E I M S™ - Smart Cards

Contact Less Smart Card

A smart card is a piece of plastic, the same size as a credit or debit card, with a silicon chip embedded in it that stores and transacts data between users. **Contact less smart card** contains an embedded antenna attached to the chip for reading and writing information contained in the chip's memory. The card is "smart" because it is "active", that is it can receive information, process it and then "make a decision". For example, when a smart card is shown to a terminal, the terminal sends its "digital signature" to the chip. If the "digital signature" agrees with the existing parameters in the chip's memory, then the memory files are opened and the data is made visible to the terminal. In the same way, the card sends its "digital signature" to the terminal and the terminal verifies it. This mutual verification is done "off-line": this means that the computer need not to keep 'on' while terminal is operating. The verification process typically takes a fraction of a second.

To access any of the below mentioned applications employee(s)/student(s) has to show his card to the contact less reader with a distance of 80mm for secure authentication & authorization. Whenever any user punches (shows) card to the reader, primarily data is stored in the 128 KB of memory embedded into the reader. 10,000 to 12,000 punches of these data can be stored in the reader itself. Later this data is to be transferred from the reader to any computer attached via data collect software developed by **Redox Technologies** specifically compatible with its readers.

The data collected by the reader using the "data collect" is transferred to the computer system connected through the appropriate communication interface **(RS 232/422/485)**.

What can smart cards are used to do?

Smart card-enhanced systems are in use today throughout several key applications, including ***healthcare, banking, entertainment and transportation***. To various degrees, all applications can benefit from the added features and security that smart cards provide.

- **Smart Identity Card**

Smart cards can store benefits, pension payments and health insurance refunds in an e-purse and securely identifies cardholders when claiming benefits.

- **Medical History**

Smart cards can store medical treatment records, emergency information and health insurance status.

- **Electronic Purse**

Electronic payment cards allow cardholders to avoid the hassle of finding correct change by loading value into an electronic purse (“e-purse”), which can to pay for small-value everyday purchases at shops, vending machines, transport ticket machines, parking meters, public payphones etc.

- **Campus Club Card**

Smart cards are very popular with closed user groups (residents of a city, students and staff of a university, staff of a company, etc.), who can use multi-application cards to pay for or access everyday services e.g. **cafeteria meals, drinks machines, library tickets, leisure center, stadium, amusement park entry, car parking, amusement park rides etc**, differentiated according to individual circumstances and status.

- **Time And Attendance**

To access the above stated application, Student(s) / Employee(s) always has to show his card to the contact less reader to mark his attendance. The data of all the employees / Students who have shown there smart cards to the reader will be stored in the readers, which is then transferred to the computer attached for further processing and reporting. The reader records the date of punching of student(s) / employee(s), in and out time(s), overtime. The software also has the option for machine raw punching (in case the employee forgets to bring his card) and generate all kind of reports MIS reports.

- **Access Control**

Access permission means restricting the entry of unauthorized person(s) or employee(s)/student(s) to a particular section of the organization. While implementing the access permission, we require to install an electromagnetic lock on the door(s) of the restricted area. The reader is connected to the electromagnetic lock, every time a person entering the area is supposed to show his card to the reader. If the person is permitted inside, the door will open automatically otherwise not and within milliseconds the information of the unauthorized person is flashed on any node/terminal attached therewith. People can be authorized and restricted for access permissions according to time and requirement. We call it ‘Masking’ which can be done for any number of employee(s) /student(s)/authorized person.

- **Utilities Of Access Permissions**

Restricting the prohibited area from visitors

If a magnetic lock is placed at the door of the restricted area. A person with a visitor pass is never permitted inside that area until unless escorted by an authorized person using a masked card.

Once a person enters the area, for exit we can have optional methods:

(a) **Push Button** of coming out if in case you are not interested to monitor the out the person who has entered the area.

(b) Another **reader** coupled to the same lock, which will monitor the outgoing of the person who has entered the restricted area. This will enhance the security system and provides complete information when a person entered and left.

Monitoring employees department wise

Using the access permission we can monitor incoming and outgoing records of any employee / student. Every time an employee enters or leaves, he will have to present the card to the reader in order to operate the gate and those records are maintained simultaneously. This can help the company's administration to increase the working potential of the backbone departments like "R&D", labs etc. a person can authorize to enter only his / her own department.

- **Other applications** (**E I M S™** modules with which the Smart cards are compatible)

✓ **Library management**
✓ **Fees Payment**
✓ **Canteen management**
✓ **Visitor management**