Keyscan Access Control Systems

Understanding Keyscan credentials

In access control applications a specific credential is assigned to authorized users in a facility. When a user presents a credential to a reader, the reader reads and/or decrypts the credential's stored data and sends the data to the Keyscan access control panel.

The control panel compares the credential data to user and permission criteria established in Keyscan Aurora Access Control Management software. The system then grants or denies access and records the transaction to the database.

Typically, a credential is a card but it can also be a fob or adhesive tag. Each contains stored data which identifies and enables an authorized individual access to, or within, a controlled facility. There are many credentials technologies and formats.

We will differentiate the Standard 26 bit format from Keyscan's 36 bit proprietary format.

The Standard 26 bit Format

The Standard 26 bit Format is an "Open" format and is unregulated with credential manufacturers. The open format means there is no regulated convention controlling the issue of data contained in the credential. As a result, virtually anyone can buy this type of credential for use in any access control application. This means duplicate credentials can exist.

As a result, a 26 bit format credential in use for one particular facility may also inadvertently function in another unrelated facility. Albeit unlikely, it can happen.

Almost all access control systems can be programmed to accept standard 26 bit credentials. They are an inexpensive option and while they do offer a benefit over traditional keys, there are more secure credential formats available for use with your access control system.

Keyscan's Proprietary 36 bit format

Keyscan differentiates itself from the competition by offering a 36 bit card format structure that is unique and exclusive to Keyscan. This format is closed and restricted.

The Keyscan 36 bit format credentials are available exclusively through Keyscan. This promotes a high level of security for Keyscan system users because the credentials are regulated strictly. No duplicate cards will exist and only a Keyscan 36 bit format credential will work in a facility using Keyscan Access Control Systems.
As a result, Keyscan systems are factory defaulted to read Keyscan 36 bit credentials.

Low Frequency credentials vs High Frequency credentials

A proximity or "prox" card is an access control term for a type of card credential that functions in an access control environment.

The term "proximity card" means it functions when it is presented in proximity to a reader device. When the card enters a reader's 'proximity', the card number and coding is transmitted.

Over time the term "Prox Card" has become tantamount with 125 kHz (low frequency) access control devices. In contrast, the "smartcard" is distinct to more modern 13.56 MHz (high frequency) access control devices. However, both are still "proximity" by definition and function when placed in various proximity to a reader.

125kHz (low frequency) credentials

The first of the proximity technologies was 125 kHz. When a 125 kHz card enters a reader's proximity range, it immediately begins to transmit a card number. Being a low frequency system, it is possible to create a device that will 'power up' a card from a distance, the same way a reader would, then read the data being transmitted. This is called Sniffing. Sniffing, makes 125 kHz (low frequency) credentials vulnerable to reproduction.

13.56MHz (high frequency) credentials

There are many types of high frequency credentials. This includes Mifare DESFire EV2, Mifare, iCLASS, iCLASS SE and recently iCLASS SE with Seos pro file. There is also UHF (ultra high frequency) technology better suited for parking and long range applications. These technologies were all created to address the vulnerability of 125 kHz technology by enabling two-way communication between the credential and reader.

When 13.56MHz high frequency credentials enter a reader range, the credential and reader begin a secure communication session using shared encryption keys. Once this is established, the card number is transmitted. The communication session is closed off. This process makes high frequency cards more secure than their low frequency counterparts.

Keyscan's K-SECURE 1K/4K with K-SMART3 high frequency readers use this trusted technology offering much greater security than low frequency credentials.

For more detailed information about available credential types and formats, contact your dormakaba EAD regional sales manager.

dormakaba Canada Inc.
901 Burns St., E.,
Whitby, Ontario
Canada L1N 0E6

1 888 539 7226

www.dormakaba.us