IDENTIFICATION TECHNOLOGY

1.0 INTRODUCTION

The need for personnel identification is a common requirement in modern societies. For example, many countries require their citizens to carry Identification cards which indicate their status. Banks issue bank cards that identify uniquely each account holder. Clubs issue cards to identify each valid club member.

Growing popularity of automatic machines for providing various facilities or services to authorized people requires that personnel identification be performed reliably without the interaction of a human operator.

A good example is the cash withdrawal procedures in a bank. The automation of this facility is made possible by 3 technologies. Firstly, the identification of an account number and confirmation of authorized account holder using magnetic cards and PIN code. Secondly, the checking and updating of his account balance by computer via data communication network. Thirdly, an electro-mechanical device that can count and issue notes (cash dispenser).

Note the 3 essential elements that bring about automation:- Identification, Processing, Activation.

A second example is the automation of door entry using a card access system. This operation requires 3 technologies to be made available. Firstly, the identification of the person. Secondly, the processing of the identity of the person against a set of access criteria. Thirdly, the automatic activation of the door unlocking mechanism. Note that the 3 essential elements that bring about automation are similar to the aforementioned example, that is, Identification, Processing and Activation.

We can quote many other examples of this nature, and in each case, personnel identification is the first step towards automation. ELID's business is automatic identification of people and objects by Electronic means, hence, the name **EL**(ectronic)-**ID**(entification). In this section, various techniques for identification will be discussed. In particular, the ID token carried by each person, and the readers used to read such tokens.

1.1 OPTICAL METHOD OF IDENTIFICATION

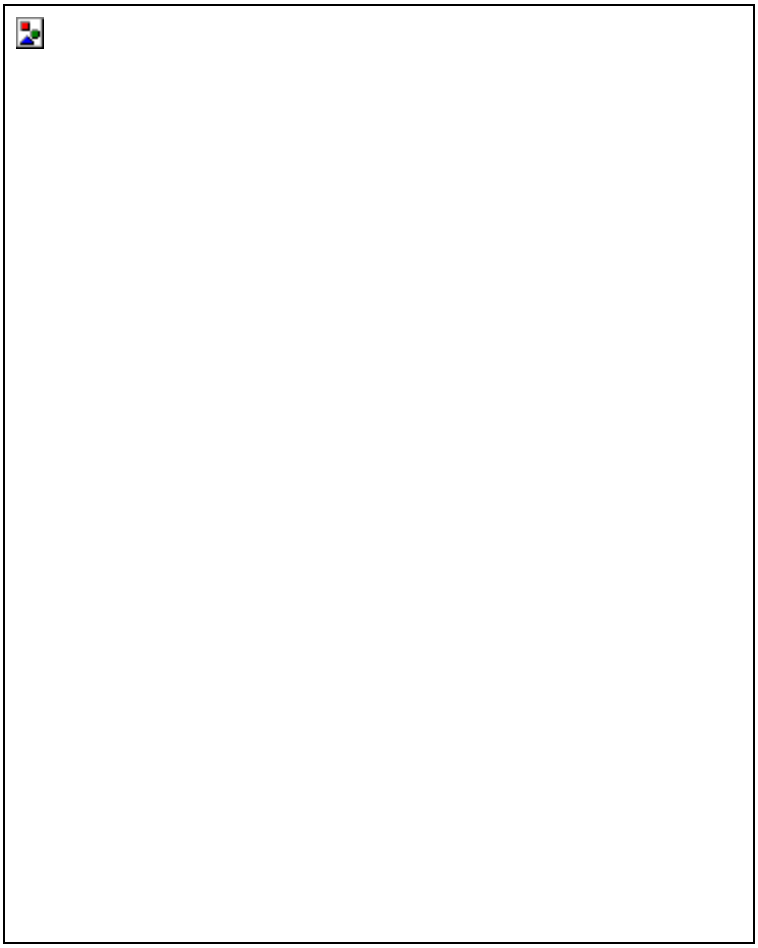
In this method, the code is stored as optical patterns. The most common optical code used is the bar code. The codes are well known to all of us. Bar codes consist of a combination of wide bars/thin bars and wide space/thin space.

A simple bar-code reader consists of a light source, usually in the infra-red spectrum, which is made to sweep across the bar code label and the reflected light is sensed by a semi-conductor device that is sensitive to light intensity. Obviously, the dark areas will reflect less light than the white area. Thus, a series of electrical signals are generated in the reader that corresponds with the bar code pattern. This signal can be passed to a processing circuit to interpret the code read.

Bar code has gained widespread usage over the years. Its main advantage is the ease of producing code labels. Almost anyone with access to a PC and a good quality printer can produce bar code labels themselves - at negligible costs. Bar-code readers of various types are also readily available at a relatively low price. Hence, it is cheap to implement a bar code system. However, Bar Code Systems are only for identification, with hardly any security feature. Therefore, it should not be used where security against unauthorized duplication is a prime consideration.

Some manufacturers use proprietary coding techniques and proprietary readers to enhance security. But in so doing, they forfeit the main benefit of the system - low price, and easy implementation. In any case, an optical system that can be visually deciphered will have limited security.

Reading reliability is lower for optical cards compared to other techniques mainly because such cards are affected by dirt marks and, reader heads too are affected by dust deposits.



1.2 MAGNETIC METHOD OF IDENTIFICATION

In this method, the code is stored on a magnetic stripe. The magnetic stripe is similar to the magnetic tape commonly used for music recording, except that it is pasted onto a hard plastic card. The popularity of the ATM cards and credit cards have made such magnetic cards a common sight. There are literally hundreds of millions of such cards used all over the world, making it by far the most popular identification technique.

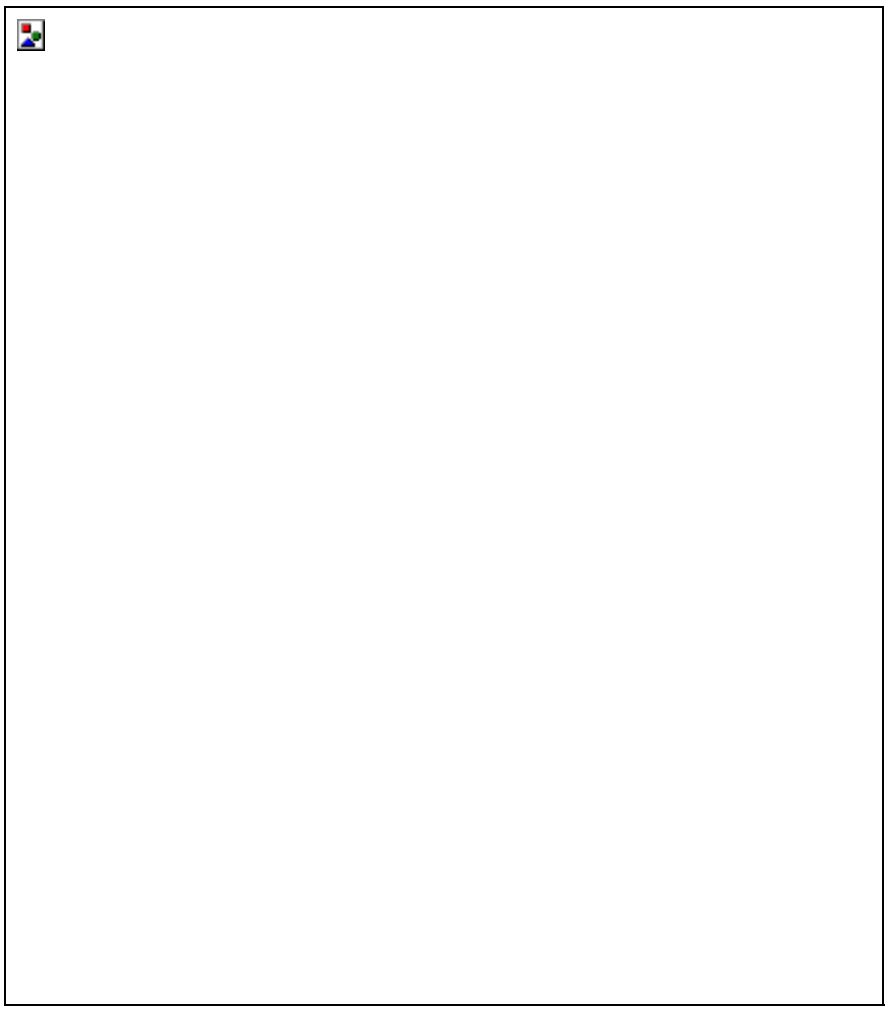
Encoding of signal on such cards is similar to recording of music on cassette tapes. The signals are recorded as a series of tiny magnets whose polarity is oriented in different directions according to the signal. The most popular method of recording is the so-called F2F method. In this method, a digit or character is represented as a binary number. The binary "0" is recorded at a frequency F and the binary "1" is recorded at a frequency 2F. Hence, such a recording consists of a combination of waveforms of frequencies F and 2F.

A standard card conforming to ISO 3554 standard will have a magnetic stripe of width about 54 mm, which can carry 3 tracks of information, commonly referred to as track 1, track 2, and track 3. The density of the recording and the format of the recording is controlled by an ISO standard. For example, take track 2, it will have a recording density of 75 bits of information per inch. This is equivalent to about 40 digits of data for the entire card.

Note that during reading of a magnetically encoded card, the card must be moved across a magnetic reading head at a relatively constant speed. If the card is passed over the head too fast or too slow or jerkily, the reading will be distorted.

The magnetic cards enjoy a number of benefits. Firstly, its wide usage, because of adoption by credit card companies and banks makes its price very affordable. Typically, around USD1/- at retail price. Secondly, the code stored in the magnetic medium can be easily erased and re-recorded as many times as one wishes with hardly any deterioration. Thirdly, its code is not visible to the naked eye, and duplication requires a relatively sophisticated equipment out of reach of ordinary people. For increased security, most manufacturers, including ELID, adopt proprietary codes that cannot be read or copied by commercial card encoders.

However, magnetic cards are subject to wear and tear, and have a definite life span of usage - much like cassette tapes. Each time the card is passed through the read head, it is rubbed against the reader head, and wear and tear results. Magnetic cards are also subject to demagnetization when used in the presence of high magnetic fields. This latter disadvantage can be overcome by using high coercivity materials. That is, magnetic materials that are "hard" or of "high energy". For example, ELID EC2H high-coercivity cards are rated at 2750 to 4000 Oersteds, and seldom demagnetized.



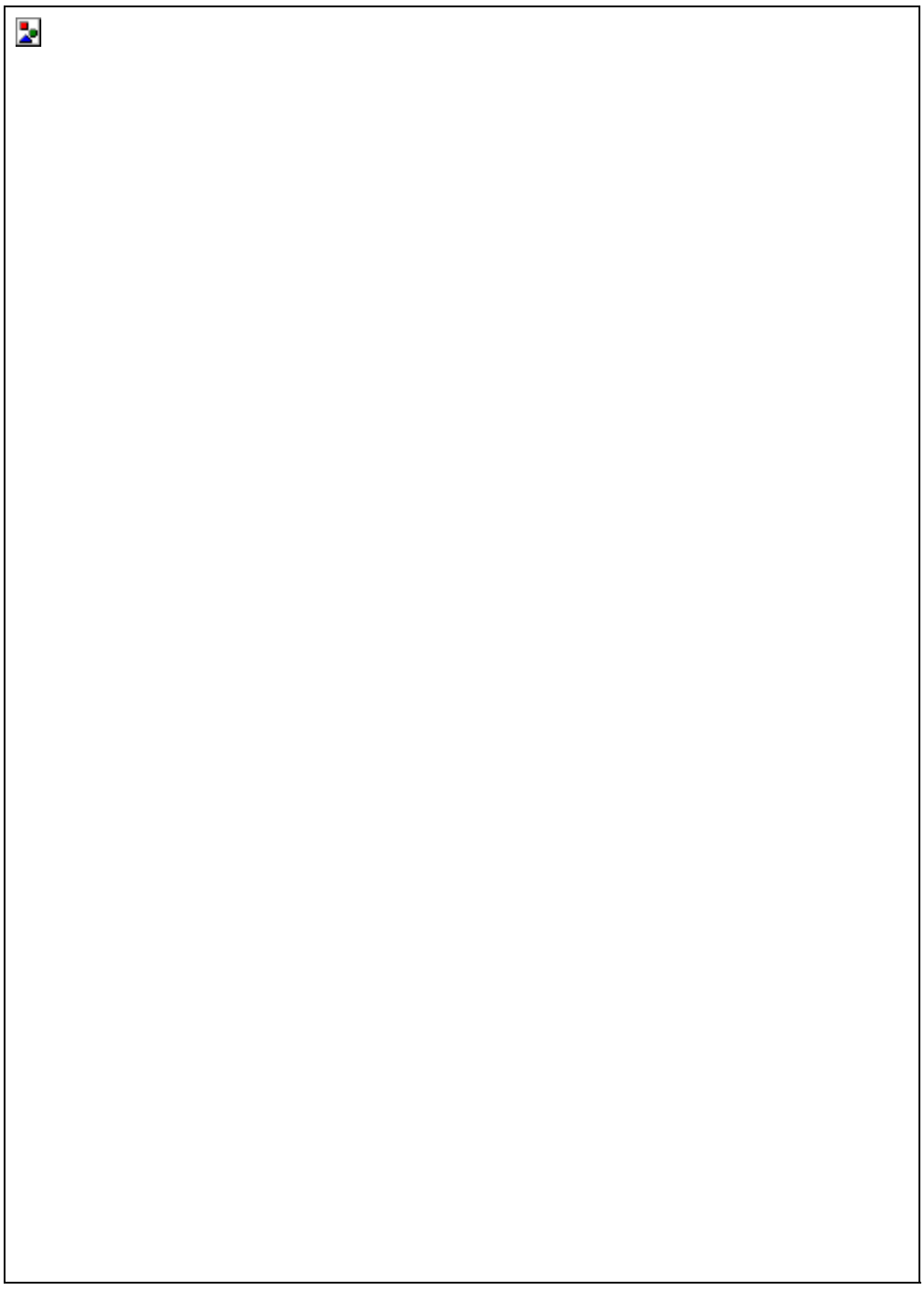
1.3 WIEGAND METHOD OF IDENTIFICATION

Certain alloy wires, when strained and twisted in magnetic fields, produce a core of soft magnet surrounded by a thin layer of hard magnet. When such a wire is subject to a magnetic field opposite to its remnant magnetism, the soft magnetic core and the hard magnetic shell will be of reverse polarity, and the resultant field is very small. As the external field is increased, a threshold is reached when the outer core suddenly snaps into alignment with the prevailing field. This sudden 'snapping' action produces a large field expansion that can be picked up if a coil is placed nearby. The pulse width is in the micro-second range and is independent of the rate of increase of the applied field.

In a typical Wiegand ID card, Wiegand wires, are laid along 2 rows, one above the other, embedded inside the card. One row will represent the presence of a binary "1" and the other row will represent the presence of a binary "0". The reader unit consists of small magnets and sensing coils that can pick up the presence of such wires because of the snapping effects they produce.

The main advantage of Wiegand cards is their very high reliability. The wires are not subject to demagnetization, or deterioration. There is no rubbing action during reading, so there is no wear and tear. Reading is accurate whether the card is passed slowly or rapidly over the reader head. Hence properly used, Wiegand cards could last indefinitely.

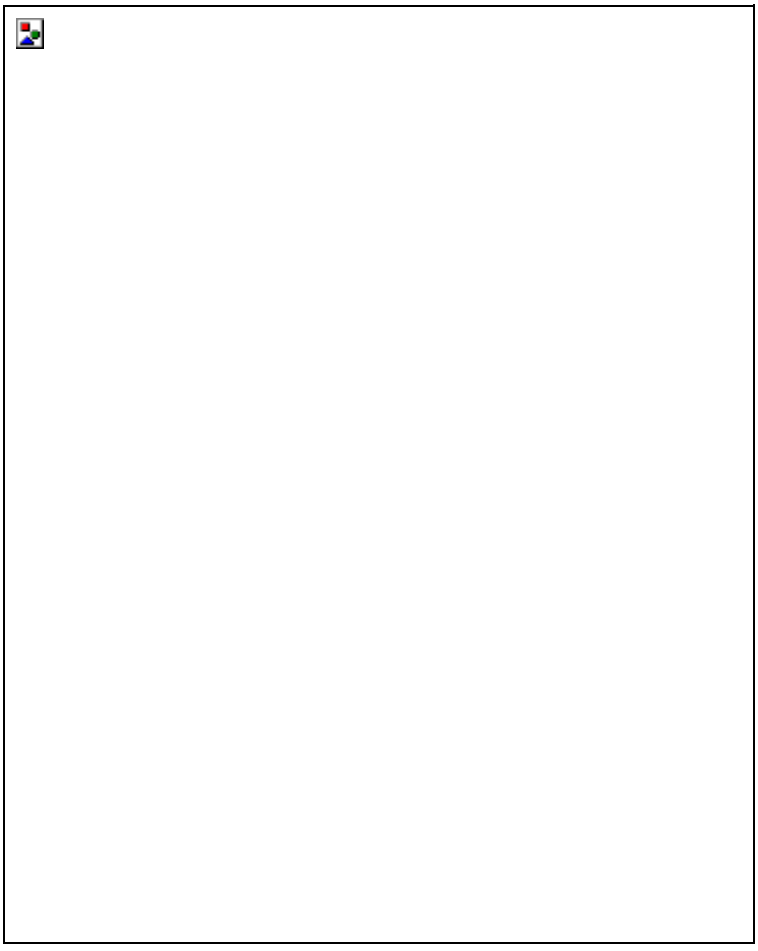
The main disadvantage is that the card cannot be user programmed. The code is physically built up during manufacturing by burying the correct combination of wires. Once it is made, the code cannot be altered. Another limitation is that the number of bits that can be encoded in a card is limited to about 42, a capacity hardly 1/5 that of a magnetic card.



1.4 PROXIMITY METHOD OF IDENTIFICATION

Proximity cards, as the name implies, work when they are brought NEAR to the reader, without any contact, or swiping. A wide range of such devices is now available from various manufacturers.
The proximity reader consists of 2 parts. The first, is an induction coil, called the antenna, which produces a strong magnetic field, the purpose being to send energy to the proximity card when it comes within range. The second, is a receiver circuit that can detect a signal sent by a proximity card that has comes into range.

The proximity card similarly consists of 2 parts. The first is a coil that receives energy from the reader antenna, this energy is then used to power the electronics embedded in the card. The second is a transmitter that transmits the ID code of the card for reception by the proximity reader.
Proximity Readers are available with different reading range from 3 inches to 3 ft. The size of the antenna increases with increasing range.
Some manufacturers produce active cards, powered by built-in battery. Such cards can have a much longer operational range, but suffer the inherent problem of limited battery life span.
Proximity ID systems have the advantage of ease of operation, as ID cards need only be presented, without any swiping action. They are particularly suitable for areas of high vandalism because the readers can be installed behind non-conducting materials such as bricks or glass, without impeding the reading function.
A major problem faced by Proximity systems used to be their pricing, especially that of the card. This is no longer so, and proximity devices are now very competitively priced and in wide demand today.



1.5 IC METHOD OF IDENTIFICATION

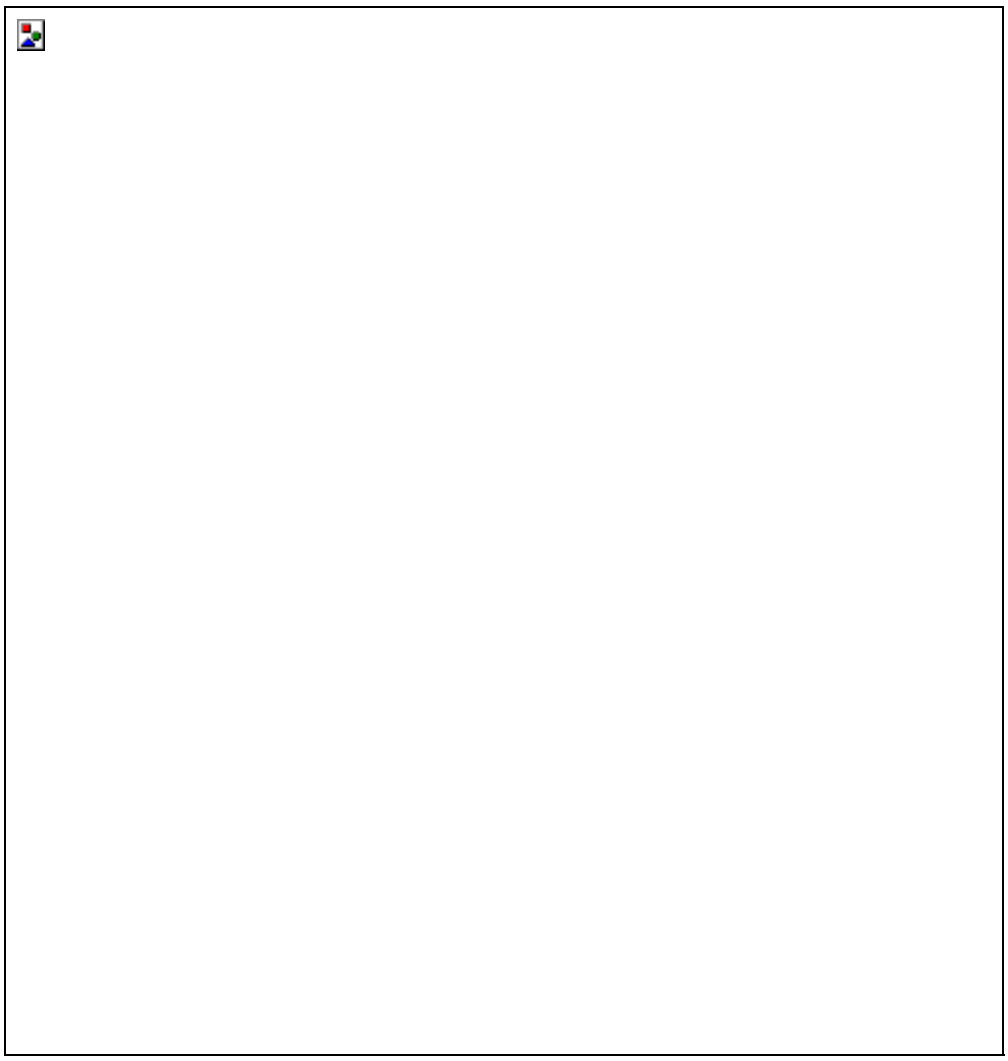
IC Cards are more commonly known as "Smart Cards". These are cards in which are embedded Integrated Circuits (IC). The IC circuits are directly accessible via gold plated contacts embedded on the surface of the plastic card. The IC Card readers are equipped with sharp metal pins which are pressed against the card gold contacts for electrical connection when the card is inserted into the reader unit.

There are 2 categories of IC cards in common use.
The first category is the memory cards. They contain memory IC's which may be one-time programmable (EPROM Cards), or continuously re-programmable (EEPROM cards). For example, the IC card EC896 has 896 bits of EEPROM segmented into 3 memory areas, and protected by 3 access codes and a fuse. The secret codes can be selected by the user before the fuse is burnt. Once the fuse is burnt, the codes cannot be altered. 3 continuous failed attempts in presenting the correct secret codes will permanently "kill" the card. The memory in EC896 can be erased and written 10,000 times. Data stored in the memory cell will be retained for more than 10 years.

The second category of IC Cards is the CPU cards. These are cards embedded with IC chips that are built from a Micro-Controller. The built-in CPU can be custom programmed to handle a wide range of functions such as data processing, security checking, encryption and de-encryption.

For example, the ECM3K has an 8-bit MCU core, 6KB of application ROM space and 3KB of EEPROM for data storage. This device is designed specifically for Smart Card application and has security features manufactured into the chip to prevent fraud. The memory contents can only be read and modified by instructions preprogrammed into the application software in the ROM; the validity of the EEPROM data is, therefore, strictly controlled. Fusible links are provided which permanently disable access to the non-User modes. There are security functions to detect any unauthorized erasure of the EEPROM; and EEPROM security bytes which can be programmed with customer determined codes.

The main advantage of IC cards is their high security. It is virtually impossible to duplicate or break into such cards. This, therefore, makes it particularly useful for applications where integrity and security are of vital importance. For example, the card can be used as a high performance stored value card where the account balance is continuously updated and transactions are recorded inside the card memory itself. Such cards can be used in charge terminals that need not require interrogation to a central computer.
The second advantage of IC cards is its flexibility. The in-built intelligence of Smart Cards allows a wide range of applications to be performed giving flexibility for modifications and upgrading as the need arises.

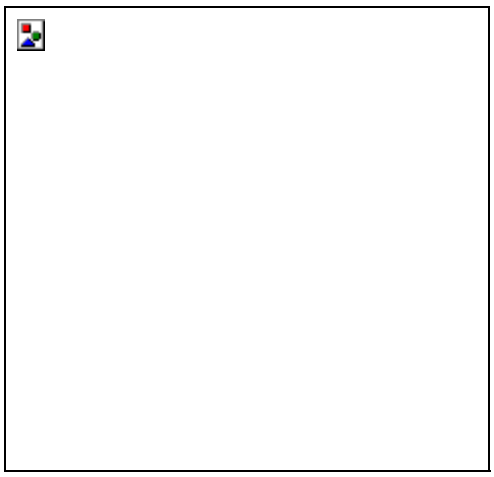


1.6 Contactless Smart Cards

A major weakness that affects the reliable operation of smart cards arise from the fact that there are physical contacts between the reader and the card. The physical contacts cause wear and tear, and sometimes give unreliable reading due to dust and dirt. Furthermore, such contacts, particularly at the reader, are frequent targets of vandalism.
To overcome the above, a new type of cards, which do not require contacts (hence the name contactless) has become popular in recent years. They work on the same principle as proximity cards, that is, using the principle of radio frequency identification. However, unlike normal proximity cards which can only be read, contactless smart cards can both be read and written into. The most popular contactless smart card is the "Myfare" cards made by Mikron. Millions of such cards are used in many parts of the world, particularly in transportation (such as the Hong Kong subway).

1.7 Touch Memory

Touch Memory, popularized by Dallas Semiconductors, is another type of ID device that has found its own band of devout followers. Each device looks like a mercury button battery (like those used in calculators), with a stainless steel housing. The top and bottom half of the housing is insulated, and form the contacts to the IC chip embedded in the capsule. Many types of chips are available, the most common type contains EEPROM cells allowing storage of information.



2. TOKEN CONSTRUCTION

The standard Credit Card is by far the most popular size, and is adopted by most manufacturers irrespective of the type of technology they use, whether optical, Wiegand or proximity.
The advantage of adopting this size is that the card will fit most wallets and card carriers. The standard credit card size allows sufficient space for visible ID to be included. This could be just a unique logo of the company, but could also include the card holder's name, job designation etc embossed or hot-stamped. There is space even for a small photograph of the card holder.
Wiegand tokens are also available in the shape of a key. The advantage is that it can be put together with ordinary mechanical keys in a key ring.
Proximity tokens are also available in the shape of a key holder. There are versions available for mounting permanently to a car.

3. READER CONSTRUCTION

Readers that can be used with credit-card sized cards can be divided into the following basic types:-

a. SWIPE type
   This type of reader has a slot running down either the middle, top or bottom side of the reader. A card is read by swiping it smoothly down the slot. This is by far the most popular type as swiping action is easy, fast and accurate. Swipe readers are able to read 100% of the available recording surface on the card. Swipe readers are normally surface mounted.
b. INSERT type
   This type of reader is equipped with a slit that allows a credit card to be inserted at the narrow end. Reading is usually made when the card is pulled out, though some readers accept data when the card is inserted. Insert Readers are normally flush mounted. It occupies less space but is more difficult to install. Insert Readers may or may not be able to read 100% of the recording surface depending on its construction.
c. ALL WEATHER type
   It may be necessary to mount a reader in open space. In this case, it is necessary to choose readers that can withstand sun and rain. Wiegand readers are inherently weatherproof. For other readers, special design is required, often by mounting the reader upside down.
d. Keypad.
   Often, readers are equipped with keypad. The keypad is provided for card holders to key in their PIN code - just like that in the ATM.

4. ELID READERS

You will find a list of ELID Readers and Tokens in the ELID product catalog.