

SOFTWARE HOUSE

Smart Card White Paper



Smart cards are more than collectible replacements of a wallet full of plastic cards. Unlike the read-only plastic card, the processing power of smart cards gives them the versatility needed to make payments, to configure your cell phones, and to increase secure access control with biometrics.

This document presents an overview of smart card and its application focusing on the MIFARE technology.

Table of Contents

What is a Smart Card?	3
ISO Standards	4
MIFARE® Overview	5
MIFARE Technical Specification	5
Security	6
Software House Multi-Technology Reader	7

What is a Smart Card?

A smart card is a standard-size plastic card with an embedded integrated circuit chip which has memory and microprocessor functionalities. There are two types of smart cards: contact and contactless. The main difference is the method in which the data is transfer from the card to the reader. In the contact card, the contact on the card must physically touch the matching contacts in a card slot on the reader. In the contactless card, the card only needs to be in the “proximity” of the reader as the transmission of the data is through radio frequency.

The contact smart card is largely used for logical access; for network and system login applications. The contact technology provides a cost effective method to transfer significant amounts of data between a card and the reader and to perform complex cryptographic operations for authentication.

The contactless smart card technology supports faster access with higher throughput rates which is important in handling high volumes of people for physical access or mass transit (fare collection).

The advantages of smart cards over 125 KHz proximity cards are:

- a) Provides higher level of security by using encryption to protect the physical access credentials
- b) Supports multiple applications on a single card such as parking, vendor, fare collection, etc.
- c) Has the ability to write information to the card in real-time
- d) Has larger memory storage capacity to store biometric templates

ISO Standards

ISO (International Standards Organization) is a network of the national standards institutes of 148 countries that acts as a bridging organization in which a consensus can be reached on solutions that meet both the requirements of business and the broader needs of society, such as the needs of stakeholder groups like consumers and users. The widespread adoption of International Standards means that suppliers can base the development of their products and services on specifications that have wide acceptance in their sectors. This, in turn, means that businesses using International Standards are increasingly free to compete on many more markets around the world.

The ISO 14443 Type A (ISO 14443A) contactless card was originally intended to be a memory card only. However, microprocessor and cryptographic cards have been developed for Type A. The most common Type A cards are referred to as MIFARE cards.

ISO 14443 Type B (ISO 14443B) contactless card was originally intended to be a microprocessor version of Type A. Again, the memory and cryptographic options have been added for Type B thereby creating competition between Type A and Type B cards. The Type B cards are not as commonly deployed as Type A cards.

ISO 15693 vicinity card technology was developed in response to the industry's need for a greater operational distance than ISO 14443 cards with a minimum read range of 10 cm. The data rate, however, is somewhat slower.

MIFARE® Overview

MIFARE is a contactless smart card technology owned by Philips. The MIFARE technology is based on ISO 14443A operating at the 13.56 MHz frequency. MIFARE is a proven, reliable, and robust technology for contactless smart card with 250 million cards in the field. It is an open architecture platform that guarantees compatibility with current and future products. MIFARE has an established customer base with the broadest offering of suppliers providing multiple sources for cards and readers.

HID *iCLASS*® and LEGIC are examples of other contactless smart card technology that are based on a proprietary architecture. The chip and antenna module for both the cards and readers can only be purchased through a single source (in the case of *iCLASS* from HID and for LEGIC from LEGIC).

MIFARE Technical Specification

The MIFARE standard card is a 1K byte (8192 bits) with 16 sectors. The memory map of the sector is as follows: each sector has 64 bytes (512 bits); within each sector, there are 4 blocks. A block has 16 byte (128 bit) of memory.

Sector 0 is reserved for the MIFARE Application Directory commonly refers to as MAD. The MAD defines the common data structures for card application directory entries; allowing terminal to identify the right card and the right memory within the card without the need to perform a comprehensive search through all of the card's sectors until the appropriate application is found. The MAD uses Application Identifiers (AID) pointing to the specific sector in which the data is stored and identifies the registered card application for that sector. For multiple applications on a single MIFARE card, there can be multiple AIDs programmed in Sector 0x0 and 0x1 to identify all registered card applications. The AID is a unique 16-bit number that is assigned by Philips to the participating registered

companies. Software House has a registered AID of 5120 (51 for access control application).

Each MIFARE cards contains an integrated chip with a unique permanent identification (UID) burned-in during the manufacturing process. The UID is often referred to as the Card Serial Number (CSN); for MIFARE, it is a 32-bit randomly generated serial number. The card serial number is not encrypted and resides in Sector 0, Block 0 and cannot be overwritten.

In each sector including the MAD, there is a set of 48-bit encryption keys: Key A (read) and Key B (write). The keys are used to protect the programmed data from being read or overwritten without authorization. Since each sector has its own pair of keys, the card can be used to store information from multiple vendors for separate applications and protecting their specific sector(s) with their respective keys.

Security

The MIFARE technology uses the three pass mutual authentication according to ISO 9798-2 to ensure the security of the card and reader data exchange. The three pass mutual authentication is used to authenticate the card and the data stored on the card. The three pass sequence encrypts the communication and the transfer of card data between the card and the reader.

Software House Multi-Technology Reader

The Software House Multi-Technology Reader has the ability to read the MIFARE CSN in the default mode or configured via program cards to read the encrypted sector data.

For encrypted sector data, the Flex version of the reader can be configured to use the AID in order to locate the sector in which the data is stored or configured to always look for a specific sector.

The Flex version of the Software House reader will also have the capability of loading and resetting the MIFARE read keys via program cards. The ability to customize the keys is critical in protecting unauthorized access to the card data.

For more information on the Software House Multi-Technology Reader or the MIFARE technology, please visit our website at www.swhouse.com.

About Software House

Software House is part of the Tyco Fire & Security Access Control and Video Systems business unit.

Software House designs, markets and supports integrated security management systems, including its flagship products C-CURE 800/8000 and the iSTAR™ controller.

From entry-level single-door access control systems to state-of-the-art integrated security management systems operating on enterprise-wide networks, Software House can provide you with a complete range of field-proven and innovative products.

For more information on Software House products,
1-800-550-6660 www.swhouse.com

SOFTWARE HOUSE