becomes their keycard. One less thing to worry about. You also have the ability to remotely unlock a door for a visitor even if you are not at the office and if you have multiple offices, you no longer need to carry different cards, all entries are stored in your app.

Cost Effective

Mobile credentials are managed in the cloud, so you no longer need to have a dedicated physical server on site to manage. Another added benefit is that they reduce the need for purchasing, issuing and replacing keycards, fobs and badges and can free up an administrators time allowing the to focus on other projects and tasks.

Transition to top-tier security for your institution by implementing mobile credentialing, a smarter access solution that's always within arms reach.