

- Uses internationally recognized Mifare contactless smartcard technology
- K-SECURE 13.56MHz contactless smartcard credentials provide the highest level of credential anti-counterfeiting protection
- K-SECURE Mifare contactless smartcards comply with international interoperability (ISO14443) standards suitable for 3rd party applications (eg. logical network access and cashless vending)
- Regular HID 125kHz credentials simply transmit their card number in the open
- Industry standard 26bit HID 125kHz credentials further expose the end-user to potential card duplication and easily ordered duplicate card and batch numbers
- K-SECURE smartcard credentials work in combination with Keyscan's K-SMART reader



#### HOW K-SECURE WORKS:

- 1) Card enters reader excite field
- 2) Card transmits an encrypted 'Max Secure Code' to the K-SMART reader
- 3) The K-SMART reader decrypts the 'Max Secure Code' and authenticates the provided code
- 4) The reader then completes a 3 pass authentication encryption/ decryption unlock algorithm with the card
- 5) The K-SECURE credential then transmits its secured access control identification
- 6) The K-SMART reader passes the cards access control identification to the controller using Keyscan's proprietary 36bit Wiegand protocol.

#### THE RESULT:

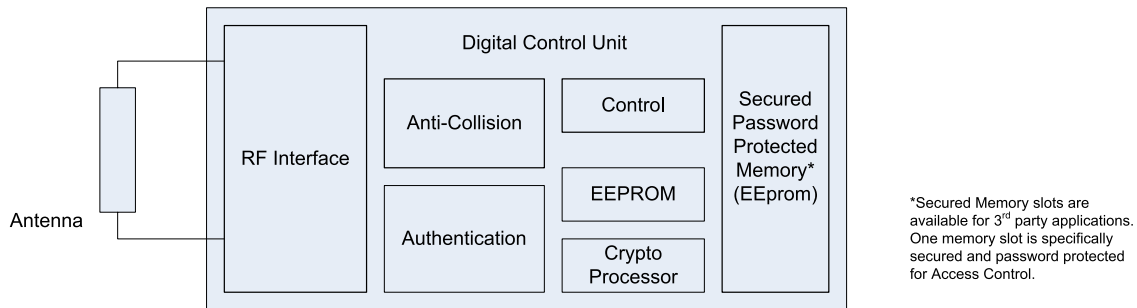
- Higher credential security and increased protection against card counterfeiting
- Keyscan assures no duplicate cards are created
- Keyscan's 36 bit Wiegand output from reader to panel adds a further level of security

### Features and Benefits

- Uses industry proven MIFARE smartcard technology
- Provides credential anti-counterfeiting protection
- Removes concern of duplicate HID 125kHz 26 bit cards

### Card Memory & Security Algorithm Diagrams

K-SECURE Contactless Smartcard – Built in Security, Built in capability for support of 3rd party applications



K-SECURE Security Algorithm



HID 125kHz cards or Mifare nonproprietary cards



1. Card Enters Readers Excite Field
2. Card Transmits MAX Secure Code
3. Reader Validates Max Secure Code
4. Reader Initiates 3 Pass Authentication Algorithm, Sends Secure Sector Unlock Code
5. Reader Transmits Secure Sector Access Identification Code
6. Reader Passes Card Details using 36 bit Wiegand Output to Keyscan Panel

K-SMART Reader



6) 36 bit Wiegand Output to Keyscan Panel



- 1) Transmit Card Serial Number