A FRAMEWORK TO PILOT TEST
BIOMETRICS AT AIRPORTS

-----

AIRPORTS COUNCIL INTERNATIONAL-NORTH AMERICA
AND
AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES

October 2008
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward</td>
<td>1</td>
</tr>
<tr>
<td>Background</td>
<td>1</td>
</tr>
<tr>
<td>Why Biometrics?</td>
<td>3</td>
</tr>
<tr>
<td>Common Framework /Path Forward</td>
<td>5</td>
</tr>
<tr>
<td>1. Overview</td>
<td>5</td>
</tr>
<tr>
<td>2. How is This Achieved?</td>
<td>8</td>
</tr>
<tr>
<td>3. Key Airport Issues</td>
<td>9</td>
</tr>
<tr>
<td>4. Timing and Next Steps</td>
<td>10</td>
</tr>
</tbody>
</table>
**Forward**

The Airports Council International-North America (ACI-NA) and American Association of Airport Executives (AAAE) developed this document to provide a clear and concise explanation for the path forward to pilot test biometric credentials and biometric access control systems at airports. It is in direct response to the July 3, 2008 memo from the Transportation Security Administration (TSA) which stated “TSA is committed to working with AAAE, ACI-NA, ACC, and ATA to further explore common framework and best practices for airport biometric access control systems that provide enhanced security ... in a cost effective manner.”

It is also intended to provide a general overview and shared understanding by airports, the TSA, Congress, and other stakeholders as to where the aviation industry is headed with implementing biometrics and how they are going to work together to move this process forward as expeditiously as possible. Additionally, this is a “living” document that can be amended and updated as appropriate.

Various documents have been developed over the last year or more that provide important information and guidance regarding use of biometric credentials. This plan recognizes those documents and their application in moving forward with a common framework for pilot testing.

**Background**

Many stakeholders responsible for and concerned with aviation security strongly believe that biometrics should be incorporated into our nation’s aviation security regime. This includes the TSA, the Department of Homeland Security (DHS), and Congress as well as some airport and airline officials.

Regarding airports, a few airports have already incorporated biometrics into their security credential and access control systems. Several others have either partial or limited
implementation, or are now testing biometrics as a step toward adding biometrics to their credentialing and access control system. To date, airports that have introduced biometrics into their credentialing or access control systems have used proprietary systems or created systems tailored to their individual airport facility.

Of note, over the last several years two key issues have affected airports in their consideration of whether to implement biometrics: (1) the quality and reliability of commercially available biometric products, including biometric readers and (2) the lack of standards and guidelines for implementing biometrics.

These two concerns have been largely addressed by (1) the significant advances made over the last several years in the quality and reliability of biometric products and (2) the recent completion by the TSA and industry of updated airport planning and design guidelines that include for the first time biometrics.1

It is also important to note that incorporating biometrics into the existing credentialing and access control systems can be a very significant undertaking for an airport, including planning and financing infrastructure and operational changes. Therefore, any migration to biometric credential and biometric access control systems by airports should be voluntary, timed to meet their operational and facility-specific needs and eligible for federal funding for all aspects of the systems, from improved enrollment processes, to card issuance, to biometric readers. We strongly urge TSA to work with DHS and Congress to create an appropriate and adequate funding source for such undertakings.

1 RTCA-203B “Integrated Security System Standards for Airport Access Control” (Issued June 19, 2008). This document provides standards and guidelines for implementing access control systems in the context of an integrated security system for an airport. This includes guidance on acquiring and designing such systems, testing and evaluating system performance, and operational requirements. The document incorporates the latest technological advances in security access control systems and identity management technologies, including biometrics.
**Why Biometrics?**

In considering whether to implement biometrics it is important to understand what it is biometrics add to an already robust and multi-layered aviation security regime. In short, biometrics add an additional security layer – identity verification of individuals that have access or requests access to security controlled areas at airports.

With biometrics, it is possible to verify that an individual is who they are say they are, and whether they are authorized to be in certain security controlled areas at airports.

Identity verification is a powerful security tool. An individual is “tied” to their biometric credential with their biometric identifier such as a fingerprint or iris. For example, since individuals with unescorted access to certain security controlled areas of the airport are required to undergo a fingerprint-based Criminal History Record Check (CHRC), the biometric identifier used for the CHRC vetting should also be used for real-time identity verification, giving airport operators the assurance that the individual that successfully completed the required background check is the same individual using the credential. As such, the biometric identifier on the credential can be checked for a match against the credential holder’s biometric identifier.

As a security enhancement, a biometric credential provides, for example, the ability to verify a person’s identity and security controlled area access privilege when they are in the security controlled area. Specifically, it is possible using a portable device to immediately determine if someone in a security controlled area is displaying an expired or revoked biometric credential or is not the person authorized to have that credential and is using someone else’s credential. This can be done, for example, by airport law enforcement officers or security personnel on patrol.²

The foregoing model provides a means to incorporate and to utilize biometric-based credentials and access control potentials. But, it does not provide the airport operator

---

² This procedure has been tested at some airports.
complete or even substantial protection from an unauthorized person gaining access to the airside through unintended access points or means. e.g., jumping a fence, or "piggy-backing." By so doing, and presuming a motivated individual's willingness to risk discovery in light of challenge procedures and even random checks using mobile biometric readers, the individual will have defeated the system and rendered valueless the expense and protection associated with the identification and perimeter control aspects of the system described above.

In addition to using biometric credentials for access to security controlled areas and to verify identity and access privilege in security controlled areas, TSA also envisions that biometric credentials could be used to verify an individual at an airport using a credential issued by another airport and presented by that individual to the non-issuing airport. This is technical interoperability and refers only to interoperable identity verification.

This could be done in cases, for example, where the individual is being transferred by their employer from the airport that issued the credential to a second airport where the individual does not have a credential. This process would only be used to verify the individual and check against a central database for purposes of then determining if the new airport would grant security controlled area access privileges to the individual. It is not to allow the credential issued at one airport to be used at the other airport, unless the second airport chooses to allow this.

It is important to note that many airports have either implemented biometrics, are in the process of implementing biometrics, or are in a planning process to implement biometrics. As such they are already in a position or will be in a position to benefit from the security enhancement that biometric credentials and biometric access control systems can provide. This common framework established for biometric credentials and biometric access controls takes into account and protects the capital investments that airports have already made in implementing biometrics. As such, since technical interoperability is focused on identity verification tied to the required vetting of the

---

3 TSA “Aviation Credential Interoperability Solution” (Version 1.0.2, February 27, 2008).
individuals, which relies on fingerprint-based Criminal History Records Checks (CHRCs), the framework should allow other biometrics modes, such as iris, hand geometry, and vascular pattern recognition, to be used in the operational environment, such as on access control doors. Airports are already moving forward and working with TSA and other stakeholders to accomplish this transition to biometrics.

As such, the important thing now is to test biometric credentialing and biometric access control systems at airports in such a way that security is enhanced in a seamless and cost-effective manner in the operational environment at airports. Several airports are willing to pilot test this common framework to provide what has not yet occurred – a process to test, assess, develop lessons learned, and provide guidance to airports, TSA, and the aviation industry at large that will help ensure success as well as the most effective and efficient implementation possible across airports and the aviation system. This is a prudent step that will help facilitate what is a very significant transition, which, again it is important to note, is already underway.

**Common Framework /Path Forward**

**1. Overview**

This document is not intended to be a technical reference document or to explain in specific terms how biometric credentials and biometric access control systems would be implemented from a technical perspective. There are already in place from various sources, documents that provide the technical and technically-related information that airports, TSA, and other industry stakeholders can draw on to implement biometric systems and for which a technical and operational assessment can be made.⁴

Rather, this document is designed give a general framework and direction, from which airports, in cooperation with TSA can implement pilot tests with an eye to actual implementation or improvement of existing airport biometric systems on the basis of

---

⁴ This includes, among others, RTCA-203B “Integrated Security System Standards for Airport Access Control”, TSA “Aviation Credential Interoperability Solution” (Version 1.0.2, February 27, 2008), AAAE “Biometric Airport Security Identification Consortium: Concept of Operations.”
lessons learned. This framework draws on the existing standards, processes and best practices already in place to test migration into interoperable biometric credentials for airports.

Again, these tests will provide, for the first time, a formal process to assess operational “real world” issues that will allow industry to move forward with its already ongoing implementation of biometrics in a prudent manner. It also sends a strong signal in a publicly recognized way that airports, TSA and other stakeholders not only plan, but are in fact, moving forward with biometric credentials and biometric access control systems.

It should be clearly stated the end objective is an interoperable biometric credential that can be used for identity authentication with electronic verification. Airports, at their sole discretion, will determine if electronic verification of the reference biometric will be used at employee portals and gates as part of an airport’s access control system.

In considering how biometrics pilot tests would work, it is instructive to look at the recent employee screening pilot test conducted by TSA with seven airports that volunteered to participate.

The employee screening pilot test provides a good model to follow because: (1) airport participation was voluntary, (2) costs were limited and airports were able to incorporate existing protocols and technologies into the tests, and (3) there was an established process in place to assess the tests at each airport, get airport and TSA feedback, and develop a document outlining the lessons learned that will benefit the aviation sector at large and inform important policy-makers, including Congress. Airports that choose to participate in the biometric credential and biometric access control pilot tests must be allowed to determine and monitor the testing protocols and the final document outlining the lessons learned. The pilot tests must be airport-driven rather than TSA-defined.

Again, it is important to reiterate that with the employee screening issue, some pilot test airports had already moved ahead with additional employee screening protocols prior to
the tests and other airports, while not part of the tests, were already doing selective employee screening activities to address particular issues at their airports – airport specific actions to address airport specific issues above the baseline TSA requirements. This is also the case with biometrics.

Concerning biometrics pilot tests, airports are generally interested in participating in such tests, but have concerns, including how to incorporate such tests into the existing security process, as well as the cost to participate when funds are tight and airlines are experiencing a particularly rough financial stretch. It must be understood that airport managers are very sensitive to adding any costs at this time.

Airports are interested and the industry at large clearly understands the benefits to providing structured tests to help airports move forward with implementing biometrics in a prudent manner. To help accomplish this, there are several options to consider, all of which would be used together, and that would help ensure timely testing and a good “jumpstart” this year to immediately help those airports already implementing biometrics, and help expedite implementation for other airports.

First, any resource assistance from TSA and DHS would be greatly helpful and encourage participation. DHS has indicated that it may be able to provide some “biometric readers” that could be used for such tests. Otherwise, DHS and TSA have indicated there are no other resources available. Airports understand and appreciate this circumstance.

Second, various vendors and consultants are likely to want to participate in the tests and would be willing to provide, at no cost, biometric equipment, software and credentials for these tests. This would allow airports to select a number of interested private sector entities to participate, help assess the test and get a solid understanding of “real world” operational issues by using standard biometric equipment and credentials from different sources at different test airports. This would also help to expedite pilot testing of biometrics.
Third, the upcoming DHS Condition Orange review that will be coordinated by TSA with participation by select airports could provide the opportunity to, as appropriate and as approved by TSA, reallocate security resources for these biometrics pilot tests. Given the security benefit biometrics provide, it is reasonable that this would be a viable option that would encourage participation and timely implementation of testing, as well as a potential method to move forward with actual implementation at airports.

Fourth, there are some airports that have a biometrics infrastructure in place and can rely on this to participate in the testing without incurring significant financial impacts. Like the employee screening pilot tests, such airports provide the capability for relatively quick implementation of testing, as well as the ability to provide valuable information “upfront” to any assessment team.

2. How is This Achieved?

In simple terms, these tests are looking at the issuance and use of biometric credentials and biometric access control systems. The framework will rely on the existing security infrastructure to incorporate use of biometric credentials, including the existing employee vetting structure with Criminal History Record Checks (CHRC) and Security Threat Assessments (STA). All testing protocols will also incorporate standardized biometric credentials and hardware using open architecture.

This framework will include the following:

- The issuance by each participating airport of a biometric credential. Local issuance is a key element because of aviation’s long history of delegated badge authority and the importance of visual challenge programs.

- The facilitation of required federal vetting of the person receiving the credential through a central data base (s), including a biometric duplicate check. There can be multiple central data bases to ensure an open architecture but all central data base(s) must be operated outside of the federal government to ensure visibility.
into the vetting process and to maintain industry standards regarding vetting processing times.

- The storage of the information on the biometric credential in the central database(s).
- The acceptance and checking by a participating airport, for vetting purposes only, of the biometric credential issued by another airport with an accompanying redundant check using the central database(s).
- Security controlled area checks of biometric credentials using portable equipment.
- Reporting from the central database(s) to all participating airports, with confirmation, when a credential has been revoked or otherwise terminated.

3. Key Airport Issues

Because the move to biometric credentials and biometric access control systems is a very significant action, it is critical that this process be done in a manner that ensures success. Therefore, it is important to highlight some key issues so that there is no misunderstanding on the part of any entity as to what the framework is, not only for pilot tests, but for implementation of biometric credentials and biometric access control systems across the nation’s airport system.

Key airport industry positions include that the pilot test and implementation will:

- Be vendor neutral with airport-by-airport selection of vendors.
- Allow for full and open competition.
- Ensure and safeguard airport control and issuance of credentials.
- Not penalize an airport that uses or plans to use for its security system an operational biometric that is different from the biometric credential used for validating an individual across various airports.
- Require cooperation and coordination between airports, TSA, and other stakeholders to work hand-in-hand to ensure success.
4. Timing and Next Steps

By building off existing security vetting processes and investments already made by airports in biometric credentials and biometric access control systems, this framework represents a cost-effective and efficient plan for voluntary testing of interoperable biometric credentials for identity verification. Testing is also eased by using a framework that recognizes airports’ operational needs and financial constraints. In fact, airports today are already working to test the framework needed to create interoperable biometric credentials for identity verification.

As such, working with AAAE and ACI-NA, the appropriate next steps are:

Identify interested airports willing to work together with TSA to test under this common framework and to collect data on operational and other issues to develop a lessons learned document and foster implementation of biometric credentials and biometric access controls. Participation is voluntary. Participating airports can select vendors to assist with the pilot. Participating airports and their selected vendors will work with TSA to define facility-specific test protocols and schedule production, including delivery of biometric credentials.

It is critical (and airports expect) that TSA will be fully engaged with the participating airports and their selected vendors, including the TSA Offices of Transportation Sector Network Management (TSNM) and Transportation Threat and Credentialing (TTAC) as well as appropriate officials from the DHS, including the Screening Coordination Office.