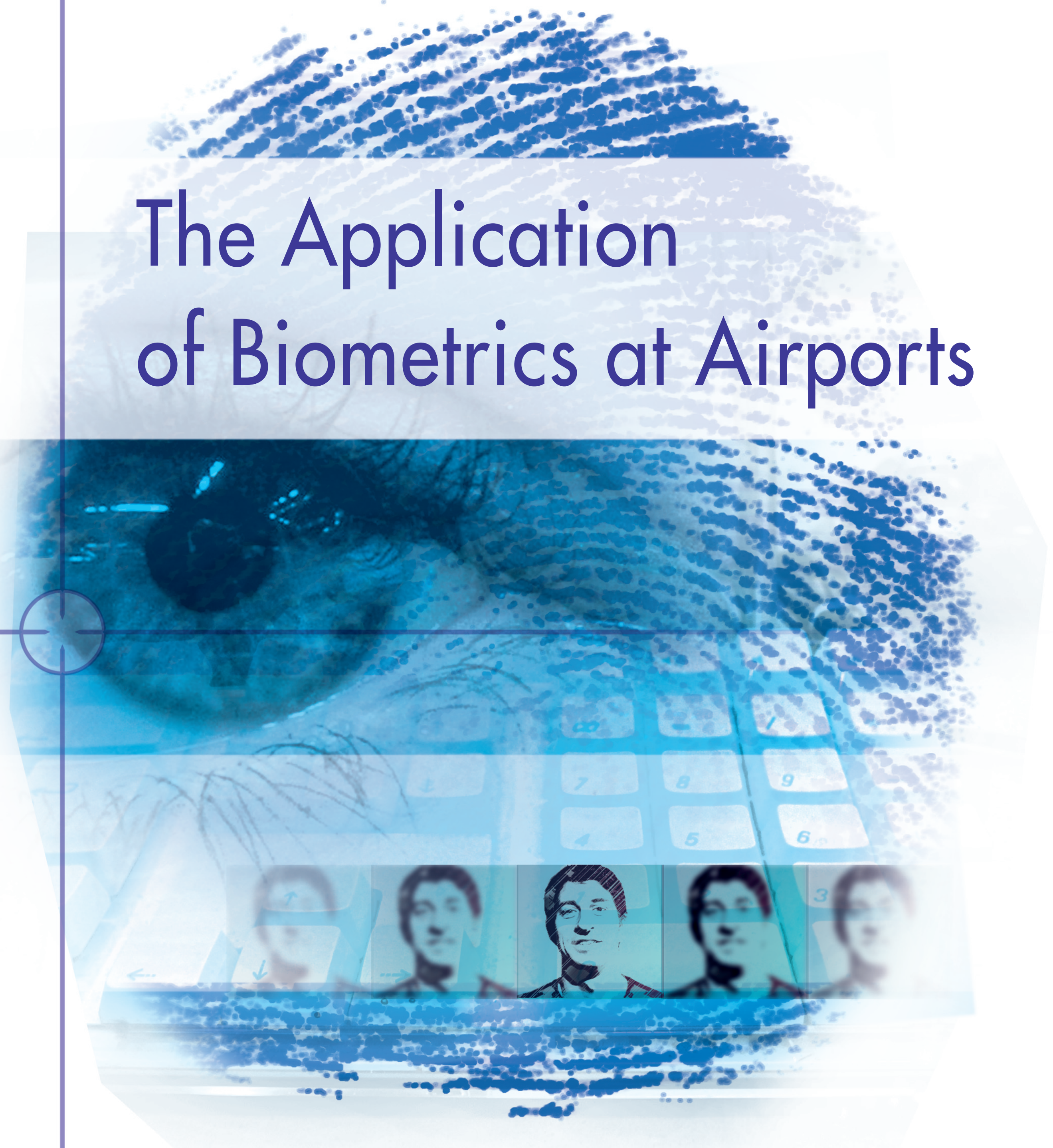
AIRPORTS COUNCIL
INTERNATIONAL

POSITION PAPER

The Application of Biometrics at Airports



November
2005

AIRPORTS COUNCIL
INTERNATIONAL

POSITION PAPER

The Application of Biometrics at Airports

PUBLISHED BY ACI WORLD HEADQUARTERS • GENEVA • SWITZERLAND

Dear ACI Members and World Business Partners,

With the increasing need for secure personal identification in the travel industry and specifically at airports, ACI believes that it is important to have a strong airport position on biometrics.

ICAO, in cooperation with its member States, has coordinated the impending introduction of biometrically enabled passports for air travellers. It is important that airport operators understand the technology and have control over the issues that affect them. Moreover, airport operators are in the forefront of efforts to apply biometric technology to passenger facilitation, especially check-in and boarding processes. Lastly, staff access control is a mandatory requirement of ICAO Annex 17, and access control systems are increasingly using biometrics to check identity.

This position paper provides general recommendations on the development and implementation of biometrically enabled programmes for border control, passenger facilitation and staff access control. It was produced by a Task Force set up by ACI's Governing Board which approved the paper at its meeting on 6 November 2005.

The Task Force developed the document keeping in mind the requirements in all regions of the world. The document has been kept to a high level, since there are many other available sources of information on biometrics, and that standards are set by other bodies – notably ICAO and ISO.

I commend this paper to you and urge you to consider the points herein when developing biometric systems at your airport.

Sincerely,

Director General

Table of contents

SUMMARY

ACI member airports believe that the implementation of biometrics at airports should apply technology to simplify, streamline and enhance the passenger travel process, including border controls and security, while reducing costs.

ACI recommends that biometric systems being deployed at airports must be:

1. Interoperable across multiple systems
2. Performance based
3. Applicable at airports
4. Fast
5. Efficient
6. Secure
7. Reliable
8. Scalable
9. Certified according to ICAO and ISO standards
10. Conscious of environmental requirements/conditions of each location

ACI position

ACI recognizes the benefits of using biometrics to confirm personal identity for border control, airport passenger processing and airport access control, to improve security, efficiency and facilitation. Identity can be verified by capturing a biometric sample from an individual, and comparing against reference data securely recorded on a Machine Readable Travel Document (MRTD), a "smart card", or stored in a database. These methods, together with APP/API (see definitions at end), can enhance security, speed up clearance and alleviate delays at airports.

ACI encourages all member airports to use ICAO standard biometrics in their border control, passenger facilitation and access control implementations, in order to increase security and alleviate congestion, as well as increase customer satisfaction.

ACI supports the worldwide use of ICAO's internationally standardized biometric programme for MRTDs, which uses face recognition as the primary biometric for machine-assisted identity confirmation. In addition, an optional secondary biometric, either fingerprint or iris, may be added to the MRTD. ICAO's standard MRTD and biometric specifications are published in ICAO Doc 9303.

ACI encourages ICAO and governments to continue to promote the use of the ICAO globally interoperable biometric for MRTDs and the use of the globally interoperable data formats for the three biometrics specified in the ICAO Standard (face, fingerprint, and iris). It is equally important that border control agencies and other stakeholders promote the installation of ICAO compliant document reading systems (as well as biometric capture and authentication systems) at airport border control points to assist in identifying the rightful holders of MRTDs.

Passenger facilitation

1. Border control

ACI supports the use of an internationally standardized globally interoperable and ICAO selected biometrics for MRTDs and standardised formats for biometric data.

ACI calls for a harmonized approach, building upon ICAO recommendations, for the use of biometric identifiers in MRTDs. Additionally, biometric systems implemented for border control must be designed to impact positively on passenger flows through the airport. Implementation of such systems is recommended, for both arrival and departure processing (origin and destination airports).

The introduction of biometrics in MRTDs is a national security and immigration issue. Consequently the costs of adapting infrastructure at airports in order to be able to accept these new documents must be borne by governments. However, airports should have the opportunity to take a role in financing the implementation of new systems as a potential business venture, where a return on investment could be developed.

2. Check-in and Boarding

Identifying individuals upon check-in and before they board a plane is extremely important in ensuring safe air travel. Biometric travel document reconciliation systems achieve this specific function. The biometrics of an individual should be used to ensure that the passenger boarding an aircraft is the same person as the one who checked in; if neces-sary, an individual's biometric data can also be matched against a "watchlist" to prevent undesirable persons from boarding.

From check-in counters to boarding gates, biometric templates can either be written on the boarding pass (ATB magnetic stripe and/or 2D bar codes) or transmitted by the Departure Control System network, in which case a provisional database is needed. This procedure takes little time and can be completed during the normal check-in boarding process; therefore no extra strain is put on the congestion of the airport.

The implementation of biometrics on a Common Use (or airline dedicated) Self Service kiosk can be a viable way to capture the passenger's biometrics upon check-in.

3. Passenger Security

The airport should provide the necessary know-how and flexibility to achieve the integration, automation and interoperability of security systems, based on biometric recognition technology. This technology should support smooth facilitation and passenger flow within the terminal.

The goal of airport security systems should be to ensure unequivocal passenger identification and to monitor passenger movement from profiling / check-in, through to boarding at the corresponding gate. Passenger identity should be checked by the system against Interpol and national watch-lists of criminals and terrorists. This would provide a significant increase in security, relying on biometric identity confirmation of passengers at each control point, from check-in until they board the right aircraft, thus avoiding identity switches or the use of fraudulent documents.

The systems to be implemented should speed up the validation processes for individuals and their travel documents. In this way, without unnecessary intrusion into a passenger's privacy, the passenger should perceive both a higher level of security and easier passage. Airport management should allocate sufficient human and budget resources to the tasks of implementation, infrastructure adaptation, maintenance and upgrading.

Airport utilization of staff biometric credentials

1. Access control for airport staff

ACI calls upon national regulators to take into account the potential benefits of implementing biometrics systems for enhancing security at airports, particularly in identifying personnel with clearance for sensitive areas of airports.

ACI considers that regulators must determine the security objectives, but leave airport operators to investigate and implement the biometric technology for staff access control that best suits the local conditions that characterise each individual airport; taking into account the robustness, interoperability and scalability of the systems to be implemented. The goal should be that only bona-fide personnel have access to sensitive areas of the airport, and that these personnel have undergone detailed background checks for any criminal history.

2. Other systems

Biometrics can be used at airports to secure and facilitate a variety of other systems than border control, passenger facilitation and access control. For example biometrics can play a role in:

- **Employee background checks:** as with corporate security, background checks have become increasingly vital to ensuring airport security. Airport authorities should conduct criminal record verifications using fingerprint identification for employees who deal with sensitive information or work on the aprons close to the aircraft. Good management practices and regulations dictate that record checks should be completed prior to employment or assignment to confidential tasks. Fingerprint capture stations can enrol staff and match their fingerprint templates with large existing forensic data bases, making background checks easier, faster and more reliable.

- **Logical access control:** airports are increasingly dependant on computer systems and the Internet and are therefore exposed to network hacking. This can be a major risk for airport operations and constitute a serious threat to civil aviation. Biometric log-in on client/ server software can add the functions necessary to secure any network biometrically. Logical access control, log-in and password management (single sign-on), encryption, certificate activation and PKI compatibility are some of the ways airport network and computer systems can be secured.

Understanding biometrics

Biometrics is a generic term used to refer to a physiological or behavioural characteristic that can be measured to verify the identity of an individual. **Physiological** biometrics measure a part of an individual's anatomy, e.g. fingerprint, hand, face, and iris; **behavioural** biometrics measure an action performed by an individual, e.g. voice, signature; in both cases the characteristics have to be identifiable, universal, unique and permanent.

Biometrics can be used to "**verify**" or "**identify**" a specific individual's identity. Verification (authentication) refers to the problem of confirming or denying a person's claimed identity (Am I who I claim I am?). Identification refers to the problem of establishing and or authenticating a subject's specific identity (see more formal definitions at end).

Biometric systems have a series of key processes that have to be completed in order to:

1.allow a person to use the system.
2. achieve verification or authentication of a user's identity.

These key processes include:

a. Enrolment – the capture of the raw biometric
b. Template creation – preserving the biometric via the use of an algorithm to extract a template from the image captured that will subsequently allow the image to be compared to others using the same algorithm.
c. Identification – takes new biometric samples and compares them to saved templates of all enrolled users.
d. Verification – takes new biometric samples of a specific user and compares them to old samples taken from the same user.

These processes can also be developed as follows:

1. Enrolment process, the individual provides a sample of the biometric which is captured by a device (e.g. a camera or a scanner). Information is extracted from this sample to create a biometric representation (template) which is recorded on a storage medium (e.g. chip or barcode).

2. Authentication/verification process: The individual provides a sample of the biometric previously recorded on the storage medium. The representation created from this sample is compared to the (stored) reference representation. As no two biometric representations are exactly identical, the authentication process must determine whether the samples are a close match.

In terms of the main objective of biometrics systems, i.e. the authentication process, the challenge is to achieve a high level of accuracy in the identity confirmation of any given individual. This involves developing a system that minimizes two key problems:

1. Incorrectly matching a sample biometric representation of one individual with the reference biometric representation for another individual **(False Acceptance Rate)**.

2. Failing to recognise a match between a sample biometric representation of an individual with the reference biometric representation of that same individual **(False Rejection Rate)**.

Consideration of ICAO recommendations

ICAO has developed standards for biometrically-enabled MRTDs. These standards concern passports (sometimes known as "e-passports") and related documents such as visas and ID cards, for border control purposes, but may also be utilized by airports developing biometric systems for other purposes, be it for passenger facilitation or access control.

Regarding the choice of biometric technology for border control, the direction given by ICAO is that face recognition is the **primary** biometric identifier, assuring global interoperability, and one or two additional, but optional, biometric identifiers - fingerprint and/or iris – as decided by each issuing State.

For purposes other than border control, it may not be necessary to use more than one biometric technology, as this will risk making the systems more complex, both for passengers and operators, and increasing the cost.

Application of biometrics

Border control

In general, the introduction of biometrics in MRTDs is a government issue therefore this implies that the costs of adapting the passport control booths at airports to be able to accept these new documents must be borne by governments.

Guidance for the use of biometrics for border control

Performance
The performance of a biometrically enabled border control system should be determined by the national regulators in accordance with the standards set by ICAO. A key factor in the performance of any system is that it must improve the passenger processing time and enhance the through-put of passengers.

When designing and implementing the system, the airport operator and border control agencies should also ensure that the system contains fall-back procedures in the event that a passenger is not recognised by the system and must be manually processed.

Standards
The biometric standards for MRTDs are set internationally by ICAO and implemented by national Border Control agencies. ACI members support the adoption of these standards internationally. Common standards for privacy and data protection should be defined between the appropriate agencies of each State.

Facilities
Eventually, biometric systems will need to be installed at all airports where the national authorities wish to benefit from them, and should be managed to complement the more traditional identification procedures. Airports urge the regulatory agencies to consult and coordinate on planning and design of the layout, and integration of the Border Control facilities within the existing airport spaces.

ACI notes that the ideal facility would be a gate or booth that is capable of reading and capturing a single or multiple ICAO standard biometrics which may be included in a passenger's travel document.

When designing a facility, there are many points to consider. System performance is a vital element; however, special attention must be paid to the flow of passengers through the layout / footprint of the system within the airport's facilities. In order to cater for this important facilitation aspect, the design of the system should reflect ergonomic considerations. Two other important items are that the process should be self-explanatory - the usage of the system should be intuitive to all users to avoid slow processing times, and the systems should meet passengers' requirements related to cultural and hygiene factors.

Technology

For the most part, the choice of technology is determined by the regulatory agencies. However, in order to facilitate interoperability, agencies should consider utilizing existing airport communications systems and infrastructure when implementing their technology – i.e. databases, communications, cabling, network, etc.

Costs

Airports request that the regulatory agencies consult them and coordinate with them on the costs and design of the systems to be implemented. The introduction of automated systems should not subject the airport to higher costs than conventional booths, such as the cost of additional or adjusted infrastructure. Costs must be borne by the agencies and NOT by airports, for example the airports are within their rights to charge a rental fee to the agencies on usage of airport facilities and infrastructure.

Passenger facilitation

The use of biometrics for passenger facilitation will benefit air carriers (which may use them in the first instance to provide a higher level of service to their premium passengers, and members of their frequent flier programmes) and government authorities through the use of ICAO and ISO MRTD standards. Airport operators may also benefit from the use of biometric systems to improve passenger throughput; however, the impact on the airport's passenger handling capacity will be largely dependent on how air carriers decide to deploy biometric systems. A "common-user" interface approach for biometrics benefits airport operators for check-in, security screening, passenger segregation boarding and border clearance. A proliferation of different biometric systems amongst air carriers and between air carriers and border control authorities would not deliver an improvement in passenger handling.

Checking that a passenger's identity is consistent throughout all the processes - check-in, border crossing, passenger security check and boarding the aircraft - is the key to ensure that the right person is boarding the right aircraft and that the person boarding is also the same person who has undergone all of the earlier processes. If the passenger uses the same token in all these processes, it is quite obvious that there are benefits to be gained.

As the use of a travel document is relatively widespread in other processes at airports, and even within airline processes, it can be foreseen that MRTDs with biometric identifiers will swiftly be incorporated into these processes. The normal chain of processes that a passenger undergoes at an airport shows that a passport is not only used for border control; the check-in process has a link with the passport as does the boarding process. Airport operators and air carriers should work together to ensure that regulators apply the same biometric identifiers for border control as for the check-in and boarding processes in order to facilitate quicker passenger flows.

In terms of air carrier frequent flier programmes, airport operators encourage air carriers to employ common user systems to avoid the proliferation of biometric systems at dedicated self-service check-in points and dedicated check-in and boarding check points. The use of common biometric representations for air carrier frequent flier programmes should be considered. The integration of ICAO Standard MRTDs with ICAO selected biometrics into the airline process may render redundant the need to use an airline frequent flier card.

Guidance for the use of biometrics for passenger facilitation

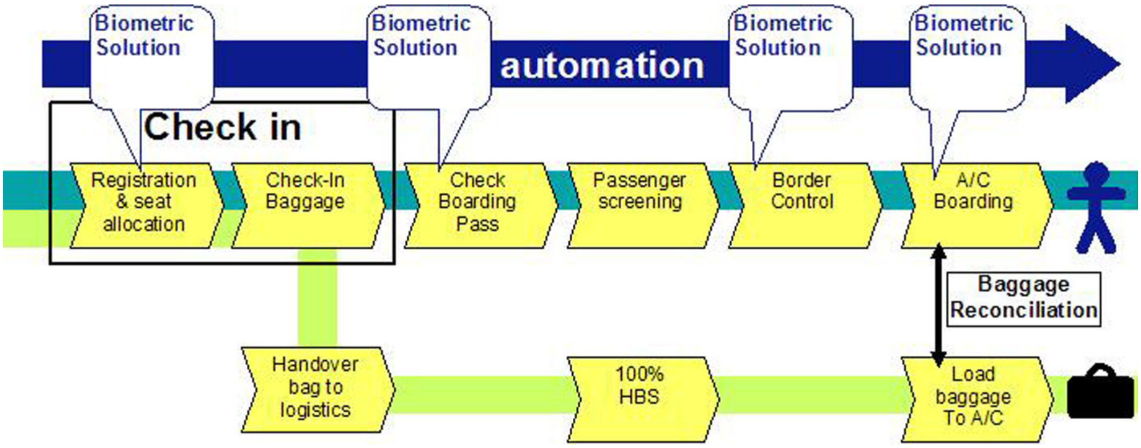


Diagram courtesy of Fraport; based on Simplifying Passenger Travel (SPT) Programme's Ideal Process Flow

The above diagram is a graphical representation of the various passenger processing steps in which a biometric solution can be added to facilitate the passenger flow through the airport. Each one of these biometrics solutions should complement the others, so that the same biometric data and token can be used throughout the system. When feasible, airports and their stakeholders in one location should work with airports and the stakeholders in other locations, to develop interoperable systems that will allow a passenger to travel from one location to another using the same travel token.

Performance

All systems implemented at airports should allow passengers to be processed according to ICAO within the times noted in Recommended Practices 3.36 and 3.39 found in ICAO Annex 9 – Facilitation. These are as follow:

> *3.36 Recommended Practice.— Contracting States, in cooperation with aircraft operators and airport management, should establish as a goal a total time period of 60 minutes in aggregate for the completion of required departure formalities for all passengers requiring not more than normal processing, calculated from the time of the passenger's presenting himself at the first processing point at the airport (i.e. airline check-in, security control point or other required control point depending on arrangements at the individual airport).*
>
> *Note.— "Required departure formalities" to be completed during the recommended 60 minutes would include airline check-in, aviation security measures and, where applicable, the collection of airport charges and other levies, and out-bound border control measures, e.g. passport, quarantine or customs controls.*
>
> *3.39 Recommended Practice.— Contracting States, with the cooperation of aircraft operators and airport operators, should establish as a goal the clearance within 45 minutes of disembarkation from the aircraft of all passengers requiring not more than the normal inspection, regardless of aircraft size and scheduled arrival time.*

Standards and Technology

The biometric standards for MRTDs and other official travel documents are set internationally by ICAO and should be used in an interoperable manner for passenger facilitation. When developing a system, the airport and all other agencies should consider the use of ICAO-standard biometrics, and if possible the same document, e.g. passport to facilitate integration and avoid duplication of systems.

Airports recommend that the implementation of technologies for biometrics be done with common use technologies, i.e. that all devices installed be interoperable across a multitude of airline systems. It is also recommended that the pre-existing airport infrastructure be used by stakeholders for the implementation of biometric systems.

Cost

Airports recommend that new systems being implemented should be designed using readily available "Commercial off-the-shelf (COTS)" technology. Airlines are strongly encouraged to use shared solutions and will be responsible for the TOTAL cost of a proprietary system. However, airports may wish to consider a role in financing a common-use system for the airport (and potential upgrades), as a business venture.

Data protection

National regulators should adopt a policy which balances the goals of protecting personal data when used and processed for biometric systems with the potential benefits that such systems can deliver in terms of increasing security for the passenger and facilitating more efficient passenger flows. Airports will work with stakeholders to ensure the protection of all shared data and will abide by any national or local data protection laws and policies.

Security access control

Airports reserve the right to determine which biometric technology (equipment and template) is appropriate for deployment in their staff access control system and infrastructure.

In its most basic form, airport security managers are looking for a solution which ensures that flight crew and airport personnel are positively identified or verified and granted appropriate access into security restricted areas. Until now, airport security for staff access has been reliant on a series of tried and tested procedures coupled with conventional token or PIN-based access control security solutions. With the recent emergence of biometric identification technology a new capability can be introduced, enabling security managers to allow access to secure areas on the basis that they are able to identify who an individual is, as opposed to what they are carrying or what they know.

The use of a credential with an employee's biometric template for access control is extremely important since, unlike the passenger handling process, access control points for employees can be automated and therefore do not necessarily have to be manned by security staff, unless otherwise required by national law.

Biometric technology for security access control in airports has been applied relatively slowly due to four key factors:

1. "Over-promise" and under-delivery by biometric technology vendors. This issue has already started to disappear as vendors become aware that for a technology to be adopted on a mass scale, the 'customer' must be made aware of the weaknesses as well as the strengths of the technology they represent; all too often, trials do not fulfil the expectations of security managers.

2. Fast progress of biometric technology capabilities. This factor is being mitigated as the leading biometric contenders for various application areas become apparent; however, an element of risk – albeit an informed risk – will always exist in the selection decision.

3. Lack of a biometric interoperability standard. This factor is being addressed by the vendors and the biometrics industry in general, because they understand that airports want to be able to utilize different pieces of hardware within their existing access control system.

4. The lack of a cohesive approach from regulating bodies. This factor is the biggest cause for concern: without the appropriate level of guidance from regulators, airports will remain intransigent on the decision of adopting biometric technology.

Regarding the last point, it is a concern of some airport operators that the use of biometric systems for controlling access of employees to the security restricted area of an airport only makes sense if the terminal area is the only area considered "critical". This is because access control points to these critical parts must be controlled by security staff, who must screen employees for prohibited items and can therefore also identify them as they pass through the checkpoint. Biometric systems can help security staff to perform employee identification as effectively as practiced for border control.

For the reasons above, ACI considers that the role of national regulators must be to determine the security objectives, whilst taking into account the potential benefits of biometrics systems for enhanced security in airport staff access control. The choice and application of biometrics for access control security at airports, however, must be left to airport operators. Airport operators must be able to investigate and implement the biometric technology that best suits each individual location, and furthermore must be able to determine whether the implementation of biometric technologies can deliver tangible benefits, as opposed to other security measures.

Guidance for the use of biometrics for security access control

Performance

The primary reason to incorporate biometric technology into an airport access control system is the ability to validate the identity of the employee who has possession of the ID credential. This will significantly improve security at all access points and airport employee checks.

National regulators must provide a minimum level of performance for any security access control point. The airport is then responsible for ensuring that the system meets the performance requirements set by the regulators and complies with all applicable national laws.

Standards and Technology

When developing plans for the implementation of a security access control system, airports should be sure to incorporate the needs of their tenants in the design of the systems as well as let tenants play a role in developing and setting the standards for the equipment designed for their specific locations, as these may vary from airport to airport.

In order to ensure the ease of development and implementation of an access control system, airports should be involved in the development of regulatory standards from the beginning. This will allow the point of view of the airport operator to be included in the standards.

Cost

Airports recommend that new systems being implemented should be designed using readily available COTS technology. Airports may wish to consider a cost recovery scheme whereby system users will be charged for the usage of the access control system or at a minimum for the development of the token being used.

Data protection

National regulators should adopt a policy which balances the goals of protecting personal data used in biometric systems with the potential benefits that such systems can deliver in terms of increasing security for the airport. Airports will work with stakeholders to guarantee the protection of all shared data and will abide by any national or local data protection laws and policies.

Definitions:

Advance Passenger Information (API):

Standardized biographical data collected and transmitted to the immigration authorities of the country of destination prior to a passenger's arrival in order to expedite the passenger's clearance. API data can include: full name of traveller, date of birth, sex, citizenship or nationality, travel document type including country of issue and number.

Biometric:

A measurable, physical characteristic or personal behavioural trait used to recognise the identity and verify the claimed identity, of an enrolee.

Biometric Data:

The information extracted from the biometric sample and used either to build a reference template or to compare against a previously created biometric template.

Biometric Sample:

Raw data captured as a discrete unambiguous, unique and linguistically neutral value representing a biometric characteristic of an enrolee as captured by a biometric system.

Biometric System:

An automated system capable of:

a. Capturing a biometric sample
b. Extracting biometric data from the sample
c. Comparing the specific biometric data with that contained in the biometric template
d. Deciding how well the two samples match
e. Indicating whether or not an identification or verification of identity has been achieved

Biometric Template:

Data, which represents the biometric measurement of an enrolee, used by a biometric system for comparison against subsequently submitted biometric samples.

Doc 9303:

The ICAO standards publication that defines specifications for MRTD's which allow compatibility and global interchange using both visual and machine readable means.

Enrolment:

The process of collecting biometric samples from an individual and the subsequent preparation and storage of biometric templates representing that individual's identity.

Extraction:

The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

Fast track systems:

expedited registered traveller systems based on the use of a biometric to identify a user as a "known traveller" therefore allowing him/her to be accelerated through the regular airport processes.

Global Interoperability:

the capability of different systems in different locations around the world to exchange data, to process data received from other systems and to utilize that data in the identification and verification process.

Identification/Identify:

The one-to-many process of comparing a submitted biometric sample against all of the biometric templates on file to determine whether it matches any of the templates. The one-to-many approach seeks to find a single identity from a database rather than to verify a claimed identity.

MRTD:

Machine Readable Travel Document

One-to-Few:

The comparison of a single biometric sample to a small number of biometric templates in a database.

One-to-Many:

The comparison of a single biometric sample to a large number of biometric templates in a database. This process is used for identification purposes.

One-to-One:

The comparison of a single biometric sample to a single biometric template. This process is used for verification processes.

Token:

A physical device that contains information specific to the user/holder Verification/ Verify: The process of comparing a submitted biometric sample against the biometric template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template.