READERS AND CREDENTIALS FOR ACCESS CONTROL

Migrating to Higher Security

Since the 1970s, proximity technology readers and credentials have been the standard for electronic access control systems. Proximity technology uses a radio frequency to power the credential and transmit the card number to the access control panel to verify that the card number is authorized to enter a secured area. This is what is called single directional verification. With the increasing number of proximity access cards and aftermarket manufacturers now able to produce proximity credentials, card number duplication is becoming a reoccurring problem.

New Standards and Technologies

In February 2005, the U.S. government issued a Federal Information Processing Standard (FIPS 201) that outlined a higher security standard for access control credentials. This standard included using smart card technology. Besides having the ability to store information on the credential to positively identify the user, smart card technology uses an encrypted two-way communication between the credential and the reader to authenticate the credential before sending the information to the access control system.

In its early development, smart card technologies were cost prohibitive in commercial access control systems. However, smart card readers and credentials today cost slightly less than standard proximity readers and credentials. Because smart card readers can communicate in Wiegand format, smart card readers and credentials can be seamlessly installed when deploying a new access control system.

Upgrading Existing Proximity Technologies to Smart Card Access Control Systems

Upgrading the reader and credential security in an existing access control system is done by using multitechnology readers and credentials. Multitechnology readers incorporate internal antennas to energize and read multiple formats of cards including standard 125 kHz proximity and 13.56 MHz smart card credentials. These readers use the same wire connections as standard proximity readers, which means they can integrate into any access control system and are able to read existing proximity cards and higher security smart cards.

Multitechnology credentials have built-in proximity and smart card technology and can replace existing proximity cards. These credentials will work on existing proximity readers and upgraded multitechnology and smart card readers.

Multitechnology readers and credentials can be integrated into an existing access control system until all of the legacy proximity readers are replaced. Once all of the proximity readers are replaced with multitechnology readers then anytime a new credential is issued, a smart card is issued. This allows the access control system to be seamlessly upgraded over time

Advantages of smart card technology readers and credentials:

- Higher security with a bidirectional authentication between the reader and credential
- Lower cost of readers and credentials
- Credential duplication is eliminated
- Smart cards have the ability to store information onboard for multiuse applications

Anixter Solutions

Even though technologies shift and standards change, Anixter keeps you up to date with the latest products and best practices. Anixter partners with best-in-class manufacturers to bring you the right access control products for your solutions and can offer the technical expertise to help you select a system that fits your needs today and in the future.

For more information, contact your local Anixter representative or visit anixter.com

About Anixter: anixter.com/aboutus
Legal Statement: anixter.com/legalstatement

13T2679X00 © 2014 Anixter Inc. · 04/14