

# **SmaX Adv**

**(Using TCP/IP and or RS485 to RS232)**

**Version 5.1.0**



Hardware.. Firmware.. Software - Integrated Solutions

**TYPE II, UNIT NO: 9, DR. V.S.I ESTATE,**

**THIRUVANMAYUR, CHENNAI 600 041.**

**PHONE: +91 (44) 22542517/1392.**

**TELEFAX: + 91 (44) 22541803.**

**MAIL: [email@electronindia.com](mailto:email@electronindia.com)**

**URL: [www.electronindia.com](http://www.electronindia.com)**

## Contents

Introduction .....	- 3 -
System Overview .....	- 3 -
System Architecture Diagram .....	- 5 -
Application Software Overview .....	- 6 -
Technical Features .....	- 15 -
Software Requirements.....	- 16 -
Central Server .....	- 16 -
Software .....	- 16 -
Hardware .....	- 16 -
Client .....	- 17 -
Software .....	- 17 -
Hardware .....	- 17 -
Abbreviations Used .....	- 17 -

## 1 Introduction

Electron India presents SMAX Adv 5.1.0 using client server architecture and Microsoft SQL Server7.0 & above or Oracle 8i & above as database.

## 2 System Overview

The supervisory level is managed by **SmaX Adv 5.1.0**, which provides the man machine interface (MMI) in order to provide personal movement tracking, system configuration, status & alarm emission and management, historical event management, access rights etc.,

At the peripheral level, the access control system consists of smart card readers. These smart card readers will be the interface to the 'external world' such as employees, students, visitors, doors, turnstiles, fire alarms etc.,

The application software will be used for central monitoring and full operation of personal movement tracking and Access Control System.

## 3 Design Feature

- The Access control system is capable of integrating multiple functions including access control, finger print(biometric) reading, smart card reading, combination reading i.e. smart card + finger-Print, alarm management and ID Badging with operation of turnstile, flap barriers, boom barriers and/or other types of access control devices to be used in future.
- The system is modular in nature and permits expansion both capacity and functionality through the addition of card readers and sensors.
- The system incorporates necessary hardware, software and firmwares to collect, transmit and process alarm, tamper and trouble conditions, access requests and advisories in accordance with the security procedures of the facility.
- The user interface at the computers (Servers/Clients) is GUI based.
- The access control system will permit access to the secured area separately by smart card reader or finger print reader or a combination of both.
- The integration of the smart card reader and the finger print reader, wherever required, will allow the smart cards and the finger impressions to be read near simultaneously in a fast and single presentation.
- All the smart card readers and or finger print readers will be connected to the LAN/WAN/MAN via TCP/IP Converters.
- The employee's data available in various readers will be transacted whether online in real time mode or offline mode to the local server.
- To avoid duplication of employee database, the entire cardholder Database of all locations will be maintained in a single server. The Employee details pertaining to a single location or a cluster of Locations will be downloaded in that particular location.

- Every location will have its own local server, which will be maintaining the data pertaining to that location only (Such as Cardholder detail for that location pre downloaded from central server, Access Levels, Reader Details etc...). The client versions will be responsible only for activities like Visitor/VIP pass issuance, generation of MIS reports, Card Personalization, Card Printing and monitoring. The communication with the Access control readers will be done only by the Server Version of SmaX Adv software.
- For maintaining a centralized MIS reporting system and cardholder Database, a Central Server will be maintained at any one of the locations. The Server Editions of SmaX Adv software which is installed in all locations will be communicating with the said central server for uploading all the transaction details. And it will download the required cardholder database.

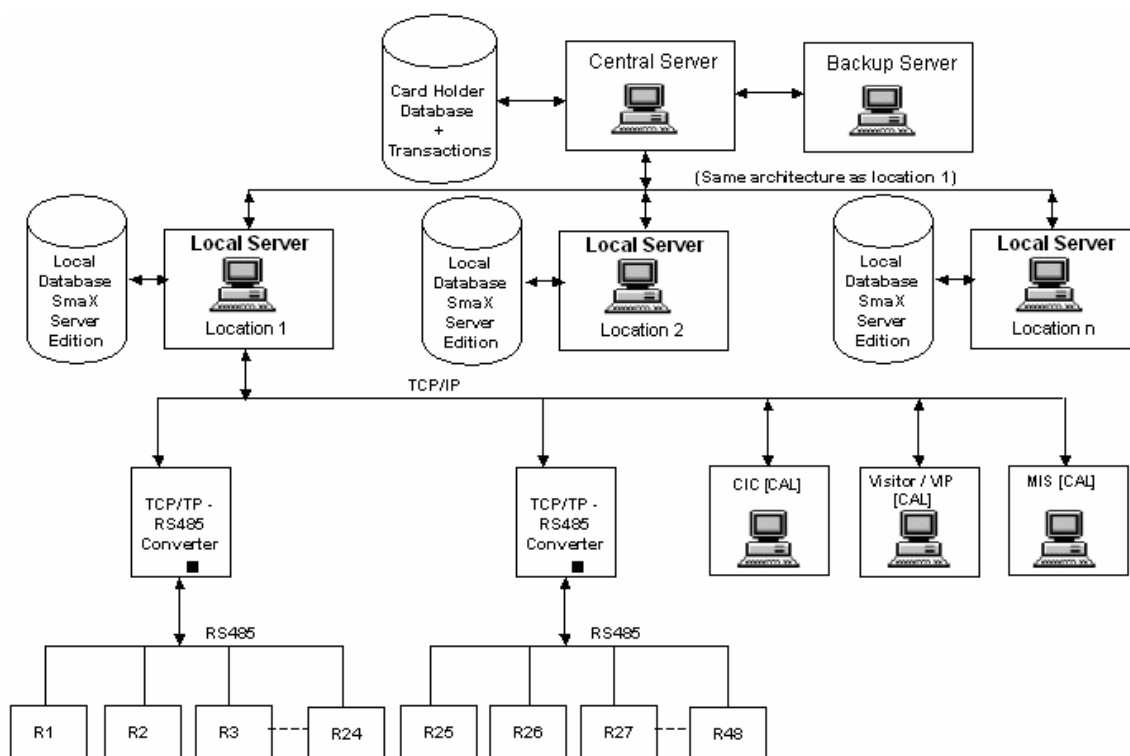
*(Note: There may be difference in the data of central server and the local server due to a communication mismatch.)*

- The movement of employees may be any of the following types
  - i. Employee on a temporary visit to a different location
  - ii. Employee on a permanent transfer to a different location

In every location whether he is an employee or visitor the person has to report to the concerned authority. In case the employee is visiting, other location on a temporary basis, he will be treated as a visitor and the concerned authority will grant/deny access for that location, through the VISITOR/VIP module. On flashing the card of the employee the system will pick up the card number.

## 4 System Architecture Diagram

### SMAx ADV Architecture



#### **Note:**

- R1, R2, R3 are the Access control readers in location 1. They are connected to the TCP/IP network via TCP/IP - RS485 converter.
- At all locations the Reader connectivity architecture will remain the same as location 1.
- The Maximum number of readers that can be connected with a Single Server Edition of SmaX Adv is 255. If it exceeds than further Server Editions to be used.
- All the Local Servers are connected to the central server through LAN/WAN/MAN cable.
- Maximum 24 readers can be connected to a TCP/IP - RS485 Converter box
- Static IP should be provided for all the Local Servers where the polling is taking place and also for the TCP/IP – RS485 converter box. Both IP should be of the same class.

## Application Software Overview

SmaX Adv is a complete Access Control Solution for any organization, employing the latest Contact less Smart Card technology for Access. SmaX Adv supports various models of Contact less Smart Card Readers in the front-end. These Readers can be networked on TCP/IP and terminated at a LOCAL SERVER via TCP/IP - RS485 converter. The readers range from simple low-end cost-effective readers to high-end complex readers. The low-end readers do not have an LCD display and keypad while the high-end readers support both and also have additional input lines and relays. There are also finger scan-based Contact less Smart Card Access Readers.

The software allows definition of multiple Time Zones and Access Levels for restricted access to Cardholders.

These definitions are transmitted to the Readers through RS485 via the TCP/IP converter. Using these definitions, the readers independently authenticate cards for restricted access even while the local server is turned off.

All the transactions (card flash) that happen at the readers are downloaded to the LOCAL SERVER automatically if SmaX Adv is running on the LOCAL SERVER. If SmaX Adv is turned off, the transactions are stored on the readers themselves and downloaded to the LOCAL SERVER when the software is up and running again.

The high-end readers come equipped with additional relays for external equipment control. They also have additional Input lines for feeding in external signals.

### Smart Card Making & Issuing System

The smart card as "Identity Card" will be the basis of entering in the work premises. The system will be such that only authorized persons should be allowed to enter.

The Smart Card Making & Issuing System i.e. Card Issuance Center (CIC) will be under the supervision of Security Section, this would ensure proper security control on making and issuing the smart cards.

The CIC system consist of a LOCAL SERVER/Workstation, Digital Camera, Scanner, personalization reader (for finger print enrollment and card programming), signature pad, Card Sticker & Thermal printer along with CIC software. Smart Card related database will be available in the Local server over the network.

### SMA X Adv Application software

The Application software will be used for central monitoring and full operation of the Personnel Movement Tracking & Access Control System.

The application software is developed on Windows 2000 Advanced Server running on an Intel platform with MS SQL Server 2000 / Oracle 8i & above as the Database. The software is Graphical User Interface as far as possible; the application is user friendly. The software modules seamlessly interact with each other for data interchange.

The application software is divided into following functional modules.

#### Master Modules:

- *Key Management Module*
- *Smart Card Making & Issuance System module (CIC module)*
- *Access Control Software module*
- *Client Module*
- *Visitor Pass Module*

#### Reporting & Querying Modules:

- *MIS Module*
- *Personnel Movement Tracking Module*
- *Time and Attendance Module*

#### User Interface Module

- *Client Module*

#### User Interaction and the Transaction

- I. User shows the card to the reader.
- II. The reader reads the data from the card and validates with the data stored in the reader.
- III. If the person is authorized to gain access then the reader flashes the welcome message and allows going in.
- IV. Otherwise, his access is denied with a message stating the reason.
- V. The above-mentioned details is stored as a transaction with date and time stamp in the reader and then transmitted to the central server through the local server.
- VI. This transaction can be viewed from the local/central server at any point of time.

#### ACS software features & functionality

- The software will seamlessly support and integrate with the Key Management System for smart cards and will be capable of supporting 3-DES based smart cards (cryptographic). (This facility is available only on demand) the relevant ACS application software shall be installed at multiple operational sites.
- **Software features will include the following:**
  - ✓ Expandable cardholder database depending upon the reader
  - ✓ Access Levels, Time Zones, Time Intervals, Security Levels
  - ✓ Input alarm points.
  
  - ✓ Output points.
  - ✓ Fully distributed processing.
- **ACS will meet following additional specifications:-**
  - ✓ User Level Security: The Access Control System will basically have three-user level Security namely.
    - Administrator

- Supervisor
- User

The Administrator will be able to use all the privileges of the Access Control System i.e. the Administrator can add New User, Enter, and View and Modify the records. The Administrator will be the Super User and the privileges for the other users is granted and/or revoked by the Administrator.

The Supervisor can view and manually register the attendance. The details of the records that are entered manually are maintained so that the Administrator can keep track of the manual entries.

The User may be a receptionist of Security person who can view the records and he is not authorized to modify or update or delete the records.

- ✓ Database Management: The system will create and maintain a master database of all smart card holder records and all system activities for all connected points.
- ✓ Input Point Monitoring: The system will collect and process status information from all monitored points.
- ✓ Alarm Annunciation: The card reader will audibly and visually annunciate all alarm for card based authentication.
- ✓ Powerful user definable trigger events. Defining a set of logical functions with sophisticated "If-then-when" conditions including the use of flags.
- ✓ Input Points Supervision: The system shall electrically supervise all input point circuits.

### Reports:

Access Control System will provide following reports

- Transaction History Report with the ability to filter by any one of the following parameters:
  - Cardholder Name
  - Cardholder Card Number
  - Reader Number/Name
  - Start date and end date
  - Transaction Type
  - Department wise
  - Designation wise
  
  - Exit switch activation
  - Door forced open
  - Door open too long
  - Door open normalized
  - Inputs Active / Normal

#### Visitor Transaction report

- Company wise
- Visitor Card number wise
- Personal visit
- Reader wise
- Transaction Type

#### Visitor card status report

- Company wise
- Visitor Card number wise
- Personal visit
- Employee wise visit
- Card Issued
- Card Returned
- Card Cancelled

#### **On-Line help System:**

The system will provide on-line context-sensitive help, which will be available at any time and from any screen.

#### **Password:**

The operator password function will control which menu the individual operator will be allowed to access.

#### **Automated polling for readers and alarm generation:-**

The system will automatically poll the readers in real-time basis and in case of any failure of any reader (fingerprint/smart card reader), audio-visual alarm will be generated on the Local Server/System administration console and local server of that particular location.

#### **Alarm Input Point Suppression:**

- The system shall support alarm input point monitoring functions.

#### **Trigger event processing:**

Trigger events will consist of a logical statement, which defines actions, which are to be performed when certain source functions occur and specified conditions are satisfied. A trigger event shall consist of three parts: the source, the conditions and the actions. When the source changes and the conditions are met, the actions shall be performed.

- a. Source – A source will initiate a trigger event. A source will be a change of state of any of the following:
  - i. Valid/Invalid transactions [by all cards or individual card, access level or invalid card type at all or a selected card reader].
  - ii. Input point [alarm or normal]

- iii. Input point group [AND – all points alarm or normal, OR – any point alarm or normal]
- iv. Time Zone [active or inactive]

**Note:** Event triggers are reader dependent

- b. Actions – If the defined source changes state and all of prescribed conditions are met then the trigger event shall carry out any combination of the following actions.
  - i. Operate output relay [turn on, turn off or turn on for upto 60 minutes].
  - ii. Operate output group of relays [turn on, turn off or turn on for upto 60 minutes].
  - iii. Enable, Disable or shunt input point.
  - iv. Enable, Disable or shunt input point group.
  - v. Change flag [set, reset or set for upto 60 minutes].

#### TIME ZONES:

Time zones refer to the restricted work-timings suited to your organization when access can be given to people. Time zones are based on 'Days of the week'. When you create Time zones, keep in mind the different groups of people who follow the same set of timings and create such sets of time zones.

Under Days, the following options will be seen:

- **Everyday** – Monday to Sunday
- **Weekdays** – Monday to Friday
- **Weekends** – Saturdays and Sundays
- **Holidays** – all the dates that you created as holidays under the Holidays screen.
- If you wish to select a particular day instead of the above options, then these days are also available for selection.
- Alphanumeric name/description of the time zone.
- Upto 24 time slots, each defining the active days of the week [Monday to Sunday] with a start and stop time during which the interval shall be active.

#### Communications:

If reader loses communication with the Local Server, the reader will continue to control access, monitor input for all connected points and perform all trigger events. Local history of all transactions will be buffered at the reader and automatically uploaded to the Local server for alarm reporting and long-term historical storage once communication is re-established.

---

### ACS integration with other systems:

The system will provide support for integrated Video imaging and ID badging. Also, it shall support integration with CCTV system, Fire-alarm system, Public Addressing System.

*Note: The standard reader version (BT843 onwards) comes with two additional inputs (Input 3 & 4) which essentially mean that only two external systems can be integrated.*

### Event and Transaction History:

The ACS will maintain a record of all alarm, card transaction and system exceptions, which take place, and provide a means for a user to access this information. It will be possible to print information in the log in real-time or by a report.

### Anti-pass back control:

When any room has IN and OUT Readers, you can define that room as an area with the corresponding In and Out Readers as Entry and Exit. Using this, you can get to know the occupants of a particular area at any given time on a live basis. Antipassback (APB) option can also be given if required for the area. The Antipassback option if enabled will ensure that the card holders compulsorily use their cards to flash at IN and OUT readers of the area instead of trying to tail in or tail out with the person going ahead of them through the door. Note that this option when enabled applies to only those cardholders who have the Antipassback option enabled under them in the cardholders screen.

- a. The ACS will provide the capability to prevent more than one person from gaining access to a controlled area by recognizing when a cardholder who is granted access is passing back the card to another person to use the same card to gain access.
- b. An alarm will be generated if the cardholder violates the anti-pass back rules.
- c. It will be possible to define on a reader-by-reader basis, which readers are subject to anti-pass back rules. It shall also be possible to by-pass this capability, if required.
- d. System will have capability to designate any command key so that when it is used to enter an area it must be used to exit that area before it can be reused for entry.
- e. System will have capability to manually or automatically reset the location of all command keys pass back status at any time.

### Auto – forgiveness:

A supervisor will have a method of selectively disabling anti-pass back protection. During the time auto-forgive is active, the system shall ignore the anti-pass back protection and reset the keys that use the door within the secured access area to Unknown.

### Cardholder Definition:

The ACS software will provide the capability for the user to define cardholders with the following identification and operating parameters through a database stored in the central server:

- Cardholder Name
- Employee I.D
- Cardholder status – employee, visitor, contract labour. Touring employees.
- Cardholder phone number and extension number.
- Trace enabled or disabled.
- Assigned access card number
- Assigned access card issue level.

#### **Real-time transaction Monitor window:**

A real time transaction monitor window will be available for display on any ACS monitor screen. The real time window will be capable of listing the following transactions as they occur anywhere in the system.

- All transactions
- Valid/Invalid card transactions
- Alarm transactions

#### **Each of these categories will be set to display during selected time zones.**

1. **Client Module:** This module will serve as an interface between the user and Database. Using this module. The user will be in a position to interact with **SmaX Adv** software application. This module will be available to all the users of the **SmaX Adv** system. The functioning of the client module is as described below.
  - i. **SmaX Adv** user will have to double click on the SmaX Adv icon present on the desktop of his/her node.
  - ii. The Login Page of **SmaX Adv** will have User ID, Password
  - iii. After entering valid User ID and password, the client module will validate the User ID and Password. In case of incorrect entries in User ID or Password, the Client Module will flash appropriate Alert message.
  - iv. In case of valid User ID/Password, the client module will invoke the main menu. It is using this Main Menu that the user will be able to enter transactions into the system.

The Client Module has the following functionalities based on the user rights.

    1. Smart Card Personalization
    2. Visitor/VIP Pass issuance
    3. MIS Reports
    4. View Site monitor & Area members

## **REPORTS**

- Monitoring of configured Areas for live report of Area Members in the Site

- Monitoring of live entry of personnel through any or specific door along with their images.
- Live report of events that happen at the Readers as well as within the software
- Historical Audit trail with the following **filters** to retrieve events from any given date range. The events are those that happen at the Readers as well as within the software
  - a) All types of transactions
  - b) Only Operator Actions within the software
  - c) Only Access transactions
  - d) Void Cards
  - e) Tracked Cards. By marking certain Cardholders as 'Tracked' and viewing only their transaction
  - f) Anti-passback violations
  - g) Specific Cardholder
  - h) Specific Operator
  - i) Specific Reader

**Note:** Can be viewed in the server edition as well as client edition also.

## Visitor/ VIP module

The visitor's card will be pre-assigned with access rights for a particular location or a combination of locations. The access rights will be provided at the main gate and will be stored in the card. The card when flashed at the designated reader will provide entry or will decline entry.

The GUI will have provisions to store the details like name, purpose, whom to meet and where to go etc., accordingly, visitor's card will be provided with access levels. The unique number of the card will be tagged against the visitor details in the software.

**Note:**

1. The Security personnel will select the Access level he has to provide which in turn will write the reader (Node) I.D for that level on the visitor card. The card when flashed on the designated reader will read for its I.D. If the reader (Node ID) matches with any node ID written on the card, then it will grant Access. Otherwise it will decline access. This process is reader download independent

## Time and Attendance Module

The Attendance Module comes separately with SmaX Adv. It picks up the transactions from SmaX Adv and processes the same to give the Attendance Reports. All or some of the Card readers present in the site can be configured as IN and OUT readers to be taken into consideration for Attendance reporting purposes.

The software allows for configuration of Shifts and departments for Cardholders. It also allows Leave of absence reasons in the reports. The reports generated by this application are explained as follows:

- List of all Cardholders with Present / Absent status (Employee-wise, Shift-wise, Department-wise)
- List of all Present-only Cardholders (Employee-wise, Shift-wise, Department-wise)
- List of all Absent-only Cardholders (Employee-wise, Shift-wise, Department-wise)
- Specific Cardholder's report for a given date range
- Monthly report of all Cardholders

- First In Last out (FILO) Flash Reports

These reports are generated taking into account the Cardholder's first card flash in an IN reader and his last card flash in an OUT reader. This report gives the Present / absent status. The reports that come under this concept are same as under Single Card Flash concept.

- Net Hours Reports

This report is generated based on the employee's Consecutive IN and OUT transactions. It is the same as the FILO reports except that for calculating total working hours, it takes the consecutive IN and OUT transactions instead of First IN and Last OUT. This report will be useful when you wish to calculate the actual amount of time spent by a Cardholder in his work area. This report is only possible with IN & OUT Readers concept.

- Late Comers Reports

This report gives information on latecomers. With reference to the Start of each Cardholder's Shift Time, the report calculates how many minutes each Cardholder has come late. The reports under this are

- List of all Late comers on a given date
- List of all Late comers for a given Month
- Specific Cardholder's Report for a date range

- Access Reports

This report gives a listing of all the Card-flashes at the various attendance readers for specified Cardholders or department-wise and date range. Each card reader will have a unique IP Address-Node ID which will be responsible for communication and configuration. The smart card readers will be connected to the turnstiles/entry gates which will form a part of Access Control Mechanism. When the valid card is flashed on the reader, the reader will authenticate the cardholder and sends a signal to the turnstile wherever installed to allow access to the cardholder. This can be additionally done along with fingerprint authentication (wherever provided). In case of fingerprint reader, the cardholder shall place his finger on the fingerprint sensor at the time of display of his card for his complete authentication. One to one fingerprint matching will be carried out between cardholder's fingerprint and the fingerprint template stored in his smartcard wherever applicable.

### For all locations

Each turnstile/entry point shall have one or two readers. One reader per turnstile/entry point has been considered for controlling the entries. For controlling entry and exit (where required), two readers (one for entry and one for exit) have been considered.

All entries/exits will be logged with a time & date. Provision will exist to limit access to an individual or a group of people to certain areas, or at certain times or from certain entry points. The operator shall have total control on such requirements based on Authorization Level.

Visitors at each location will be required to collect visitor smart cards from the security entrance at respective location, desired work centre access levels will be programmed by operator at time of issue of the card (Note: These access level are the same as the access control module)

### **For locations where turnstile gates are to be installed**

At places where turnstile gates are to be installed, the timings for each entry point can be field defined i.e. can be programmed by the user as and when desired. The entry point will automatically get closed after 5 seconds for "normal users". For VIP visits and special events, it will be possible to manually override the turnstile gates at the site itself via an egress switch, but this facility will generate alarm logs in Application Software.

### **For locations where Boom Barriers are to be installed**

The boom barrier mechanism is planned at locations for entry/exit of vehicles/material trucks or any other type of automobiles with drivers through the secured area, the smart card reader shall validate authenticity and authorization of the smart card issued to the driver [cardholder] and lifts the vehicle barrier. The time of entry and exit along with date, card and the cardholder details will be recorded in the reader. A manually operated override switch for opening/closing of the barrier will be provided at a convenient location specified by security section at the time of implementation. The override would enable manually controlled operation of the barrier.

## **Technical Features**

This software has the following features.

### **SOFTWARE USAGE**

- Easy-to-use Menu-driven graphical interface
- Secure Log On to Software
- User Levels and permissions by Super User to ensure authorized usage of software

### **ACCESS FEATURES**

- Configuration of Locations
- Network monitoring tool which gives status of readers in the network
- Coupling to Finger-scan Reader for biometric based Access
- Configuration of upto 40 Time zones
- Multiple Access Levels for any Cardholder
- Specific Access definitions for Holidays.
- In / Out flag processing for locking out cards that have violated the anti-pass back feature
- Denial of lost / stolen cards by Readers. These cards are referred to as void cards.
- Tracking specified cards for transaction viewing
- Provision for Entry-Reader-Controlled Egress Switch to Exit a room

- Built-in cards-personalization and cards-issue menus. Hence customer can personalize cards at his will.
- Configurable Beep from Reader to indicate Door-Open-too-Long
- Software-controlled Door Open and Close
- Door open time zone
- Configuration of Areas
- Event task
- Area members

## SERVER – READER COMMUNICATION

- Remote download and update of local database of Readers from SERVER. Hence SERVER-independent validation of cards by Readers.
- Support of up to 255 Card Readers on a single TCP/IP to RS485 Line.
- Automatic download of time-stamped transactions from Readers to SERVER via the RS485 to TCP/IP and stored in the local server database.

## READER SPECIFIC FEATURES

- On-board lithium backed memory on Readers for retention of data up to 10 years
- On-board transaction storage on Readers for deferred download to LOCAL SERVER in event of LOCAL SERVER downtime. Upper limit of storage is 6,000 transactions; can be augmented
- Support of upto 3,000 Cardholders; can be augmented
- Customized message display on Readers for various types of card flash events.
- Suitable tri-Colour LED indications to differentiate between valid card flashes, invalid car flashes and Door-Open Too-Long event.
- Different types of Buzzer indication along with the appropriate LED Colour indication.

## Software Requirements

### Central Server

#### Software

Windows 2000 Server & Above  
MS- SQL Server 2000 or Oracle 8i & above.  
Internet Explorer 5.0 & Above

#### Hardware

Any standard business IBM/HP Server system with processors 3.0 GHZ & above.  
1 GB RAM and (HT – Hyper Threading) 80/120 GB Hard Disk.  
COMM ports required - 2  
Network switch - 10/100 MBPS

## Client

## Software

Windows 98/2000  
Internet Explorer 6.0  
MS SQL Server 2000 / Oracle 8i & above

## Hardware (Optimum)

Any Standard IBM/HP Server Machine with processor speed 3.0 GHZ and above. 1 GB RAM or above, 80 GB Hard Disk or above.  
COMM ports required - 2  
Network switch - 10/100 MBPS

## Abbreviations Used

The following are the abbreviations used in this document.

DB	- Database
SmaX ADV	- Smart Access control System, Advanced Version.
TCP/IP	- Transfer control protocol/Internet Protocol
DOTL	- Door Open Too Long

**(Note: This is a Draft/Suggestive Copy only. Contents in this document are subject to change without any notification)**