Interoperable Identity Credentials for the Air Transport Industry

A Smart Card Alliance White Paper

Publication Date: October 2008

Publication Number: PAC-08002

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

Table of Contents

1 INTRODUCTION 4

1.1 DEFINING INTEROPERABILITY 4
1.2 DEFINING HIGH ASSURANCE IDENTITY CREDENTIALS 4
1.3 KEY INDUSTRY STANDARDS AND GUIDANCE 5
1.3.1 FIPS 201 5
1.3.2 RTCA DO-230B 6
1.3.3 Aviation Credential Interoperability Solution 6

2 TECHNOLOGIES AND PROCESSES FOR INTEROPERABLE IDENTITY CREDENTIALS 7

2.1 STANDARDIZED INTEROPERABLE DATA MODELS FOR SMART CARDS 7
2.2 INTEROPERABLE BIOMETRIC TEMPLATES 7
2.3 INTEROPERABLE AUTHENTICATION USING CRYPTOGRAPHY 8
2.4 INTEROPERABILITY OF IDENTITY VS. ACCESS CONTROL PRIVILEGES 9
2.5 INTEROPERABILITY AND LOCAL CONTROL OF BADGE ISSUANCE AND DESIGN 10
2.6 INTEROPERABLE CONTACTLESS BIOMETRIC ACCESS CONTROL 11

3 INTEROPERABLE IDENTITY CREDENTIALS: AIR TRANSPORT USE CASES 13

3.1 INTEROPERABLE IDENTITY CREDENTIALS: INCREASING AIRPORT IDENTITY ASSURANCE AND EFFICIENCY 13
3.2 PHYSICAL ACCESS USE CASES 13
3.2.1 Physical Access Control and "Transient" Credentials 13
3.2.2 First Response Officials and Airport Access 14
3.2.3 PACS Migration from Traditional to High Assurance Identity Badges 15
3.2.4 Use of Reference and Operational Biometrics 16
3.3 LOGICAL SECURITY 17

4 STATE OF CURRENT AIRPORT GUIDANCE 18

4.1 TSA GUIDANCE PACKAGE FOR AIRPORT ACCESS CONTROL BIOMETRICS 18
4.2 TSA ACIS 18
4.3 RTCA 18
4.4 BASIC 18
4.5 SMART CARD ALLIANCE WHITE PAPER: EMERGENCY RESPONSE OFFICIAL CREDENTIALS 19
4.6 SECURITY CONSTRUCTION GUIDELINES 19

5 CONCLUSIONS 20

6 PUBLICATION ACKNOWLEDGEMENTS 21

7 APPENDIX A: PACS REGISTRATION INTO A SMART CARD 22

1 Introduction

Since September 11, 2001, the air transportation system—airports and air carriers—has been subjected to significantly more security measures and procedures to counter threats to U.S. civil aviation. One area of security that has received considerable attention is the deployment of an interoperable identification (ID) credential system that would provide identity assurance, electronic identity verification, and potentially, automated access to airport security controlled areas.

This white paper discusses the use and applicability of interoperable identity credentials for airport facilities. It covers the following topics:

- The definition of an interoperable, high assurance identity credential.
- The existing standards and guidance for Federal identity credentials and airport access control and the support they provide for implementing an interoperable identity credential for the air transport industry.
- The technologies and processes that are needed to support an interoperable identity credential.
- The use cases of an interoperable identity credential within an airport.
- The status of current guidance on airport credentialing and access control systems.

1.1 Defining Interoperability

For the purposes of this document, interoperability is defined as follows:

- All personnel are vetted according to a universally accepted standard.
- Breeder documents meet a universally (within the anticipated user community) accepted standard.
- Adjudication and card production processes are conducted according to a universally accepted standard.
- The credential data structure and content, including any biometric data, are standardized.
- Activation and issuance procedures follow a universally accepted standard.
- Card usage causes the local card reader to produce a universally accepted (by all conforming entities) data stream from both valid and invalid access attempts.

As these interoperability elements are documented and processes implemented, the origin of a compliant individual credential becomes irrelevant. Electronically, a credential produced in Seattle behaves the same way as one produced in Chicago and can be read by any conforming reader at any location. A standardized validation and authentication infrastructure can then accept the claimed identity of local employees, contractors, and flight crews with a high level of confidence. Local airport authorities still maintain full control of access privileges.[1]

1.2 Defining High Assurance Identity Credentials

An identity credential is a means to assert an individual's claim of identity. Such claims are normally made when a person requests access to a restricted area or IT network. Because the requesting individual's identity may not be known to the local authority responsible for authorizing such access, the identity credential may be the only item used to establish that the person is who the person claims to be. Often the identity credential that is used is a driver's license with a photo and expiration date. In some scenarios, such a credential may be sufficient to grant an individual the requested access.

Printed credentials are relatively simple to duplicate, manipulate, or otherwise tamper with. They therefore offer very little assurance that the credential is indeed authentic and in the hands of the right person. In summary, the credential-to-user binding is considered to be weak and use of the credential would produce low assurance verification of identity.

[1] It is important to note that trusting and validating "other" identity credentials raise indemnification issues.

A high assurance identity credential produces a strong credential-to-user binding, so that a relying party (e.g., an airport) would have high degree of confidence that the individual presenting the credential is who they say they are.

As an example, within the Federal government, the Federal Information Processing Standard 201 (FIPS 201) Personal Identity Verification (PIV) program defined both the processes and technologies required for high assurance identity credentials. FIPS 201 established a set of criteria for vetting the identity of an individual before an identity credential is created and issued. The vetting process consists of a background investigation that includes several elements, including a biometric check through the Automated Fingerprint Identification System (AFIS). When the FIPS 201 vetting procedure is complete, an individual's identity is established in a manner that is mandated to be universally accepted by all relying parties (i.e., all Executive Branch agencies).

Using a combination of smart card, biometric, and cryptographic technologies, biometric information is then encoded on the smart chip of the card, creating an identity credential that is very difficult to manipulate or duplicate without authorization. When used with electronic readers capable of accessing, reading, and verifying the encoded biometric data against a live biometric sample, these smart credentials can link (bind) a particular person to the presented credential. The result is that the claimed identity is verified with a high level of assurance.

Used in combination with proper cryptographic IT infrastructure, these smart identity credentials can be deployed with an additional validation check against the individual's record maintained with the authority that vetted the individual's identity and created the identity credential. This process can prove not only that the claimed identity is valid but also that the credential is indeed authentic and that the individual is employed by the stated organization. For an airport, the individual carrying such a card could be an airline employee or contractor who needs access to the most critical areas of an airport. This process would establish the individual's identity so that the local airport can make a decision about granting the individual such access privileges.

By using the process and technologies described above, the credential-to-user binding is considered to be very strong, the credential is verified as authentic and valid, and the airport can have high confidence in the identity verification process.[2]

1.3 Key Industry Standards and Guidance

While formal guidance on airport credentialing systems is still being developed, several critical industry standards and guidance should be considered in order to implement systems that are interoperable and deliver high identity assurance. This section provides an overview of the key standards and guidance that are essential to the discussion of interoperable identity credential technologies and processes later in the white paper.

1.3.1 FIPS 201

In 2004, Homeland Security Presidential Directive 12 (HSPD-12) mandated the need "to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification." HSPD-12 specifically calls for the use of a common identification credential for "gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems." HSPD-12 defines the following requirements for Federal identity credentials:

- They must be issued based on sound criteria for verifying the employee's identity.
- They must be strongly resistant to fraud, tampering, counterfeiting, and exploitation.
- They must be capable of rapid electronic authentication.

[2] There are currently no universally accepted standards for defining the relative "strength" of binding card to holder or resistance to tampering with a card or transaction, nor are there universally defined "levels" of confidence or assurance in identity transaction processes.

As a result of this directive, the National Institute of Standards and Technology (NIST) published FIPS 201. FIPS 201 defines the identity vetting, enrollment, and issuance requirements for a common identity credential and the technical specifications for a government employee and contractor ID card—the PIV card. The FIPS 201 PIV card is a dual-interface smart card that is now being issued to all Federal employees and contractors.

A growing number of approved vendors of logical and physical access systems and applications have developed products built on FIPS 201 and industry standards for smart cards. FIPS 201 has attracted international attention and is under consideration for government, public safety, and critical infrastructure personnel in other countries. Within the next five years, 12 million[3] PIV cards will be used in the Federal Government alone, driving a significant expansion of FIPS 201 infrastructure and applications.

Unfortunately, the events of September 11, 2001 placed the airport industry at the forefront of Federal national and international travel security concerns. Many of these concerns encompass identity verification, access control, and facility protection. HSPD-12 and FIPS 201 are the Federal Government's attempt to mitigate identity fraud and the resulting threats to secure information systems and facilities.

1.3.2 RTCA DO-230B

The RTCA DO-230B, *Integrated Security Systems Standard for Airport Access Control*, provides standards and guidelines for implementing access control systems in the context of an airport's integrated security system, including acquiring and designing such systems, testing and evaluating performance, and determining operational requirements.

The document incorporates the latest technological advances in security, access control systems and identity management technologies, including smart cards and biometrics. The document identifies best practices and system requirements to meet the current regulatory standards, as well as information for airports wishing to go beyond these requirements and logical and reasonable methods for implementing advances in security technology.

1.3.3 Aviation Credential Interoperability Solution

The Aviation Credential Interoperability Solution (ACIS) is a program currently under development by the Transportation Security Administration (TSA). It is intended to provide standards and recommendations for an aviation identification credential (and related subsystems) that is interoperable among participating entities. The program uses biometric verification to assert an individual's identity. When complete and implemented, the program will establish proper identity vetting procedures.

The ACIS specification is a draft, and as such, is subject to change. However, it provides a view of identity assurance and the identity management process that is substantially in harmony with RTCA DO-230B.

The specification presents a three-step model for airports to transition from current credentialing and access control systems to interoperable high assurance identity credentialing systems:

1. Identity assurance and identity credential issuance
2. Identity assurance and identity credential issuance with electronic identity verification
3. Identity assurance and identity credential issuance with electronic identity verification and a privilege application for access control

This model provides for the transition as described in the RTCA DO-230B in a controlled and consistent manner. It shows how to gradually adopt the use of an identity credential and grow into a physical access solution.

[3] Figure provided by the General Services Administration.

2 Technologies and Processes for Interoperable Identity Credentials

This section reviews critical technologies and processes – and the standards and guidance that specify them – that are needed to implement an interoperable identity credential system.

2.1 Standardized Interoperable Data Models for Smart Cards

Open and standardized smart card data models allow product manufacturers to design and build products that satisfy customer requirements without incurring the expense of developing the associated infrastructure needed to support those devices. In addition, standardization and data interoperability increase competition and help assure customers that required products and services are competitively priced.

For end users, products supporting open and standardized data models alleviate some risk—if a product does not meet requirements, a competitive product can easily be installed without reissuing identity credentials to the entire staff. Standardized data models also allow for different manufacturers' products to be mixed in a single integrated system. For example, a facility may require card-only access at one portal but require both a biometric and a card at another portal, using a biometric reader from a different manufacturer.

A number of standardized data models have been developed for different smart card-based applications. For identity applications, two data models are in wide use: ICAO for e-passports and FIPS 201 for Federal employees and contractors.

Adopting both HSPD-12 and FIPS 201 would allow members of the airport industry to leverage a Federal standard for identity verification and access control interoperability. One immediate benefit would be identity and system interoperability with other Federal credentials (including the TSA Transportation Worker Identification Credential (TWIC)). However, more important, if the airline industry adopted or modified the FIPS 201 requirements for the verification of an individual's identity, the results—credentials resistant to tampering and counterfeiting, and the capability to rapidly authenticate an individual's identity electronically—would represent substantial improvements in the area of secure access control.

2.2 Interoperable Biometric Templates

The Aviation Transportation Security Act (ATSA) of 2001 described the comprehensive deployment of biometrics for access control at the San Francisco International Airport. ATSA encouraged airports to adopt a biometric solution for vetting access to ensure that the person in possession of access media is the person to whom the media is assigned.

Biometrics must be acquired at two points in the identity credentialing and verification process: during enrollment when identity is vetted and the identity credential is created, and during identity verification to validate that the individual using the card is indeed the person to whom the card was issued.

Raw biometric data acquired by a sensor, such as a bitmap image of live fingerprints, must first be converted into a small biometric template format before matching (template comparison) can occur. A fingerprint biometric template is a collection of extracted fingerprint features, commonly called minutia, which are used for comparison with other templates. Templates are generally significantly smaller in data size than their original bitmap image representation.

An interoperable smart card identity credential should contain an interoperable biometric template generated from the enrollment process, so that any organization using the template can authenticate the identity of the cardholder upon presentation of the card. The interoperable biometric template should conform to an industry-recognized standard data format to simplify implementation and reduce cost by providing a choice of multiple vendor products. The American National Standards Institute (ANSI)

International Committee of Information Technology Standards (INCITS) has published interoperable template standards for fingerprint, face, iris, and hand geometry biometrics.[4]

The FIPS 201 PIV card standard for Federal workers and contractors uses the ANSI/INCITS 378-2004 Finger Minutiae Format for Data Interchange standard for the reference biometric template which is created during the initial enrollment process, encoded on the card, and used for identity verification. Two fingerprint templates are stored in the PIV card memory, and the record is digitally signed to prevent tampering with or replacement of the templates. The two templates are obtained by segmenting the images of the full set of fingerprints captured during the enrollment process. The templates usually correspond to the two index fingers, unless the image quality for these fingers does not meet acceptable standards or the index fingers are not available due to injury or disability.

Interoperable fingerprint templates based on these standards have been independently tested for minimum performance and interoperability by NIST through their on-going Minutiae Exchange (MINEX) interoperability testing program. Information on the test and the relative performance scores of vendors whose template generation and matching algorithms conform to the minimum requirements are available at http://fingerprint.nist.gov/MINEX/.

2.3 Interoperable Authentication Using Cryptography

One of the major goals of the Airport Credential Interoperability Solution (ACIS) program is the ability to use credentials from multiple organizations at multiple facilities. FIPS 201 includes identical requirements: government employees and contractors from multiple agencies can use FIPS 201 credentials to access not only their own facility but also any government building or network, providing that access permissions are granted according to local authorization policy.

Achieving credential interoperability has certain prerequisites:

- A common enrollment and issuance process that meet required assurance levels
- A common method of authentication
- A means of trusting credentials issued by other organizations

The last two requirements are addressed through the use of cryptography and the related cryptographic processes used by a public key infrastructure (PKI).

One common method of authentication that takes advantage of cryptography and PKI uses a digital certificate to fulfill the authentication requirement for "something you have."

When using FIPS 201, two certificates can be leveraged for this purpose. The first is the PIV authentication certificate, which is stored in the smart chip on a dual-interface PIV card and accessed through the contact interface. The PIV authentication certificate requires a personal identification number (PIN) for access and is used to establish that the PIV credential is authentic and valid. The second certificate is the card authentication certificate, also stored in the PIV card's smart chip. The card authentication certificate is accessed through the contactless interface and does not require a PIN for access. In both cases, authentication takes place as a result of a challenge to the private key of the certificate and a response that can be recognized by the reader.

According to the current draft of NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*[5], use of the two certificates meets the requirements for high assurance (in the case of the PIV authentication certificate) and some assurance (in the case of the card authentication certificate). Both certificates can be complemented by an additional biometric authentication factor to raise assurance levels.[6]

---

[4] A complete listing of INCITS biometric standards can be found at http://m1.incits.org/Oct%2025_2007_FP_Published_INCITS_Standards.pdf.

[5] The second draft of NIST SP800-116 is available at http://csrc.nist.gov/publications/PubsDrafts.html.

[6] For a detailed description of this process, see *Security Industry Association Quarterly Technology Update*, Q4 2005, "The Roles of Authentication, Authorization and Cryptography in Expanding Security Industry Technology."

Establishing trust also involves leveraging cryptography and PKI. In this case, trusted credentials contain digital certificates and are tied back to a root certificate authority. In the case of FIPS 201, this authority is the Federal Bridge Certificate Authority.

The first step in establishing trust for a credential is to determine that the credential has not been revoked. Credential revocation status should be determined both initially, on enrollment into the local physical or logical access control system, and then periodically, when new revocation information becomes available. A number of standards-based techniques can be used to determine certificate revocation status, including certificate revocation lists (CRLs), online certificate status protocol (OCSP), and server certificate validation protocol (SCVP).

The second step in the process of establishing trust is to determine whether the issuing authority is trusted. To trust the issuing authority, a chain of trust must exist between the authority that issued the certificates for a particular organization and the certificate authority for all credentials that must be interoperable. Although it is possible to check the status of the chain of a certificate to each issuer for each transaction, checking each transaction is tedious and does not scale. A chain of trust to the Federal Bridge Certificate Authority is the best way to achieve interoperability on a wide scale, particularly interoperability with FIPS 201 credentials.

One of the requirements for FIPS 201 credential interoperability is the use of digital certificates issued by a certificate authority that is cross-certified to the Federal Bridge Certificate Authority at a medium hardware assurance level. An increasing number of organizations are making their cross-certified certificate authorities available as a shared service provider (SSP) for physical access control systems and other systems (e.g., logical access control applications, such as digital signatures and network logon) using interoperable FIPS 201 credentials.

An ideal solution would give airports the flexibility to choose among these cross-certified certificate authorities for obtaining digital certificates. The ability to choose would mean that airports would follow the model being established for emergency response officials (whose credentials must also be recognized by airports in mutual aid incidents) and would also be consistent with the possibility that airports be able to trust any FIPS 201 credential (and associated certificates) issued to a government employee or contractor. Interoperability of FIPS 201 would thus be extended to this very important component of the nation's critical infrastructure.

To summarize, cryptography can help achieve interoperability by leveraging PKI techniques. The use of private key challenge and response as an authentication method for digital certificates that have been validated (checked for revocation) and issued by a trusted certificate authority is the key component of an infrastructure required to achieve interoperability in a secure manner.

2.4 Interoperability of Identity vs. Access Control Privileges

An important point for airports is that the existence of interoperable identity systems does not imply or result in universal access privileges.

Interoperable identity means a standardized method for cardholders to assert their identities to relying parties within a community of airport authorities or aircraft operators so that the relying party can use automated measures to authenticate the card and associate the cardholder with the card. Each asserted identity must be unique within the defined community. Uniqueness can be achieved by assigning a unique identification number to each individual and identification credential used within the community. The numbering scheme used must have sufficient length to ensure that each assigned number is unique. FIPS 201 uses a numbering scheme designed for a specific community of users—the U.S. Government and government contractors.[7] The aviation industry is significantly different from the government and may require a different numbering method, especially when international staff is included.

Interoperable smart cards conform to an agreed-upon set of technical specifications so that all relevant data (including credential identification number, digital certificates, issuing authority designation,

[7] The full text of FIPS 201-1 can be downloaded from the National Institute of Standards and Technology web site at http://csrc.nist.gov/publications/PubsFIPS.html

expiration date, biometric data, and other attributes) stored in memory can be read automatically by readers that conform to the specification. When a card is presented to a reader, the relying party can invoke agreed-upon authentication and validation procedures to verify the following:

- The card was issued by a legitimate and trusted authority.
- The card has not been revoked.
- The data stored in the card have not been altered, duplicated, or replaced.
- The person presenting the card to the reader is the person to whom the card was originally issued.

Airport operators can leverage interoperable technologies and processes for identity-based transactions. Identity-based transactions for access to facilities (physical access) or information systems (logical access) rely on three essential elements: identity assertion, credential authentication, and access authorization. Identity is asserted by presenting the smart card-based identity credential to a reader. The card and the cardholder are authenticated using digital certificates, private keys, asymmetric (public) key cryptography, and biometrics. The final element, authorization (granting or denying access to physical or logical assets) is identity-based, but it is conditional.

Possession of a legitimate interoperable identity credential does not mean that a person is authorized for universal access privileges. Whether to grant access is, typically, the decision of the local custodian of the asset. Access privileges are based on a set of business rules that apply to the authorization process, and these rules may be independent of the rules used to assert identity. For example: “I know who you are, but you still can’t come in because you don’t have a need to access this area."

Unless the access control process can answer two questions—“who are you, and why are you trying to go here?”—access to a facility or information system should not be granted. Trust in an identity credential (such as a smart card) is generally not enough. In most cases, identity assertion and authentication and justification for access are completely separate decisions.

The simplest and most secure solution to grant access privileges is to register or enroll a credential in the local access control system (called privilege granting). To grant a privilege, the local access control system administrator verifies the identity of the cardholder requesting the privilege and also confirms the reasons given for granting the privilege. One approach is to then register the unique ID number stored in the smart card into the local access control system database as belonging to an authorized credential holder.

Another non-FIPS-201-compliant approach is to register the access control system information into the smart card itself. This approach requires the local administrator to write local site identifier and encryption key information into a table stored in the smart card’s memory. The information in the table is used to establish mutual trust between the card and the reader before data is exchanged. (A more detailed description of this approach is contained in Appendix A.)[8]

2.5 Interoperability and Local Control of Badge Issuance and Design

An interoperable identity credential can be implemented while airports retain local control of badge issuance and design.

Local control of badge design is extremely important to airports. Physical appearance is important to airports; all airports are different (layout, system, cards) and colors have unique meanings.

Most airports currently use a unique design for their physical access control credentials. The airport owner/operator wants to be sure that the access credential displayed is the one issued by the local security office, ensuring that all local requirements are met.

[8] More information on the concepts of interoperability of identity and access privilege granting can be found in Sections 3 and 4 of the recently published RTCA DO-230B document entitled “Integrated Security System Standard for Airport Access Control.” This document can be downloaded for a fee from the RTCA web site, www.rtca.org.

Typical designations that are visually identified on an airport credential are no secure access, sterile access, and secure access, although many airports have more complicated structures and, in many larger airports, credentials are terminal-specific. Based on these visually distinguishable aspects, a whole series of challenge programs have been developed and are subject to both Federal regulations and security directives.

The core concept of the challenge programs is that every airport employee or credential holder has both the duty to observe everyone else in a secure area and the right to challenge anyone who is not wearing what appears to be a valid badge. Employees and credential holders also have the right to challenge people at random and to check a badge in more detail. This right is a significant component of every U.S. airport's security program and is emphasized strongly in almost all airport security training programs.

The RTCA DO-230B *User Integrated Security Systems Standard for Airport Access Control* contains extensive information about visual and printed topology features for ID credentials.[9] The document discusses color codes, topology features, and mitigation strategies to defeat threats such as forgery, counterfeiting, alteration, and cloning. A short extract from the document (§A-3.2.2.2) is presented here:

> Design of credentials using color codes must consider:
>
> - Location of color code (e.g., part of the ID card body or part of the background of the photograph)
> - Colors and their designation as verification for access to an area
> - Resistance to counterfeiting, alteration, substitution
> - Regional influences of color codes (e.g., a port authority that encompasses an aviation and maritime facility within the same authority)
> - Federal influences of color codes (i.e., FAA/TSA guidance and regulation; FIPS 201)
>
> Handheld devices may be a useful tool in an ID challenge program. They can be used to read additional information from the credential (e.g., from a smart card chip) and to show the color code registered in secure memory. Color codes that are not protected by secure laminates or other means to ensure resistance to tampering may not provide sufficient security in an ID challenge and verification program.

More recently, in compliance with the guidance stated in the DO-230B, airports have supplemented visual verification challenge processes with electronic verification of badges and credentials by handheld portable terminals. Some airports can also compare biometric data. This check verifies that a badge is still valid, which a visual inspection cannot.

If ACIS-compliant credentials are issued by a local airport owner/operator, it is expected that the airport will have full authority to define the credential. The credential topology defined in Appendix D of ACIS is proposed for use only by aircraft operators (in particular, airlines) who issue their own ID credentials.[10]

2.6 Interoperable Contactless Biometric Access Control

At this time, the proposed ACIS specification only defines operations through the smart card's contact interface. A business case could be made for adding a contactless inlay (e.g., proximity, ISO/IEC 15693, ISO/IEC 14443) to an ACIS-compliant credential to enable local airport owner- or operator-controlled contactless access control. Such a credential may allow airports to avoid requiring two badges: one for identity verification according to ACIS and one for access according to the local access system's requirements.

While the ACIS specification published by TSA is a draft proposal, it is an excellent starting point. It enables the following:

[9] See §A-3.2.2.1 and §A-3.2.2.2.

[10] The draft ACIS technical specification is posted on the TSA secure airport web boards (ACO-200) under General Information. Access to the secure web boards is restricted to authorized airport personnel.

1. Identity assurance through an ACIS-compliant credential and trust model that supports local decisions for access control
2. Field challenge programs for identity within an airport
3. Over time, the opportunity for an interoperable access tool using contactless technology

3 Interoperable Identity Credentials: Air Transport Use Cases

This section describes several uses cases for an interoperable identity credential system, showcasing their benefits to the air transport industry.

3.1 Interoperable Identity Credentials: Increasing Airport Identity Assurance and Efficiency

Over the past several years, airports and air carriers have been issued TSA Security Directives (SDs) that ostensibly focus on vetting individuals before issuing an identification/access credential. Currently, airports are required to conduct a Criminal History Records Check (CHRC) and a Security Threat Assessment (STA) for all individuals who apply for authority to access controlled areas without an escort. These vetting processes must be completed before issuing an ID or access credential.

Over the past year, TSA has been developing a program to provide guidance and standards for an aviation interoperable identification credential system. The ACIS program is designed to properly vet an individual's identity through data and biometrics verification while providing relevant and appropriate airport access according to local policy.

However, ACIS has not yet been fully introduced to or accepted by airport operators. ACIS presents substantial benefits and increased value for identity verification and credentialing. It supports an airport's authority to assign access privileges independently, based on local policies, guidelines, and procedures. To comply with the Transportation Security Regulations (TSR), Part 1542—Airport Security, airport operators assign access authority to individuals based on need, span of movement, and local regulations, if applicable. The ability for airports to assign access authority is absolutely essential in the context of an interoperable identification credential system.

An interoperable identity credential system, such as ACIS, would enhance and enable identity assurance across the entire airport and air carrier security spectrum. Once an individual's data and biometrics are captured electronically, pertinent information could be verified immediately for the purposes of issuing a local ID or activating a credential. An interoperable identity system could significantly improve the current card issuance process, making it more effective and efficient.

ACIS describes a three-step approach that represents a structured transition to an industry-wide interoperable identity and access system. When an identity management and credential information system issues an ACIS-compliant identity credential, the applicant presenting that credential to a registration workstation is providing high assurance identity information to an airport's access control system (ACS). The identity information from the credential is parsed and used to establish a user record in the ACS, while substantially improving the identity assurance for that applicant. Following this, an airport simply completes the enrollment process according to local policies and guidelines, issuing an airport-specific ID or access card or credential. For example, flight crew members with interoperable credentials can be issued airport ID or access media very efficiently or have their credentials activated for local access if permitted by local regulations.

However, one point should be underscored. To ensure absolute control of an individual's access privileges at an airport, the airport operator must ultimately be responsible for issuing and assigning access privileges to individuals with unescorted access authority. Allowing individuals to have universal airport access without local control and authorization completely contradicts the principles and fundamentals outlined in the Federal regulations for airport security.

3.2 Physical Access Use Cases

3.2.1 Physical Access Control and "Transient" Credentials

"Transient" credentials – or non-locally issued credentials – are presented at airports by a number of categories of individuals:

- Flight crews (cockpit and cabin crews) who are not based locally, as well as other airline staff
- Airport staff
- Regulatory agency and other Federal staff
- First responders and mutual aid staff

Today, the main use of transient credentials at airports is by non-local flight crews, including both the cockpit crew, which uses credentials to access the ramp around the aircraft for safety and security checks, and the cabin crew, which controls the passenger loading process in association with local staff.

At most airports these crews do not have local airport badges. In these cases, the airline badge is frequently used as a "flash" pass. In addition, some airports have briefing rooms for cockpit crew and lounges for cabin crew, which are either accessible from the sterile area or through the secure area. The main identification used to access these areas is typically the airline badge, sometimes in association with a PIN. Sometimes access to this area requires that personnel be escorted through a secure area by a local staff member.

In large hubs (for example, O'Hare International in Chicago), some airlines manage their own security in their parts of the airport and use their airline IDs in association with a local system. This ID is not issued by the airport and, outside of these specific areas, is a flash pass only.

Other airline staff with transient credentials are the "deadheads," off-duty cabin and cockpit staff, and occasionally maintenance and customer relations staff who travel using an airline ID to access sterile and airline-specific areas.

In addition, some airports move staff between their operating sites. However, such movement is a limited requirement and can be ignored for credentialing systems unless airline staffing policies change as a result of economic pressures.

Regulatory agencies present additional requirements. At present, the Federal Aviation Administration (FAA) has an agreement with most airports that under certain restricted and airport-specific circumstances, an FAA badge can be used to access sterile and secure areas. TSA and U.S. Customs and Border Protection (CBP) have similar arrangements, but these arrangements are more limited, since typically these staff also have local airport badges. Specialists in various fields are another example of staff that is required to move between several airports. Although individual requirements may vary, they generally require access to both secure and sterile areas.

Finally, first responders and mutual aid staff are occasionally required to access the sterile, secure, or Security Identification Display Area (SIDA) parts of an airport. These staff have until recently used their own agency IDs as flash passes, leading to a number of reported cases of abuse. The TSA First Responder Authentication Credential (FRAC) program is designed to resolve this problem. But again, an interoperable credential would enhance security. This credential would, in many cases, need to be verifiable by a mobile device to be effective.

In all of these transient credential cases, the use of an interoperable credential (combined with a solution to the visual verification and challenge procedure which becomes an issue with non familiar credential designs) could clearly enhance security and provide operational convenience for staff.

In addition, use of interoperable credential as a "breeder" ID whose status could be verified quickly by an airport security office can offer several advantages. Airports could realize significantly enhanced badge issuance to holders, increased security, and reduced costs, even if the end result were the issuance of an airport-specific ID (after any local checking and training requirements were fulfilled).

3.2.2 First Response Officials and Airport Access

The goal of the TSA FRAC initiative is to provide state and local emergency response officials and first responders with a new, Federally-approved smart ID credential designed to achieve the following:

- Securely establish emergency responders' identities at the scene of an incident

- Confirm first responders' qualifications and expertise, allowing incident commanders to dispatch them quickly and appropriately
- Enhance cooperation and efficiency between state and local first responders and their federal counterparts[11]

A number of recent FRAC demonstrations and pilots of ERO programs have been implemented, including programs that involved emergency response officials in the National Capital Region (NCR), Virginia, Maryland, Pennsylvania, Texas, Illinois, Florida, and Colorado.

The FRAC adheres to the FIPS 201 standard and, as a result, supports a wide range of applications. To some extent the range of applications supported depends on the credential profile and the certificates provisioned onto the credential. Since in most cases the companies that are providing the credentials do not charge by certificate but rather charge a fixed price for the credential, it is assumed (and strongly suggested) that the credential contain all available certificates: PIV Authentication, Card Authentication, Signature, and Encryption.

The power of this interoperable credential derives from its ability to support not only emergency and incident use cases but also everyday use. Any access control application contains processing that answers two questions: "Who are you?" and "What are you allowed to do?" The FRAC and FIPS 201 PIV card provide a basis for determining the answer to the first question at a very high level of assurance. The ability to answer the second question depends on the associated infrastructure, be it federal, state, or local.

Armed law enforcement officers often require access to airport facilities. However, airports do not issue their credentials to these individuals, and, at present, these credentials typically cannot be recognized by the physical access control system or by the airport. FIPS 201 can provide a means of interoperability with armed law enforcement officer credentials. State and local public safety officials (which include armed law enforcement officers) are increasingly using FIPS 201 as the basis for interoperable first responder credentials. In addition, Federal armed law enforcement officers will be issued FIPS 201 credentials. Therefore, interoperable FIPS 201 credentials provide a means for airports to address the challenge of recognizing transient armed law enforcement officer credentials.[12]

3.2.3 PACS Migration from Traditional to High Assurance Identity Badges

Airports will need to migrate their installed PACS from using traditional badges to interoperable, high assurance, smart card-based identity credentials.

New smart card-based identity credentials equip security directors with a tool to validate and authenticate the identity and status of individuals requesting access to their resources. The latest state-of-the-art smart card with biometric and cryptography technologies can store data that is significantly different from traditional physical access cards. With one- to three-factor authentication, airport managers can implement a range of identity authentication options and tailor the methods as appropriate for local airport risk assessment and security requirements.

Airport security directors can select the authentication factors they need to confirm the identity of a person before the person is granted access to a secure area:

- Something you have (an identity credential)
- Something you know (a PIN)
- Something you are (a biometric, typically a fingerprint that is verified using the increasingly common FIPS 201-compliant ANSI 378 standard for minutiae templates)

The process by which airport employees, flight crews, and contractors transition to using high assurance identity credentials can present unique challenges and opportunities to airport security directors. Most

[11] http://www.govtech.com/gt/articles/104398

[12] The Smart Card Alliance publication, *Emergency Response Official Credentials: An Approach to Attain Trust in Credentials across Multiple Jurisdictions for Disaster Response and Recovery,* covers topics related to identity and attribute credentialing and credentialing management for first responder officials in depth.

airports already use traditional ID badges and systems for managing physical access. Aviation security directors should ask several questions:

- Will what I have today work with the new directives and requirements? If not, what can I do to comply?
- How do I take advantage of the high assurance identity credential's enhanced security technology to improve my organization's security profile?
- How much of my existing system can I reuse (i.e., how can I mitigate costs)?
- Can I use the same method of authentication for airport employees, transient flight crews, Federal employees, and contractors?

The answers to these questions depend on several factors. Compliance methods range from visual presentation and validation (a flash pass) of the new identity credential (a minimal process with low assurance) to a trusted process using the high assurance identity credential for fast electronic authentication.

Whether an airport is considering upgrading an existing PACS or procuring a new system, certain operational parameters are common and crucial to successful completion.

Today, a typical PACS (new or currently operational) consists of three major components that must be evaluated for compatibility with the new ID credential. These components are:

1. PACS servers
2. Access control panels
3. Readers or multi-factor reader combinations with keypads and biometrics

Any migration strategy must consider that the PACS solution in place may already be tightly integrated with other control technologies, such as intrusion detection systems, video monitoring, and alarm/response management.

It is important to consider that PACS migration activities involve multiple stakeholders, each with some level of jurisdiction in the process. Facilities, IT, and security staff members must cooperate as a team to ensure that the migration process is as smooth as possible.

The migration to high assurance identity credentials also enables an airport PACS to work in coordination with the credential issuance infrastructure. This coordination enables automatic revocation of access privileges registered to credentials that are no longer valid. Coordinating the two systems may require interfacing with new identity system components and pulling information into the local PACS, as opposed to the old method, where identity information was frequently entered manually in the local PACS server.

Before altering an airport PACS to accept high assurance identity credentials, it is recommended that the airport security director define identification verification and authentication goals. The next step is to decide what equipment, if any, is needed to help accomplish this goal. Finally, a transition and migration plan must be developed that meets the airport's needs and budget. The local PACS administrator and the system manufacturer's representative together can evaluate the current level of compliance and develop a migration plan.

3.2.4 Use of Reference and Operational Biometrics

Two categories of biometrics can be used in an interoperable credential program for privilege-based access control at airports: reference biometrics and operational biometrics.

The reference biometric is an interoperable fingerprint template that meets FIPS 201 specifications and is stored on each credential as part of the enrollment process. Each FIPS 201-compliant credential will be issued with a reference biometric to be used for identity and privilege-based access control transactions.

Operational biometrics can include modalities such as iris, hand geometry, face recognition, or proprietary fingerprint systems. Use of an operational biometric is optional and can provide the card issuer with

deployment flexibility in an access control system. This biometric may not be interoperable with other entities and can be used as an alternative to the reference biometric.

There are several cases for using operational biometrics. Operational biometrics can be part of a migration plan to leverage an existing biometric reader infrastructure while adding devices that are compatible with the reference biometric. Under this scenario, as migration occurs, there can be a mix of devices, some of which use the reference biometric, while others use the legacy operational biometric.

In other cases, there may be some site-specific operational requirements that are well-supported by an alternative to the reference biometric. One example might be a secured area where a non-touch biometric is required; iris or face recognition could be options here. Again, a mix of devices can be deployed to leverage the reference or operational biometric that best suits the specific environment. There can be many other cases that support using an operational biometric; the above are simply two examples.

To ensure consistent product performance, operational biometric products should be selected from the TSA Qualified Products List (QPL) of biometric technologies for use in airport access control systems.[13]

3.3 Logical Security

The current funding separation at airports makes it difficult to use security systems for operational requirements (which include information technology systems). Operational systems and facilities are not funded by the FAA Airport Improvement Program (AIP), which is the prime source of funding for airport access control. Until this requirement is waived, the convergence of logical and physical control outside of security systems will be restricted to those airports that do not take Federal funding (currently about 3 out of 475). The use of Passenger Facility Charge (PFC) funding in this regard is not clear since this function may be considered information technology which is not eligible for PFC funding.

However, within security systems, use of an interoperable credential for identification, computer logon and secure communication is permitted. Use even at larger airports has so far been limited, and the use of such technology is growing slowly.

[13] For more details, see http://www.tsa.gov/join/business/biometric_qualification.shtm.

4 State of Current Airport Guidance

One consequence of the incomplete transfer of responsibility for access control from the FAA to the TSA under ATSA in 2001 is that guidance on airport systems is not complete.

The following guidance documents are available:

- TSA guidelines for the use of biometrics at airports, which are still valid but predate FIPS 201.
- The TSA ACIS program.
- Updated RTCA standard, DO-230B, dated July 2008, which contains comprehensive detail and migration guidance on almost all aspects of airport access control. This document was developed after FIPS 201.
- The Biometric Airport Security Identification Consortium (BASIC) white papers.
- The Smart Card Alliance white paper on interoperable emergency response official credentials.
- Security construction guidelines

4.1 TSA Guidance Package for Airport Access Control Biometrics

In response to a request from Congress,[14] TSA issued a guidance package on biometrics for airport access control in September 2005. The package is composed of three documents: *Requirements*, *Implementation Guidance*, and a *Plan for Biometric Qualified Products List (QPL)*. The package includes basic criteria and lists the standards that TSA believes biometric products should achieve in order to meet the technical requirements of acceptable performance for airport access control systems. In addition, TSA has tested and placed certain vendor products on its QPL. The guidance package can be accessed at the TSA web site, http://www.tsa.gov/join/business/biometric qualification.shtm.

4.2 TSA ACIS

The ACIS is a program currently under development by TSA. It is intended to provide standards and recommendations for an aviation identification credential (and related subsystems) that is interoperable among participating entities. When complete and implemented, the program will establish proper identity vetting procedures and use biometric verification to assert an individual's identity.

For more information, contact http://www.tsa.gov.

4.3 RTCA

The comprehensive RTCA DO-230B standards, *Integrated Security Systems Standard for Airport Access Control*, were created by a collaboration of FAA, TSA, the Smart Card Alliance, the airlines, and other industry organizations. The document provides guidelines for the acquisition or upgrade of identify management, physical access control, and intrusion detection equipment for the aviation industry. This document, unlike its predecessor, was developed after FIPS 201.

For more information, contact http://www.rtca.org.

4.4 BASIC

In an effort to bolster airport security, the American Association of Airport Executives (AAAE) and a number of representatives from key airports across the country are working with TSA to create a biometric-based solution for the next generation of aviation worker credentialing and access control. The effort, known as the Biometric Airport Security Identification Consortium, or BASIC, is intended to use the experience and expertise of the airport community to ensure that ongoing efforts to deploy biometric-

[14] Section 4011 of The Intelligence Reform and Terrorism Prevention Act of 2004 directed TSA to develop requirements and performance standards for biometric access control for airports.

based systems in airports come to fruition as quickly as possible and do not disrupt airport operations or diminish security.

Participating airports have identified key principles that must be part of future biometric-based credentialing and access control systems:

- Safeguard local control and issuance of credentials
- Leverage existing capital investment and resources
- Promote a phased implementation approach
- Support the use of a common data set for multiple government vetting requirements
- Encourage vendor neutrality and local determination of vendors
- Strive for resource efficiency
- Target a near-term pilot implementation
- Design an implementation road map that migrates over time

The ongoing work of BASIC focuses on defining a concept of operations and technical standards for a biometrically encoded aviation worker security badge that achieves the following goals:

- Verifies the identity of aviation workers
- Validates worker background information
- Adds security value to the local airport facility
- Limits the number and need for redundant credentials and vetting procedures
- Allows for technical interoperability for identification verification

Additional information regarding the BASIC initiative and a copy of the latest version of the BASIC concept of operations can be found at http://www.aaae.org/government/150_Transportation Security Policy/.

4.5 Smart Card Alliance White Paper: Emergency Response Official Credentials

The Smart Card Alliance white paper, *Emergency Response Official Credentials: An Approach to Attain Trust in Credentials across Multiple Jurisdictions for Disaster Response and Recover*, was developed to describe the benefits of using FIPS 201-based smart cards for emergency response official (ERO) credentials and to present credential use cases that support both emergency response and daily use.

This document is available at http://www.smartcardalliance.org/.

4.6 Security Construction Guidelines

Security construction guidelines, *Recommended Security Guidelines for Airport Planning, Design and Construction*, were issued in March 2006 and are a revision of the 2001 document. These are available from AAAE, Airports Council International - North America (ACI-NA) and the Airport Consultants Council (ACC).

For more information, contact http://www.aaae.org, http://www.aci-na.org or http://www.acconline.org.

5 Conclusions

FIPS 201, ACIS and the RTCA DO-230B are important standards and guidance that form the foundation for an interoperable trusted identity aviation credential.

FIPS 201 provides an established architecture for identity assurance. A FIPS 201 conformant identity credential is PKI-enabled, may be deployed to establish trust across multiple organizations and provides strong authentication verification for access control applications.

The number of air transport industry workers is expanding and includes members from a wide variety of private as well as government organizations. Staff from these organizations provide services ranging from baggage handling, aircraft maintenance, critical operations and management functions. Each individual has legitimate access requirements to controlled areas for both routine as well as for emergency purposes.

All organizations in the aviation community should take advantage of the experience of the Federal organizations that are now deploying FIPS 201-interoperable credentials.

Only an interoperable credential can fully leverage the experience and investment made by the Federal government and industry. Only a FIPS 201-aligned smart card-based credential can meet the requirements of chief information officers and airport security directors who are looking for a cost-effective solution for secure physical access.

This white paper captures best practices and defines use cases for interoperable identity credentials that meet the identity goals of trust, privacy, interoperability and usability. The paper was developed by the Smart Card Alliance Physical Access and Identity Councils after discussion with both government and air transport industry personnel to understand the complexities of trusting identity credentials at airports

The Smart Card Alliance offers an independent assessment of how standards, technology and processes can support the implementation of a high assurance, interoperable identity credential for the air transport industry, while local airports retain the ability to determine access privileges and design and issue local ID badges.

6 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Physical Access Council and Identity Council to provide the air transport industry with educational material on the use and applicability of interoperable identity credentials for airport facilities, and to propose a model for an interoperable identity credential that can leverage FIPS 201 and meet airport operational requirements. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance thanks the Identity and Physical Access Council members and guests for contributing to this report, including: American Association of Airport Executives (AAAE), Airports Council International, BearingPoint, Diebold, DMJM H&N, EDS, General Services Administration (GSA), Hirsch Electronics, Identification Technology Partners (IDTP), IDmachines, IQ Devices, JMF Solutions LLC, L-1 Identity Solutions, Lenel, San Diego Airport, Thales e-Security, Tyco International, U.S. Department of Defense (DoD), U.S. Department of State, U.S. Department of Transportation/Volpe Center

Special thanks go to **Lars Suneborn**, Hirsch Electronics, who led the white paper project, to our guests from the air transport industry – **Colleen Chamberlain**, AAAE; **Marc Dinari**, San Diego Airport; **Lydia Kellogg**, Airports Council International; and **Christer Wilkinson**, DMJM H&N – who contributed to this project, and to the following Physical Access Council and Identity members who contributed to the development of this white paper:

- **Dave Auman**, IDTP
- **Ben Black**, BearingPoint
- **Sal D'Agostino**, IDmachines
- **Mark Dale**, EDS
- **Tony Damalas**, Diebold
- **Major Mark DiCarlo**, DoD
- **Mike Dinning**, U.S. DOT/Volpe Center
- **Clay Estes**, Lenel
- **Ryan Fosegan**, Lenel
- **Marty Frary**, JMF Solutions LLC
- **Bob Gilson**, DoD/DMDC
- **Walter Hamilton**, IDTP
- **Daryl Hendricks**, GSA
- **Steve Howard**, Thales e-Security
- **Gilles Lisimaque**, IDTP
- **Cathy Medich**, Smart Card Alliance
- **Roger Roehr**, Tyco International
- **Steve Rogers**, IQ Devices
- **Mike Sulak**, U.S. Dept. of State
- **Lars Suneborn**, Hirsch Electronics
- **Ryan Zlockie**, L-1 Identity Solutions

About the Smart Card Alliance Physical Access Council

The Smart Card Alliance Physical Access Council is focused on accelerating widespread acceptance, use, and application of smart card technology for physical access control. The Council brings together leading users and technologists from both the public and private sectors in an open forum and works on activities that are important to the physical access industry and address key issues that end user organizations have in deploying new physical access system technology. The Physical Access Council includes participants from across the smart card and physical access control system industry, including end users; smart card chip, card, software, and reader vendors; physical access control system vendors; and integration service providers.

About the Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

Identity and Physical Access Council participation is open to any Smart Card Alliance member who wishes to contribute to Council projects. Additional information about the Identity and Physical Access Councils and about the use of smart cards for secure identity and access applications can be found at http://www.smartcardalliance.org.

7 Appendix A: PACS Registration into a Smart Card

This Appendix is a brief description of a non-FIPS-201-compliant approach for granting access privileges and enabling an identity credential to be used with a local PACS.

Many access control systems have a system identifier as well as a local security authentication key. These two basic data elements could be loaded into an access table within the memory of the smart card, as could a local identification number under which the local access control system registered the card. This local identification number can be different than the credential number that was assigned to and loaded in the card by the card issuer.

The access table, which is maintained and protected within the smart card memory, would be used as a repository for "virtual access control cards" to be used each time a reader device identifies itself to the card as being a component of a particular system. Such an approach allows mutual authentication to establish trust between the card and the reader and does not require universal key management (which is nearly impossible to manage over time, since all keys would need to be changed or revoked in the event of a suspected key compromise).

The reader device initiates the dialog with a smart card by identifying itself first (instead of asking the card for its credential identifier) and allows the card to configure itself for a dedicated secure response to the reader (e.g., using the local identifier ascribed to that system and the local mutual authentication cryptographic key). This approach prevents an attacker with a rogue reader from capturing any of the public identity information available in the presented smart card (e.g., the cardholder's unique identity number or the unique credential identifier). Security and privacy are enhanced because the card is configured to never talk to "strangers."