

# What are the general differences between the following card types?

## *Proximity, MIFARE<sup>®</sup>, MIFARE DESFire<sup>®</sup>*

While their general appearances may seem similar, not all cards are created equal. It's important to understand the general differences in card types, as the corresponding reader will need to match the card's capabilities to fully benefit from the available feature sets and wide array of security parameters. Cards are becoming increasingly more sophisticated in terms of encryption, virtualization and mobile applications.

### **Proximity or Prox Cards**

Standard proximity cards operate at 125 KHz (low frequency), and are from 26 to over 60 bit of format. The primary function of the microchip embedded within a proximity card is to provide the prox card reader with the card's identification number and/or site facility code so that it can be verified and access granted. The typical access control system only reads the identification numbers from a prox card when presented. Prox cards do not have the capability to store additional information, and are commonly used for door access. Prox cards are contactless and replaced cards requiring direct contact or insertion, such as Wiegand and magstripe technologies.

- 125 KHz (low frequency)
- 26 to over 60 bits, Contactless
- Commonly used for Door Access and Parking
- No storing of additional data

### **MIFARE<sup>®</sup>**

An evolution of "smart" cards, MIFARE cards operate at a frequency of 13.56 MHz (high frequency), and offer higher card ID number capacities. These cards are designed to keep sensitive information safe by utilizing encryption keys. Data is not emitted until both the MIFARE card and reader mutually authenticate each other, handshake. MIFARE provides several "user" data areas that can be utilized by other applications called data sectors and is secured by a key which is only

known to the application. In addition to the user sectors, MIFARE cards are manufactured with a randomly generated 12 digit number or Card Serial Number (CSN). The CSN is sometimes used as the card identification number due to the uniqueness of the number.

MIFARE cards were originally developed for transportation payment transactions in Europe. MIFARE cards can contain both authentication and identification information, as well as additional useful information within the card's embedded microchip and memory (usually about 1 kilobyte of data can be stored). MIFARE cards can contain multiple credentials and can be programmed to be used for cash card payments or pre-paid memberships.

MIFARE was originally developed by Mikron during the early 1990's. The term Mifare actually refers to the Mikron FARE-collection System. Later in 1998, it was obtained by Philips under the label of NXP. The Classic 1k chip from MIFARE was introduced in the year 1994 and was licensed by the firm Infineon Technologies. Infineon Technologies also produced the Infineon MIFARE 1k that is technologically compatible with the Classic series.

- 13.56 MHz - RFID Smart Card
- Uses Encryption Keys
- Limited to 1k of stored data
- Commonly used for ID purposes, Card Payments, Loyalty Programs

*Continues...*

# What are the general differences between the following card types?

## *Proximity, MIFARE<sup>®</sup>, MIFARE DESFire<sup>®</sup>*

*Continued...*

### **MIFARE DESFire<sup>®</sup>**

The MIFARE DESFire family of cards consists of the EV1 and EV2. MIFARE DESFire chips contain a full microprocessor, and with much more robust security features compared to MIFARE Classic. They are based on open global standards and designed to be interoperable (to work with other systems and manufacturers). They are a contactless, scalable solution for multi-applications, such as identity, access, transportation, loyalty and closed-loop micropayments. They are fully NFC (Near Field Communication) capable.

These cards contain an on-chip backup management system and mutual three pass authentication, the EV1 smart card can hold up to 28 different applications and 32 files per application. The EV2 can hold an unlimited number of different applications, limited only by the memory size. New applications can be loaded after the card has been deployed into the market. The DESFire family of cards is flexible and convenient, offering increased transfer rates, security and reliability among consumer-friendly design. Data can even be shared between applications, for increased interoperability.

The “DES” in the name refers to the use of DES, 2K3DES, 3K3DES and AES hardware cryptographic engine for securing transmission data, while “Fire” is an acronym for “Fast, Innovative, Reliable, and Enhanced” operation in contactless proximity applications.

- 13.56 MHz - RFID Smart Card
- Interoperable, Contactless, Scalable, Consumer-friendly Design
- Open Global Standards
- On-chip Backup Management
- EV1 can hold up to 28 applications and 32 files per application
- EV2 can hold an unlimited number of applications, limited only by memory size
- EV2 is backward compatible to EV1
- EV2 utilizes virtual smart card architecture for privacy protection
- Multi-application smart card solutions for campuses, corporate and student ID, access management, transportation, loyalty and micropayment applications