TECHNICAL SPECIFICATIONS

*Airport Entry Card (AEC) Program*

Card, Readers & Biometrics Technologies
Introduction

The Bureau of Civil Aviation Security hereby issues an integrated card and biometrics based airport access control solution for the airports in India. The current airport complexes are a cluster of buildings spread over many acres of land. Security agencies are handling the most difficult task of ensuring safety of both assets and people with available resources and a largely manual system for identification of personnel.

Entry/exit gates are manned by officers and men of CISF/APSU and IDs of all personnel entering into the building are physically checked by this para-military force. At present personnel are issued simple plastic ID cards, called Airport Entry Pass (AEP) for accessing the secured areas in the buildings, based on a designed colour coding scheme. The personnel may exit/enter the buildings any number of times while they are on duty and may go to public places for refreshment etc. at any time.

As the personnel are manually checked there are many possibilities of human errors thereby compromising security. The current Plastic Identification card is not a fully secure media and can be easily duplicated. There is no mechanism to monitor the movement of personnel inside the premises and no means of knowing whether the individual is on duty. There is also the possibility of unauthorized individuals entering the premises using forged, stolen, or expired identification cards or gaining access because of their familiarity with the security procedures.

To overcome the shortcomings of the manual operation, BCAS proposes to provide personnel with a Secure Contactless Card for access which allows for Biometric template to be stored in the Card for multi-factor authentication which shall be a part of a simple but completely automated system for authentication and access. The Contactless Card shall be fool-proof and almost impossible to replicate, creating a mechanism for monitoring/control of the movements of personnel and vehicles into the airports.

The doors and access points will be released only to authorized personnel after they have been identified by the system. Each entry/exit will be logged centrally for future reference. The system shall also be able to generate any level of information required on the persons available in the building at any given point of time. The system shall provide comprehensive historical data of all personnel who have visited the building. The solution will have minimal manual operation for overall success.

The committee has developed this document with inputs from various agencies, references of similar installations in the world and leading technology developers in the Electronic Access Control industry. This Airport Entry Card (AEC) Program has been developed and presented further in this document. BCAS is responsible for program delivery, including system administration and training of personnel. The User segment will be:

1. Airlines
2. Airport operators
3. Indian Customs, Immigration
4. APSUs and other security agencies, NSG, etc
5. Related service providers and others
The AEC program will encompass the issuance and administration of a restricted area identification system also. This system will incorporate biometric technologies to positively confirm the identity of the card holder. The biometric templates captured during the enrollment process will be stored within the integrated circuit chip of the card. The AEC will be issued by and remain the property of the BCAS.

The Contactless card reader is required to perform a comparison between the biometric template stored on the card and the live sample supplied by the card holder. In the case of a positive match of these samples, the reader must be able to communicate the successful match of the biometric with the access control system of the host airport.

In summary the Objectives are to Develop and Implement a highly secured access control system for the airport complex to:

- Enhance the safety and security of the valuable infrastructure and prevent unauthorized entry into the airports.
- To identify, categorize, verify and validate personnel data and biometrics credentials in real time.
- To minimize human error and opportunities for misuse/encroachment in operational and sensitive areas.
- Alert authorities to an attempted intrusion or other irregularities.
- Analyse incidents in real time and post event.
- Use of advanced technology to minimize human intervention.

**Proposed Solution**

Following are the key components of the proposed solution.

a. Access Control System
b. Application Software
c. CCTV Surveillance System
d. Web Infrastructure
A. ACCESS CONTROL SYSTEM

To the user, an access control system is composed of:

- A Card that is presented to a door reader;
- The card/biometrics reader, that responds with a secure card format that communicates via Wiegand to a Controller;
- The Controller with the Access Control Software indicating a Valid / In Valid card and Authorization rights assigned to gain or deny access into restricted area.
- The door or gate is then unlocked or remains locked based on the authorization rights.

In the background will be a complex system of computers, software, networking and highly skilled personnel that incorporates robust security, ease of use and functionality to meet the complex needs of the security agencies. This section describes the components and operations of the physical access control solution that will be put in place.

Access Control system Components

The system has been designed to cater to the following: -

- All entry/exist points will have Controlled Access in the form of Turnstiles, doors, etc.
- Biometrics Card Readers will be installed at entry/exit points of designated Restricted Areas.
- Long Range RF Readers will be assigned to allow Authorized Vehicle where vehicles can be automatically identified over 10 meters distance to allow access to Restricted Areas.
- To make biometric verification secure, the biometric data shall be stored in a secure application area within the Card. The live biometric template will be matched against the templates stored inside the card.
- Card issued to the personnel will hold the BCAS AEC Card Format protected by globally unique BCAS AEC Keys inside the card for gaining access into any restricted area.
- Two Biometric templates will be captured for each employee.
- The entire system will be networked for monitoring.
- Data transfer is totally secured through encryption and mutual authentication between the Contactless Card and Readers.
- Authentication of the cardholder will be at the backend Access Control system.
- All successful/unsucessful attempts will be transferred to the database server over the Access Control network on Wiegand.
- The application form will be revised based on a simpler layout without changing/modifying the requirements/data as currently assessed by BCAS.

Access Control Card and Reader

1. Card issuance Process

A Personalization system will be installed at the BCAS HQ in New Delhi and in each of the four BCAS regional office where this activity shall be performed. The system allows BCAS authorized official to run the personalization software to create the AEC cards. The official enters the employee details in the card personalization system, captures the biometric templates and the digital photograph of the employee along with other relevant data. All this data will be stored in the card and formatted as per laid down BCAS AEC Card Format. To personalize the card, the card will be inserted in a Card Printer for printing. The data will then be stored in the central server for future reference. The cards may be colour coded as per the existing scheme of BCAS.
2. **Data Storage in the Card**

Data is stored in the Contactless card after encrypting it. The BCAS AEC Secret keys and BCAS AEC Card Format are pre-initialized inside the card and the Access conditions are specified during the Card Personalization process. To access the Contactless card, the BCAS AEC Secret key has to be authenticated between the Card and Reader.

Every additional Read/Write operation specific to Card personalization on the card is based on a secure authentication process for the authorized personnel. A log of such operations is created and the Management Information System (MIS) will report it to the concerned officials as per guidelines of BCAS. This will ensure complete control of the card issuance/preparation process and avoid any unwanted card creation.

The Data to be stored in the Contactless card chip is as follows:

- The total number of Application Areas should be 32 or more Application Areas within the Card to allow room for more applications in future.
- Application Area 1: BCAS AEC Card Format – This will be a unique 35 Bit Card Format which will be used for Access Control.
- Application Area 2: Will be personalized with the following information
  - Name
  - Date of Birth
  - Designation
  - Organization
  - Valid airports
  - Zones
  - Validity date
  - Father’s name
  - Digital Photo (3 x 4 cms)
  - Unique Srl. No.
- Other Application Areas will be used for Biometric Templates and future enhancements for Information capture.

Following information shall be printed on the body of the BCAS issued AEC

**Front of the Card**

- An embedded hologram
- AEC to be written as an Ultra-Violet Fluorescent Image
- Working airport/region
- Card ID Number (Not to match with internal BCAS AEC Format Number)
- AEC Cardholder name
- AEC Cardholder digital photograph size (3 x 4 cm)
- Organization Name
- AEC Cardholder signature
- Valid till Date
- Issuing authority signature
- Appropriate color for the card

**Back of the Card**

- BCAS AEC to be written as an Ultra-Violet Fluorescent Image
- Emergency Contact numbers
- Date of birth
3. Card Usage

The card holder will enter the building through authorized Access Controlled Doors for entry to the building or designated Restricted Area. The staff or authorized personnel on entering the High Security Doors can access the defined areas inside the building using the secure BCAS AEC Card on a Card Reader mounted on a Normal Security Door. Subsequent movement inside the building is based on a Biometric authentication for High Security Doors and Access rights as specified on the card at the time of personalization. Card Readers with biometric authentication are installed at entry/exit point of all main access control and high security doors.

For Normal Security Areas incase of entry into terminal buildings the process to move from an unsecured area to a Secure Area involves the cardholder to flash the AEC card on Contactless Card Reader mounted on a Pedestrian barrier (Flap Barrier, Turnstiles, automated door, etc.) or the nearby wall. The reader after it authenticates the cardholder allows or denies access. The flaps/ turnstiles shall open if there is a valid card and will not open in the event of a failed attempt besides generating an alarm on the host system for further action/analysis. On successful verification, the reader records the entry time of the card holder in the host Access Control System. Lost/stolen/duplicate/hot listed cards will be checked from the host system prior to opening the gate.

For High Security Areas, the employee has to first present the card to the access control unit, which after initial verification will ask for the biometric template to be presented on the template scanner. The Card Reader with a Biometric module unit verifies the live template against the template stored inside the card. On successful validation the turnstile gate is activated to open and the Host Access Control System stores the data to the database server within the facility.

Vehicle Entry to restricted areas in the airside and for secured parking areas on city side will be regulated. The Vehicle Entry Card (VEC) shall be installed inside the vehicle and the Long Range Reader at vehicle entry point shall be able to read this information from a distance of 10 meters to authenticate the permit for vehicle entry. The Long Range Reader sends the BCAS VEC Format to the host Access Control System for validation of the card. On successful validation the boom barrier is activated to open and the Host Access Control System stores the data to the database server within the facility. The driver and other occupants will get down from the vehicle and present their cards for authentication after which the boom barrier will open and the vehicle shall pass through after all security checks will be performed on it as per existing guidelines. Each passenger must be individually authenticated by the system prior to entry. All vehicle gates with direct entry to the airside will have the system and process in place.

The BCAS central server will hold details of all the cardholders across the entire system whereas each of the facilities will hold the database of only those cardholders who shall be given access to that particular airport. Every 24 hours the BCAS Central server will replicate with the local facilities server and update the local facilities database with any update of cardholder information relevant to its facility.

On any unauthorized access, the facilities server will alert the security person in the control room who will then be required to perform tasks as specified by BCAS. The lockout policy for any cardholder can be initiated by the authorized personnel within a facility. This is updated into the local server and this is then replicated with the BCAS Central server which when replicating other facilities server will ensure central lockout of the cardholder from all facilities across the entire system.
All events and subsequent action taken by the security personnel will automatically result in a log file that will be sent to the designated officials for further action/intimation.

The employee access card will hold two biometric templates for each cardholder. This eliminates the problem of identification in case of injury. When the BCAS AEC card is presented to the Card enabled biometric reader, it will provide an Audio Visual response on the reader to convey Access Granted or Denied.

4. **Duplicate Access Card**

Access cards can be re-issued to a cardholder in case the card is lost/stolen. However the BCAS AEC Card will feature a non matching sequential BCAS AEC Card Format to ensure no card duplication occurs. The Access Control System will lock out the lost/stolen card by disabling the Card Format (system-wide) and the reissued AEC Card will be associated to the cardholder. The issuance is similar to a new card issuance with all data to be loaded during personalization. The new card will be created from the existing database and issued.

5. **Security**

The card shall conform to ISO 15693 standards. The BCAS AEC Card Format and other application data inside the card are protected with a 48 or 64 Bit Encryption key (minimum). To write or access data in the card, valid BCAS AEC secret keys should be present in the card and Reader. It shall be impossible to copy the content of one card to another without supplying the proper BCAS AEC secret key. Data transmission between the card reader and the card will be encrypted. It is not possible to tap the data flow between the reader and the card. The Cryptographic algorithms must meet the Data Encryption Standards (DES).

**BCAS AEC Card Format**

The BCAS AEC Card Format is a 35 Bit Card Format which is programmed into the card memory (Application Area 1) permanently during manufacturing of the card. The card Format is unique and cannot be duplicated. This ensures that BCAS has its own unique identifier and eliminates the possibility of creating another ID card from a standard card bought in the market.

**Ultra-Violet Printing**

BCAS AEC is printed in Ultra-Violet (UV) printing which increases card security and are easy to validate compared to other card security methods. The UV printing can be preprinted with a High Definition Printer (HDPO) to overprint employee information.

**Card Preparation**

During this phase, the initialized card will be permanently stored with personnel details and the biometric template. After storing the cardholder credentials inside the card, the card is then printed with cardholder photograph and other details in the visual portion of the card.

**Card Issuance**

In this phase, the prepared card is transferred from the card issuer to the cardholder after biometric authentication.

**Access Control Reader Preparation**

Readers are manufactured with the BCAS AEC secret keys. The reader key must match the BCAS AEC secret keys thereby ensuring the keys on the Card and Readers are unique.
AEC / Reader Equipment Specification

Airport Entry Card Readers: Card readers should be "single-package" type, combining electronics and antenna in one package, in the following configurations:

1. **Short Range Airport Entry Card Reader**
   1.1. The reader should be of potted, polycarbonate material, sealed to a NEMA rating of 4X (IP65).
   1.2. The reader should contain an integral magnet for use with an external magnetic reed switch to provide tamper protection when connected to an external alarm system.
   1.3. The reader should be UL/C 294 listed, and should be FCC and CE certified,
   1.4. Should conform to ISO 15693 (Read only) Standard.
   1.5. Transmit Frequency: 13.56 MHz
   1.6. Should have a read range of 2”-3” when used with the compatible access card.
   1.7. The reader should require that a card, once read, must be removed from the RF field before it will be read again, to prevent multiple reads from a single card presentation and anti-pass back errors.
   1.8. The reader should have a Wiegand output port and should operate under internal control for read-only access control applications.
   1.9. The reader should have separate terminal control points for the green and red LED’s, and for the audio alarm.
   1.10. Should be capable of providing unique tone sequences for various status conditions.
   1.11. Security keys in the cards and readers should be required to match.
   1.12. Should have flash memory to allow future feature enhancements to be added in the field.
   1.13. The reader should meet the following environmental specifications:
      1.13.1. Operating temperature: -20 to 55 degrees C
      1.13.2. Operating humidity: 5% to 95% relative humidity non-condensing
      1.13.3. Weatherized design suitable to withstand harsh environments
   1.15 Reader should have a lifetime warranty against defects in materials and workmanship.

2. **Long-Range Vehicle Identification Readers: All specifications to be similar to Short-Range Readers, other than the following:**

   2.1. The reader should have a read range of 10 meters (33 feet) when used with a compatible booster placed inside the vehicle.

   2.2. Booster unit shall have the ability to amplify the read range of the Vehicle Identification Card up to 10 meters (33 ft) to provide convenient vehicle access. In addition the embedded Vehicle ID it enables simultaneous identification of driver and vehicle.
3. **Smart Card Read/Write Equipment: All specifications to be similar to Short-Range Readers, other than the following:**

3.1 Should conform to ISO 15693 (Read / Write) Standard.

3.2 The reader/writer should provide two communication ports.

3.3 Wiegand port, for connection to standard access control panels.

3.4 RS232 Port, for connection to PC’s or dedicated microcontrollers.

3.5 The reader/writer should provide two operational modes.

3.6 Internal Control: Read-only Access Control applications, transmitting Wiegand Data.

3.7 Host Control: Read/Write applications, externally controlled via the RS232 Port, supporting stored value or data applications including biometric template storage and retrieval.

4. **Contactless Biometric Card Reader**

5. **Airport Entry Card Specification**

5.1 Airport Entry Cards should be used with access readers to gain entry to access controlled portals (e.g.; gates, turnstiles) and hold information specific to user.

5.2 The card should meet ISO 15693 standard for Contactless Smart Cards.

5.3 The card should meet ISO 7810 specifications and should be in a form suitable for direct two-sided dye-sublimation or thermal transfer printing on the specified printer.

5.4 Unique number card serial number.

5.5 The card should support read/write capability, with a minimum of 32Kbits [4048 bytes] of memory. The 32Kbits card should have a minimum of 32 Application Areas to support future applications.

5.6 The card shall have the capability to store Biometric Templates along with other personal data, as specified.

5.7 The card should allow the reader to compare the biometric template stored on the card and the live sample supplied by the card holder.

5.8 Application Area 1 will have BCAS AEC Card Format – This will be a unique 35 Bit Card Format which will be used for Access Control.

5.9 Application Area 2 will contain personal information.

5.10 It should be possible to store a Digital Photo of size - 3 x 4 cms.

5.11 Other Application Areas will be used for Biometric Templates and future enhancements for Information capture.

5.12 Each Application Area on the card should be secured with a unique, diversified security key, such that data stored in that area cannot be accessed or modified until the card and reader have completed a mutual authentication process.

5.13 The card should be capable of completing any write operation, even if the card is removed from the RF field during that operation.

5.14 Card should be warranted against defects in materials and workmanship for lifetime.
5.15 The card should be capable of accepting a slot punch on one end, allowing it to be hung from a strap/clip in a vertical orientation.

5.16 The card should meet the following environmental specifications:

5.16.1 Operating Temperature: -20 degree C to 55 degree C.

5.16.2 Operating Humidity: 5% to 95% relative humidity non-condensing.

6. **Airport Entry Card Encoder**

6.1 Provide an AEC Encoder and Programming Software or equivalent, compatible with the selected Readers and Cards. The Encoder should be connected to a compatible PC, to support field programming of user data and security keys.

6.2 The encoder should use encryption on all serial data transmission to and from the PC, and should encrypt all files before storing them on the PC hard drive. The Encoder should also support field programming of reader configuration cards used to configure and program matching security keys into the AEC Readers and Reader/Writers.

7. **Controllers**

7.1 The Controllers shall be UL/EN certified and conform to UL/294 standards. The Integrated Security Management System (ISMS) hardware shall comprise of modular components that connect over standard interfaces to one another called intelligent controllers. Each Intelligent Controller shall have a database storage and processing module (DBU), and once data has been downloaded to the DBU it shall locally make access control decisions. Access granted or denied decisions (excluding card & biometric validation time) shall be made in under 0.5 seconds.

7.2 The DBU shall store firmware in non-volatile flash memory to allow for convenient updates through the head-end software application. The DBU shall store the cardholder and configuration database information in battery-backed memory so that loss of primary power will not cause the loss of the database. The DBU shall support configurations that include upto 8 or more card readers, minimum 44 monitored input points or more and minimum 14 auxiliary output points or more.

7.3 Network Communications: The Access Controllers should have an on – board Ethernet, TCP/ UDP with its monitoring client PC over the local or wide area network. It should have an on – board web server and should support reading technologies as defined in the reader specifications.

7.4 Memory Management: Controllers shall be capable of holding a card database of at least 100,000. The access control system should also support a card database range of one million. Each controller should be capable of storing minimum of 100,000 events with date and time stamp.

7.5 The Controller shall support minimum 90 time zones.
B. APPLICATION SOFTWARE

Integrated Security Management Software)

1. The software should match the controller to support various applications and shall have following features:

1.1 The ISMS shall start up as part of the Operating System and shall be based on Microsoft.NET technology and capable of using open industry standards. It should also support third part applications like CCTV, Perimeter Intrusion Detection System using web services and SQL / Oracle 9i RDBMS.

1.2 The system shall be based on a multiple client – server architecture.

1.3 Disaster recovery: The ISMS product shall support disaster recovery solution using off-site database replication. It shall be capable of supporting options for 99.99% and 99.999% availability.

1.4 Report Generation: History reporting shall include the ability to review all system alarms, access control activity, and operator actions. The system shall support generation of reports detailing the system operation. It shall be possible to replay video clips associated with events by directly interacting with the report as published to the computer screen. The system shall allow custom reporting options by providing an interface to a commercially available ‘off the shelf’ reporting products. The interface shall present all database fields in a structured format, which does not require detailed knowledge of the database design and table relationships.

1.5 Clients: The system shall support an unrestricted number of clients to suit growing requirements. The system shall provide the means for multiple operators to simultaneously administer the system from convenient locations connected via a LAN / WAN.

1.6 System Partitioning: The ISMS shall support an unrestricted number of partitions. The access point readers, monitor points, and auxiliary outputs shall be managed on a partition basis by simply defining which devices are to be included in a partition.

1.7 Events and Alarm Notification: The system should be capable of segregating events and alarms. Alarm management should be capable of being user defined based on priority levels and escalation. The ISMS shall be optionally configured to require operator comments when acknowledging alarms. Each alarm shall be capable of linking video from digital video recorders (if applicable) for incident playback. E-mail Alarms: The ISMS shall support the ability to automatically e-mail alarm condition messages to a destination e-mail address to be defined by the user.

1.8 Graphical Site Maps: The system should have the ability to import and use graphical maps. Maps shall be linked together and the navigation should be user definable. A comprehensive graphical user interface should be custom definable using a library of images, icons and specific animations. Maps shall also have the ability to be configured to appear automatically on presentation of a new alarm, providing the operator with prompt visual indication that an alarm has occurred.

1.9 History Archive and System Back up: The system shall allow on line archiving of history logs, along with database back up of system configuration and cardholder details.

1.10 Anti-Passback: The system shall support both “hard” anti-passback and “soft” anti-passback alarm reporting modes.
C. **CCTV**

CCTV systems as laid down vide BCAS specifications shall be integrated with the Access Control System. Central management software provided will be loaded on existing computers of Central monitoring room and any other computer on the LAN, as desired. This software facilitates the control & Management of all the DVRs connected on LAN.

D. **WEB & IT INFRASTRUCTURE**

1. Within the airport connectivity shall be on LAN/WAN.
2. Airport to Regional BCAS Offices on Broadband Connectivity with a Back up VSAT.
3. Regional office to HQ- BCAS- ‘Same as above’.
4. Regional offices are only connected to the HQ BCAS office and the airports in their region and not to other regional offices.
5. Central, Local and Host Servers and Desktops shall have latest configuration and supporting softwares.

E. **FACILITIES INFRASTRUCTURE**

A central Control Room of 4500 sq. ft. shall be established for integrated monitoring of Access control systems, gates, intrusion alarms, CCTV surveillance and perimeter surveillance to activate real time response. The control room will interface with a node in each building to communicate with QRT for localized action.