PARAS PROGRAM FOR APPLIED RESEARCH IN AVIATION SECURITY

PARAS 0017 October 2019

Access Control Card Technology Guidance

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Author(s)
TranSecure Inc.
Olney, MD

National Safe Skies Alliance
Louisville, TN

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about airport security technologies and procedures.

Through the ASSIST (Airport Security Systems Integrated Support Testing) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the Performance and Operational System Testing (POST) Program, Safe Skies assesses the continued operational effectiveness of airport-owned security technologies.

Through PARAS (Program for Applied Research in Aviation Security), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee, but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request for proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies Special Programs Manager*

PARAS 0017 PROJECT PANEL

Martina Benedikovicova *Charlotte Douglas International Airport*
Patricia Harder *Omaha Airport Authority*
Douglas Mansel *Port of Oakland*
Michael Pilgrim *International Security Concepts*
Christer Wilkinson *AECOM*
Lori Anderson *National Safe Skies Alliance*

AUTHOR ACKNOWLEDGMENTS

TranSecure would like to acknowledge the following for their contributions in the development of this guidance:

- PARAS 0017 Project Panel members, who provided significant review and contributions.
- Chicago Department of Aviation, who provided invaluable input during technology pilots, project implementations, and input for this guidance.
- This research would not have been possible without the help of TranSecure's international network of aviation security experts, design engineers, project managers, and technical writers, who provided support throughout the process. In particular, appreciation is given to:
  - James McGuire, Technical Director, TranSecure International
  - Lars Suneborn, Director, Training Programs at Secure Technology Card Alliance
  - Steve Howard, Technical Director at Appian Logic, LLC
  - Don Zoufal, Lecturer at University of Chicago
  - Kristina Dores, ICAO Chief, Aerodromes, Namibia Civil Aviation Authority
  - David Moore, Editor, TranSecure International; filling in for Nancy Hill Ward
  - And especially, Nancy Hill Ward, of Hill-Ward Consultants, who passed away during this effort, and had been a subject-matter expert contributor and editor for TranSecure for over 18 years

CONTENTS

TABLES & FIGURES

SUMMARY

This document reflects the rapid evolution of security-related technology in the airport environment. Specifically, it covers the relatively narrow title field of access control cards. The guidance is intended to give the reader a working knowledge of the range of access control card technologies available, and the operational attributes and constraints of each, in order to aid in the selection of an appropriate upgrade or replacement technology.

The body of knowledge presented here is not prescriptive; it provides a range of alternatives, each of which has both positive and negative characteristics. The guidance found here may stimulate discussion for determining the best card technology options for each airport's unique operational security environment.

PARAS ACRONYMS

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

GLOSSARY OF KEY TERMS

Terms, acronyms, and abbreviations relevant to this document and its subject matter

49 CFR § 1542 Airport Security: US regulations governing airport security

Access Card: A coded card, recognizable to the access control system (ACS) and read by a reader to allow access. It can be used for photo identification of the cardholder and for other data collection purposes. Card technologies include magnetic stripes, Wiegand-effect, proximity (active/passive), and smart/intelligent cards.

Access Control Device: A hardware device that detects the presence of electronic cards. A device has a sensor, which detects the card, and a card reader interface, which decodes the card's electronic data and transmits that information to the computer. The device also detects state changes for doors and monitor points.

Access Control: A set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access.

Access Point: Each means of entry into a controlled security area, consisting of a card reader, monitor switches, and/or latches.

Authentication: The process of establishing the legitimacy of a node or user before allowing access to requested information. During the process, the user enters a name or account number (identification) and password (authentication).

Authentication Assurance: The strength of the technology and its ability to prove the bearer is who they claim to be at time of access to a physical access control system (PACS).

Authentication Token: A portable device used for authenticating a user; authentication tokens operate by challenge/response, time-based code sequences, or other techniques.

Authentication Types:

- Something you know—passwords (cognitive, dynamic, one time, passphrase, static), PINs, specific information known only to the subject
- Something you have—smart cards, proximity cards, magnetic stripe cards, identification tokens, keys, ID badges, passports, transponders
- Something you are (biometrics)—face, fingerprint, iris, vein pattern, voice

Barcode: A machine-readable representation of information in a visual format on a surface. Originally, barcodes stored data in the widths and spacing of printed parallel lines and now in patterns of dots, concentric circles, and hidden in images.

Biometric Access Control: Any means of controlling access through human measurements, such as a fingerprint or voice print.

CIV: Commercial Identity Verification card; a smart card that leverages the PIV framework, but can be used by organizations outside of the federal government.

Central Registry: Each manufacturer keeps records of card numbers used, customer organization, and exact facility location of each card.

DESFire: Data Encryption Standard Fast, Innovative, Reliable and Secure; a proprietary encryption conditional access microcontroller that supports ISO/IEC 14443 A 1-4 & ISO/IEC for radio frequency (RF) interfaces and cryptographic transmissions.

Encryption: The process of scrambling files or programs, changing one-character string to another through an algorithm.

FIPS 201: Federal Information Processing Standard that provides for a common means of identification for persons entering US government facilities.

ICAO: The International Civil Aviation Organization, a precursor and later specialized agency of the United Nations since 1944, is the permanent body charged with the administration of the principles laid out in its Convention and sets the standards for aviation safety, security, efficiency and regularity, and aviation environmental protection.

iCIASS: A brand of credential cards manufactured by HID Global.

Identity Assurance: The strength and process of verifying the individual who is to be granted an access control card for use within a PACS.

IP65: IP rating refers to ingress protection to qualify levels of dust- and water-sealing effectiveness. An IP rating is defined by the letters IP, followed by two numbers. The first number offers a scale of 0–6 and relates to the protection levels against solids like dirt, sand, dust, and debris, while the second number (0–8) represents protection against liquids like moisture and water. The higher the number, the greater the protection against solids and liquids. Equipment rated with any of the three of these ratings is equally protected against dust, dirt, sand, and debris (as indicated by the "6" digit). The liquid/water protection for each of these three ratings is unique: IP65 – Water resistant, IP66 – Water resistant against powerful jets, IP67 – Protected against complete temporary water submersion.

Interoperability: Interoperability is defined as capability to use an access control card issued from any approved issuer, in any conforming ACS regardless of manufacturer. This concept of interoperability may also be applied to cards issued for access to multiple facilities, such as two or more airports operated under one port authority.

ISO: International Organization for Standardization, a primary standards development and issuance organization based in Geneva, Switzerland.

ISOProx: A line of 125 kHz proximity cards manufactured by HID Global

Keypad: A device containing ten numerical digits (0–9) for entering a PIN for multifactor verification.

kHz: Kilohertz, a measure of electronic frequency 1 kHz = 0.001 MHz

Logical Security: An IP network security term that includes electronic measures, such as permissions within the operating system, and access rules at the network layers, such as the firewall, routers and switches.

Magnetic Stripe Card: A technology that allows data to be stored on a plastic card by magnetically charging tiny bits within a magnetic stripe on one side of a card.

MHz: A measure of electronic frequency; 1 MHz = 1,000 kHz

MIFARE: A proprietary encryption conditional access microcontroller that supports ISO/IEC 14443 A 1–4 and ISO/IEC for RF interfaces and cryptographic transmissions.

Man-in-the-Middle: A form of attack in cryptography and computer security, where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other.

Multifactor Authentication: A means of accessing systems, networks, servers, and secured areas controlled by a PACS with multiple security factors such as passwords, PINs, and/or biometric identifiers.

Multiple Technology Card: An access card that hosts multiple, independent technologies that do not communicate or interact with each other.

NIST: National Institute of Standards and Technology is a US Department of Commerce standards development and issuing body.

OCR: Optical Character Recognition; the mechanical or electronic conversion of scanned images of handwritten, typewritten, or printed text into machine-encoded text.

Optical Memory: Optical memory cards are defined in ISO/IEC 11694-4 for security devices for personal identification. Data is stored on the cards in optical domains, which are read-only and cannot be altered by external electromagnetic fields.

Physical Security: The hardware and software components of a PACS that open the physical points of access (portals, doors, gates).

PII: Personally Identifiable Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

PIN: A Personal Identification Number assigned to a user. It is used either by itself or in conjunction with a card.

PKI: Public Key Infrastructure, wherein a Certification Authority algorithmically creates a key pair (public and private) for authenticating requests for access via a Registration Authority.

PIV Card: Personal Identity Verification card; a US federal smart card that contains the necessary data for the cardholder to be granted access to federal facilities and information systems, and assure appropriate levels of security.

Private Key: In encryption, one key (or password) is used to both lock and unlock data.

Proprietary: Not standard among vendors; specific to one vendor only.

Proximity System: No direct contact is required between the card and the reader for the system to operate; the card must only be in the proximity of the reader. The read range will vary depending upon the card/token and the type of reader, from 1/2 inch to up to 33 feet.

Public Key: In encryption, a two-key system in which the key used to lock data is made public, so everyone can “lock.” A second private key is used to unlock or decrypt.

Reader: Refers to the front end that a user must interact with to allow access.

Relying Party: An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.

Replay Resistance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Replay resistance is in addition to the replay-resistant nature of authenticated protected channel protocols, since the output could be stolen prior to entry into the protected channel.

RFID: Radio-frequency identification; wireless non-contact use of radio-frequency electromagnetic fields to transfer data for the purposes of automatically identifying and tracking electronically stored information tags attached to objects at short ranges (a few meters) via magnetic fields (electromagnetic induction); using a local power source such as a battery for greater distances; or by collecting energy from the interrogating electromagnetic field, and then acting as a passive transponder to emit microwaves or UHF radio waves. Battery-powered tags may operate at hundreds of meters. An RFID tag does not necessarily need to be within the reader's line of sight, and may be embedded in the tracked object.

SEOS: A line of 13.56 MHz proximity cards manufactured by HID Global.

Smart Card: A plastic card with a built-in microprocessor, used typically for electronic processes such as financial transactions and personal identification. Available in contact and contactless forms.

SmartKey: A wireless device, such as a fob, that contains encrypted data and user authentication for accessing portals. Similar to the fobs used for keyless entry for automobiles.

Sniffing: The capture of data as it is transmitted over a network. This technique is used by network professionals to diagnose network issues, and by malicious users to capture unencrypted data, like passwords and usernames.

Token: A physical artifact produced (via hardware/software) to interface with PACS and house a PKI certificate (if required). A token is an authentication tool that is utilized to send and receive challenges and responses during the user authentication process.

TWIC™: Transportation Worker Identification Credential™ is required by DHS/TSA to gain unescorted access to secure areas of Maritime Transportation Security Act regulated facilities and vessels

Two-Factor Authentication: Authentication is based on something a user knows (factor one) plus something the user has (factor two). In order to gain access, the user must have both factors.

UHF: Ultra-high frequency radio transmissions, the band from 300 to 3000 MHz (1 m – 10 cm).

UUID: Universally Unique Identifier, a 128-bit value used for identification used in software construction. UUID is the same as Globally Unique Identifier (GUID).

Voice Recognition: Use of voice characteristics as a biometric identifier.

Wiegand: A three-wire wiring standard used to connect a card swipe mechanism to the rest of an ACS. The sensor in such a system is often a Wiegand wire, based on the Wiegand magnetic effect.

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

ABS	Acrylonitrile Butadiene Styrene
ACS	Access Control System(s)
ANSI	American National Standards Institute
CIV	Commercial Identity Verification
FIDO	Fast ID Online
FIPS	Federal Information Processing Standard
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ID	Identification (card/credential)
ISO	International Organization for Standardization
MRTD	Machine Readable Travel Document
NIST	National Institute of Standards and Technology
NFC	Near Field Communication
OCR	Optical Character Recognition
PACS	Physical Access Control System(s)
PET	Polyethylene Terephthalate
PETF	Polyethylene Terephthalate Film
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PIV	Personal Identity Verification
PVC	Polyvinyl Chloride
RF	Radio Frequency
RFID	Radio Frequency Identification
SP	Special Publication(s)
TWIC	Transportation Worker Identification Credential
UHF	Ultra-high frequency
UUID	Universally Unique Identifier

SECTION 1: BACKGROUND

An ID badge is an aid to verify the identity of the person carrying it and the areas of the airport that person is permitted to access. Access authorization may be communicated electronically between a card and reader, or manually through non-technology security features such as background colors, logos, or holograms on the face of the ID badge for examination at a manned door/gate or within the SIDA.

Because of the wide range of operational access requirements across numerous types of employees—including tenants, airlines, service providers, contractors, and governmental entities—it is essential to meet with representatives of each employee type early in the access control technology selection process to determine their requirements and constraints. Further, some circumstances may necessitate special accommodations for non-airport entities, such as local police, fire, or medical personnel in an emergency.

The TSA has identified several technical and administrative security concerns regarding ID cards and access media, and has recommended that airport operators examine access control card technology currently in use at their airports to determine if operational vulnerabilities exist and to explore implementing technologies that provide higher levels of security/encryption.

The guidance provided herein cannot identify a single definitive technology that fits each airport's local environment; it can only help to lead an airport operator to recognize its unique operational and administrative requirements using the pros and cons offered.

To be clear, ID cards and access media are two separate security items whose technologies and operational purposes are closely related; however, this guidance document deals primarily with access media.

SECTION 2: INTRODUCTION TO AIRPORT ACCESS CONTROL CARD TECHNOLOGY

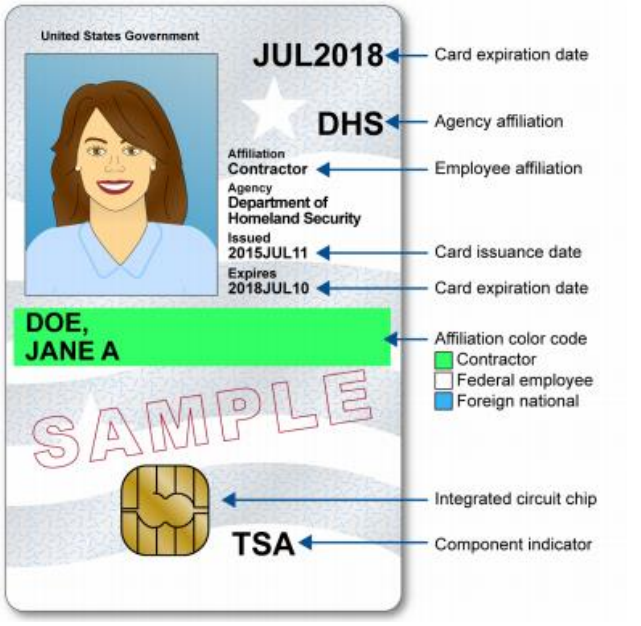
TSA access control regulations under 49 CFR § 1542 provide general procedural requirements that apply to all persons seeking unescorted access to secure parts of an airport. TSA currently does not require the use of any specific access control card technology, only that airports "secure access to the airport" and present the airport's plan to TSA for approval.

Airports can choose access control cards that are available in many types (e.g., contact, such as magnetic stripe, and contactless such as proximity); in many form factors, although the credit card size is the most common; in many different combinations (e.g., the use of photos and imprinted data on the user); and in many types of materials (e.g., Polyvinyl Chloride [PVC], polycarbonate, etc.)

Access control cards with surface-printed personalization features such as first and last name, printed color photo, and organizational affiliation have been around a very long time. Initial use cases for the identity card were to display the claimed identity of the card bearer to a challenger, who would visually examine the card to determine that it was unaltered and that the printed photo looked like the person presenting the card. When the card was deemed authentic and valid, the card bearer would be granted a privilege, such as physical access to a restricted area.

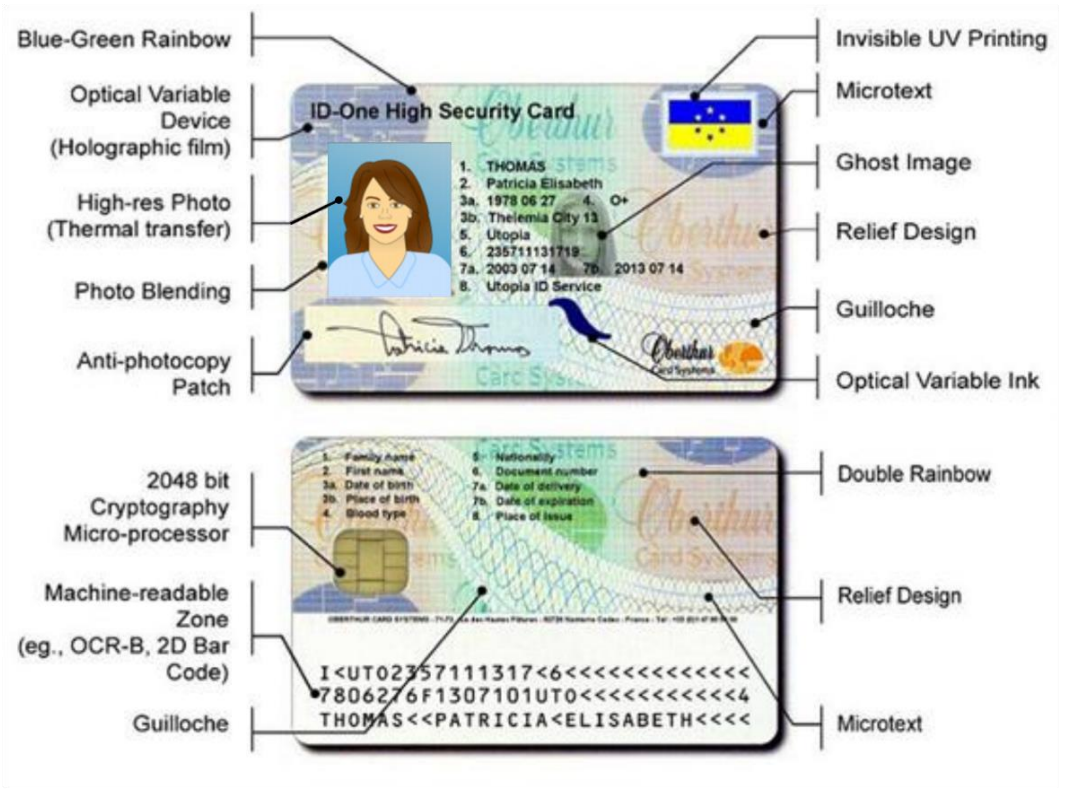
Security access cards have since evolved into many forms with different features, samples of which are shown below in Figures 2-1 and 2-2.

Figure 2-1. Basic ACS Access Card



Source: GAO I GAO-19-138

Figure 2-2. ACS Access Card with Enhanced Security Features



Source: Adapted from NATO NIAPC

As the value of access privileges increased, the threat of forgery, being copied/cloned, or alteration of the identity card also increased. Improved surface-print technologies made forging cards more difficult, thereby increasing the level of assurance in the claimed identity on the card, but the visual authentication process remained unreliable, depending heavily on the human examiner. Subsequently, the addition of magnetic stripe and other technologies provided obstacles to forgery, alteration, or copying of cards, so the level of ID assurance increased.

As technology developed, machine-readable identity cards with non-visible internal or non-human-readable external electronic data elements became available. Magnetic stripe technology required electronic card readers and, typically, that those readers be connected to a back-end airport-wide electronic system pre-programmed with determinations as to whether an individual cardholder had authorization to access controlled areas.

Systems were developed that enabled multiple cardholders to validate identity and verify access authorization at remote access points simultaneously. System and card manufacturers also created a simple card numbering format that permits distinct cards and systems to be produced for each specific location.

Manufacturers keep records of what card numbers are sold, the purchasing organization, and the facility location of each card, if provided by the user. Each card manufacturer's Central Registry enabled manufacturers to minimize the risk of selling cards encoded with the same numeric identifier to different organizations in the same geographic area, while being able to deliver additional cards to any given customer using their own unique sequence of identifiers.

The rapid expansion of access control system (ACS) manufacturers meant that the market for card-based ACS was (and still is) vast. Though some cards still used the initial, simple numbering method for identification, new card technologies were introduced that offered higher levels of user convenience, such as various types of contactless cards/readers, and stronger binding to the authorized card bearer (such as biometric modalities and multifactor authentication methods) became common.

Many airport operators procure ACS that use card technologies that have served the industry well for many years. Consultants often recommend systems that they are familiar and comfortable with, that have worked well for their clients in past projects, and are readily available at an affordable cost. Many such systems have reached or are about to reach the end of their useful life cycle, and airport operators are now beginning to evaluate their options and alternatives for full or partial replacement.

However, similar technology advancements and cost reductions have provided easier access to reasonably priced tools that can compromise card technologies and duplicate cards that only a few years ago were considered difficult to duplicate. Fortunately, technology advancements driven by federal agencies have resulted in new card technologies that mitigate most of the vulnerabilities inherent in legacy access control cards. The pros and cons of these technologies are discussed throughout this document.

2.1 Card Technology Selection Considerations

Card technology selection is driven by the Physical Access Control System (PACS), a key element of an airport's physical security system, and by IT networks, the airport's logical security system, which governs how information is transferred among the many users of an airport. Physical access control refers to the hardware and software installed at portals. Logical access control refers to IT networking permissions, port controls, and other means of security access and the transfer of data across a network. PACS is usually the responsibility of the Airport Security Department, while logical access control is an IT Department responsibility. Both must work together to ensure effective airport security.

The PACS design process may involve completely new readers and software, often requiring new types of access cards, or it may be updating firmware and/or software that may or may not require new card types. PACS reader functional and technical characteristics determine:

- Access card type (contact or contactless)
- Card physical dimensions and surface properties, including the ability to imprint color on one or more surfaces
- Data contents (possibly including biometric data)
- Data storage considerations
    - Magnetic stripe
    - Digital electronic chip
    - Optical electronic chip
- Means of authentication (single/multifactor, biometric/non-biometric)

Additionally, there are high value areas of an airport where positive user authentication is important, including telecommunications rooms and Security Operations Centers. Multifactor authentication is the preferred solution for such areas. For other areas, an airport must assess the risk and vulnerability, as well as the cost-value received, of single and multifactor card technologies.

It should also be noted that training and personnel vetting, while not card technology considerations, are also critical functions of IT security. Other key IT issues include poor password usage and insider attacks, which are not card technology issues in the context of specifying and purchasing access control cards, but access cards will not serve their intended purposes if such issues are not properly addressed.

2.2 Governing Standards

As card technology has become more advanced, card manufacturers are complying with standards developed by various organizations, such as the International Organization for Standardization (ISO). ISO is an independent, non-governmental organization, the members of which are the standards organizations of the 164 member countries. The US member is the American National Standards Institute (ANSI), which publishes its own standards but often adopts ISO nomenclature where ANSI and ISO have agreed on common standards.

ANSI and ISO promote standards to aid in the creation of products and services that are safe, reliable and of good quality. The standards serve to safeguard consumers and the end-users of products and services, ensuring that certified products conform to the minimum standards set internationally.

Additionally, the International Civil Aviation Organization (ICAO) sets standards for aviation safety, security, efficiency, regularity, and aviation environmental protection. The ISO International Electrotechnical Commission (ISO/IEC) and ICAO have created standards that apply to access control cards. Below is a summary of those standards:

- ISO/IEC 7810: Defines physical characteristics of identification cards. Characteristics specified include dimensions, resistance to bending, flame, chemicals, temperature, humidity, and toxicity.
- ISO/IEC 7811: Defines recording techniques related to embossing and magnetic stripes on identification cards. The standard is divided into nine parts related to different recording techniques.
- ISO/IEC 7816: Defines standards for electronic identification cards (smart cards). This standard has 15 parts, each of which pertains to a specific card characteristic.
- ISO 30373: Defines the test methods for identification cards in 9 parts. Part 1 pertains to general characteristics of testing and Parts 2–9 pertain to test methods for specific card types.
- ISO/IEC 14443: Defines proximity cards (e.g., 125 kHz) used for identification. It has four parts that cover physical characteristics, radio frequency power and signal interface, initialization and anti-collision, and transmission protocol.
- ISO/IEC 15693: Defines vicinity cards (13.56 MHz) used for identification. The standard specifies protocols and commands, other parameters required to initialize communications between a vicinity integrated circuit card and a vicinity coupling device, methods to detect and communicate with one card among several cards (“anti-collision”), and optional means to speed up the selection of one among several cards based on application criteria.
- ISO/IEC 24727: Defines the layered framework to support interoperability of smart cards providing identification, authentication, and digital signal services.
- ICAO 9303: Defines specification for machine readable travel documents

The US National Institute of Standards and Technology (NIST) maintains the Federal Information Processing Standards (FIPS) and Special Publications (SP) supporting various applications. The following NIST documents are related to access control card technology:

- NIST FIPS 140-2: Specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments.
- FIPS Pub 197, (May 2002): Defines the Advanced Encryption Standard.
- FIPS 201: Provides for a common means of identification for persons entering US government facilities. It is not mandated for use at commercial service airports, but the standard represents best practices worthy of consideration. More information is provided in Section 3.7.
- NIST SP 800-63: Provides Digital Identity Guidelines, which define levels of security assurance for various credential and token implementations. SP 800-63A covers enrollment and identity proofing; SP 800-63B covers authentication and life cycle management; and SP 800-63C covers federation and assertions.
- NIST SP 800-73: Provides interfaces for personal identity verification (PIV).
- NIST SP 800-76: Provides biometric specifications for PIV.
- NIST SP 800-78: Provides cryptographic algorithms and key sizes for personal identity verification
- NIST SP 800-79: Provides guidelines for the authorization of PIV card issuers and derived PIV credential issuers
- NIST SP 800-96: Provides PIV card to reader interoperability guidelines
- NIST SP 800-100: Information Security Handbook: A Guide for Managers
- NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- NISTIR-7316: Assessment of Access Control Systems, September 2006

SECTION 3: CARD TECHNOLOGY PROPERTIES AND ISSUES

Types of access control card technologies, and their properties and vulnerabilities are described below.

3.1 Assessing Vulnerabilities

The vulnerabilities of access control card technologies include:

- **Forgery:** A fake, unauthorized card is made that looks like an authorized card.
- **Copying/Cloning:** A card is duplicated without authorization.
- **Alteration:** An authorized card is altered in a way that is not authorized, potentially providing increased access opportunities.
- **Skimming:** A nefarious card reader performs a free read of the card to obtain stored credentialing information.
- **Sniffing:** Capturing an entire message being relayed between a proximity card and contactless reader.
- **Capture & Replay:** An adversary captures/sniffs a message from a card when it is presented to a reader and relays the message to the reader at a later time to gain access. This is sometimes known as Man in the Middle, in which an attacker secretly relays and possibly alters the communications between two parties.
- **Known Software Settings:** Some access control reader software comes with industry known default settings. If these settings are not changed, the software has the potential to be hacked.
- **Lack of Binding:** Many card technologies originally enabled a single-factor authentication and were thus more vulnerable to misuse. ACS with the ability enable a second (and third) authentication factor offer a higher level of probability that the presented card is indeed in the hands of the authorized person to whom it was issued. These additional authentication factors help to bind the card and the authorized person, reducing the opportunity for misuse.
- **Interoperability:** Interoperability is defined here as the capability to use an access control card issued from any approved issuer, in any conforming ACS, regardless of manufacturer. This concept of interoperability may also be applied to cards issued for access to multiple facilities, such as two or more airports operating under one port authority. While it can be seen as a benefit, interoperability also requires that the security features of the card comply with the least secure system for which it is used.

Cards containing microcontroller chips greatly reduce, and in some instances eliminate, some of the vulnerabilities cited above, but security professionals at airports should continuously review the adequacy of their ACS to cope with evolving threats and fraudulent actions.

Until a card is associated with a specific individual, its use is uncontrolled and could be abused by other people to gain unauthorized access. Positive user authentication is provided only when a biometric factor is implemented in ACS.

Single-factor, non-biometric ACS are vulnerable to misuse, since the user is not positively identified. Multifactor non-biometric ACS can mitigate this risk by requiring an additional user action, such as entering a numerical code transmitted to the user by email or mobile phone. This is still not considered

positive user identification, but it does increase security, in many cases to a level adequate for the perceived risks.

A PIN is the simplest component of multifactor identification. It is not immune to abuse, but requiring a PIN is still a step up from magnetic stripe technology in providing minimal access control card security. There are several areas of vulnerability associated with PIN use:

- PIN selection at the time the individual is registered into the ACS
- System operators may have access to system user records
- Codes may be observed ("shoulder surfed") by others during the PIN entry process at the door
- An adversary may make attempts to guess PINs at the door, sometimes aided by the wear pattern on the PINs, since a 4-digit PIN has a very small number of possible sequences.

PIN pads may provide more security by scrambling the numbers so that a by-stander does not capture your PIN by observing the pattern of data entry.

Some additional resources on performing risk and vulnerability assessments are listed below:

- Risk Assessment Techniques for Civil Aviation Security
  Tamasi et al., 2011
- Risk Assessment of Aviation Security and Evaluation of Aviation Security Policies
  Yalcinkaya, 2005
- Risk Assessment
  SKYbrary, 2019
- PARAS 0016: Airport Security Vulnerability Assessments
  Safe Skies, available late 2019

3.2 Manually Read Access Control Cards

A manually read access control card is typically a laminated ID card that includes the card holder's name, photograph, and some logo or identifying mark to identify the airport or company where it is valid. The card might also have a number and an expiration date, and may be color coded to denote authorization to be present in a specific area of the airport. This card does not have features that can be read by an ACS, and most likely is used to gain access through a manned access point. Table 3-1 summarizes the pros and cons/vulnerabilities of this ID type.

Table 3-1. Pros and Cons of Manually Read Access Control Cards

Pros	Cons/Vulnerabilities
Low cost	Easily forged, copied/cloned, and altered
Easy to print	If information on the card needs to be changed, a new card must be issued
Enables visual challenge and verification programs	Minimal identification assurance using a trained guard to compare bearer to photograph

Keypads or smart keys and locks can be economical forms of access control that can be used in conjunction with photo/color-coded cards to enhance security. Keypads can be operated in standalone

mode or integrated with other sensors and control mechanisms. Newer keypad technology provides more security by scrambling the numbers so that a bystander does not capture a user's PIN by observing the pattern of data entry.

Smart keys and locks enhance security when combined with this card type as the keys are programmed so that individual users have a unique identity and there is a traceable record of when and where the keys have been used. The battery in the key or lock provides the power to release the cylinder.

3.3 Printable Access Control Cards

These types of cards are becoming increasing rare and likely do not provide adequate security for an airport. However, their descriptions and pros/cons are provided here for informational purposes.

3.3.1 Barcode Cards

Barcode cards can use many different barcode schemes, with the most common being a series of lines of varying thickness. They are available in visible and infrared types. Cards with visible barcodes use a swipe or insertion reader, while cards with infrared barcodes use a reader that can read infrared light. Figure 3-1 shows a barcode swipe through a reader.

Figure 3-1. Barcode Swipe through Reader

Source: Barcodes Inc.

Today, the barcode is mostly abandoned as an access control technology, and readers of that type are available from a limited number of sources. Table 3-2 summarizes the pros and cons/vulnerabilities of this ID type.

Table 3-2. Pros and Cons of Barcode Access Control Cards

Pros	Cons/Vulnerabilities
Low cost	Easily forged and copied/cloned
Issuers may print barcodes during card personalization at the time of issuance	If information is incorrectly encoded, the card must be destroyed and a new one issued
Rapid deployment	If you lose your card, anyone picking it up can use it at unmanned card reader access control points
Can be combined with other technologies	Card reader lens requires periodic maintenance
Easy to integrate with most ACS	

3.3.2 Optical Character Recognition (OCR) Text Cards

OCR access cards, a contact technology, contain scanned images of handwritten, typewritten, or printed-text identity information that has been mechanically or electronically converted into machine-encoded text. The OCR text is scanned by a card reader and the credential number is sent for verification to the ACS. Table 3-3 summarizes the pros and cons/vulnerabilities of this ID type.

Table 3-3. Pros and Cons of OCR Text Access Control Cards

Pros	Cons/Vulnerabilities
Low cost (often free)	Easily forged and copied/cloned
4 MB capacity to store credential numbers, names, and related information	If you lose your card, anyone picking it up can use it at unmanned card reader access control points
Easy to print	If information is incorrectly encoded, the card must be destroyed and a new one issued

OCR text has been adopted for use by the US federal government and has two subsets, OCR-A and OCR-B. The shapes and dimensions of OCR-A are specified in ANSI INCITS 17-1981 (R2000), and the nominal shapes, sizes, and printing positions of OCR-B are described in ANSI X3.49-1975 (R1982). The choice of sizes for OCR-B application is based on requirements for the printing device.

3.4 Writeable and Rewriteable Cards

Magnetic stripe, optical memory[1], and proximity cards allow stored information on the card to be changed without having to issue a new one. These cards can be either contact or contactless. The contactless capability is dependent on technology. Some cards can support multiple modes of contact and contactless technologies, so these cards are often used when migrating from one card technology to another.

3.4.1 Magnetic Stripe Cards

Magnetic stripe cards, a contact technology, are a legacy access control solution that is still widely present in airports. Variable reader configurations exist, including swipe and insertion readers.

There are two types of magnetic stripes, low and high coercivity. Simply, the difference between the two types of cards involves the degree of difficulty in erasing and encoding. Low coercivity cards, generally used for short-term applications, contain brown mag stripes. High coercivity cards, generally used for long-term applications such as access control, contain black mag stripes that are more durable. It should be noted that many card manufacturers switched to low coercivity cards for access control because ATM cards (low coercivity) failed to work when they were stored near high coercivity magnetic stripe access control cards.

Magnetic stripe capability can be used alone or with other card modalities, including proximity contactless cards and PIN pads. These cards can also be used with a biometric to enable two-factor identification; however, the biometric must be centrally stored. Figure 3-2 shows a magnetic stripe card being swiped on a reader with a PIN pad.

[1] Optical memory is add only

Figure 3-2. Magnetic Stripe Card in PIN Reader

Source: Locksmith Pros

Magnetic stripe card technologies continue to exist where upgrade options are limited by cost, or where a high level of security is not a priority. The trend, however, is to use contactless cards and to move forward with multifactor security systems in the face of continuously evolving threat levels and technologies. Table 3-4 summarizes the pros and cons/vulnerabilities.

Table 3-4. Pros and Cons of Magnetic Stripe Access Control Cards

Pros	Cons/Vulnerabilities
Widely used, low cost, reliable	Easily forged, copied/cloned, altered, and skimmed
Encoding at 75 bits per inch, which allows longer identifiers than many 26-bit formats (e.g. barcodes)	If you lose your card, anyone picking it up can use it at unmanned card reader access control points without an additional access control factor
End user may encode cards instead of purchasing pre-encoded cards	High fragility
Compatible with most ACS	Increasingly outdated technology & diminishing in popularity
Variety of reader forms available	
Can be added to cards with other technology embedded to increase interoperability	
Easily deactivated when required	
Capacity to store credential numbers, names, and related information	

3.4.2 Optical Memory Cards

Optical memory cards offer identification and other functions with high data capacity (4 MB), good reliability, fast transaction speed, and high standards compliance. Once data is written to a specific area of optical media, the written information cannot be changed. This means that memory is irreversible and permanently marked with information that identifies the cardholder, and if that information needs to be

changed, a new card must be issued. Memory is generally 1.1 MB (formatted) and typically uses a polycarbonate base-material cardstock. Table 3-5 summarizes the pros and cons/vulnerabilities of this ID type.

Table 3-5. Pros and Cons of Optical Memory Access Control Cards

Pros	Cons/Vulnerabilities
High capacity (4 MB) to store credential numbers, names, and related information	If you lose your card, anyone picking it up can use it at unmanned card reader access control points without an additional access control factor
Additional valid information can be written to the card	An attacker can add malicious information to the card
An attacker cannot delete or alter information once it has been written to the card	Legitimate information cannot be deleted or altered; any changes to existing information would require a new card
	Relatively difficult and expensive to print
	Costs of readers/writers

3.4.3 Wiegand Wire Cards

A Wiegand wire card is similar to a magnetic stripe card, but contains a series of embedded wires instead of a band of ferromagnetic material. The wires are made of a special alloy with magnetic properties, and are read by passing the card through or near a Wiegand sensor, which parses the wire pattern into a binary format. The cards and readers are low cost and durable. Table 3-6 summarizes the pros and cons/vulnerabilities of this ID type.

Table 3-6. Pros and Cons of Wiegand Wire Access Control Cards

Pros	Cons/Vulnerabilities
Credential numbers are fixed in the card at the time of manufacture	If you lose your card, anyone picking it up can use it at unmanned card reader access control points without an additional access control factor
Difficult to clone/copy and counterfeit	
Capacity to store credential numbers, names, and related information	

Wiegand wire cards are no longer widely used, but the Wiegand data format (especially 26-bit binary) and interface are still standard options in other types of access cards, card readers, and biometric devices.

3.4.4 Proximity and Vicinity Cards

Proximity and vicinity readers operate by constantly emitting a radio frequency (RF) field. When a card comes within range of this field, an integrated chip within the card is powered up and the chip transmits a card number back to the reader. The contactless card and reader market is moving toward the technology defined in ISO/IEC 14443 (proximity) and 15693 (vicinity), as evidenced in such major

credentialing programs as FIPS 201 personal identity verification (PIV) and ICAO 9303 machine-readable travel document (MRTD) for ePassports. See Section 3.7 for more information on FIPS 201.

The read range for vicinity cards is much longer than the read range for proximity card, which may have unintended consequences, such as doors opening as a cardholder walks by. Vicinity cards are not widely used for airport access control, with the exception of vehicle access. Because of the limited use of vicinity cards, the focus for this section will be on proximity cards, which are more widely used for airport access control. However, not all proximity cards are equal, and it is important that the differences are weighed before making a decision about which technology to adopt.

3.4.4.1 125 kHz Proximity Cards

The first of the proximity technologies was 125 kHz. This card transmits its data wirelessly to a wireless-enabled reader. Functionally, this is similar to the magnetic stripe readers, but now the card can be read at a limited distance, so contact is not required. 125 kHz proximity technologies used in radio-frequency identification (RFID) PACS are based on de facto industry standards (i.e., HID Global ISOProx) rather than international standards. 125 kHz technologies allow for a uniquely coded number to be transmitted and processed to an ACS. The ACS then determines the rights and privileges associated with that card.

The advantages of 125 kHz are its lower power consumption for the small amount of data being transmitted; read range up to 4 inches (10 cm); and a short read time, allowing users to present, swipe, or wave their card in the general proximity of the reader to get a successful read. For applications where greater read range may be desired, such as at vehicle entrance points, longer read range is relatively easy to achieve. Using a larger antenna and more power in the reader, 125 kHz proximity read range can easily reach 2–3 feet. Table 3-7 summarizes the pros and cons/vulnerabilities of this ID type.

Table 3-7. Pros and Cons of 125 kHz Proximity Access Control Cards

Pros	Cons/Vulnerabilities
Relatively low cost	Easily copied/cloned; susceptible to capture & replay
Convenient	If you lose your card, anyone picking it up can use it at unmanned card reader access control points without an additional access control factor
Easy to print	More expensive than contact cards
Capacity to store credential numbers, names, and related information	Requires firmware and software updates to protect against evolving threats
Rewriteable	
Read range up to 4 inches	
Short read time	

There are several different types of 125 kHz proximity card:

- **PVC cards:** thin plastic cards that are durable but flexible to withstand some wear and tear
- **Composite cards:** cards made from a blend of PVC and polyester that are the same thickness as PVC cards, but more durable and can withstand higher temperatures without warping. These cards can be used with reverse transfer ID card printers or laminating printers.
- **Clamshell cards:** cards made from two pieces of PVC card with the wireless RFID antenna placed in between. They are too thick to use with an ID card printer, so a print option is to print on thin adhesive-backed cards and apply to the clamshell cards.
- **Magnetic stripe proximity cards:** thin dual technology cards that can be used for multiple purposes, such as access control (proximity) and access to restricted parking areas (magnetic stripe). These cards have high coercivity magnetic stripes.

An approximate price range for these cards is under $1 per card. Price will vary by card manufacturer, the volume of cards purchased, card material, and features.

3.4.4.2 13.56 MHz Proximity Cards

13.56 MHz card technology was developed in an effort to lower the cost and increase functionality of proximity cards. These cards typically cost $2–$5 per card, but price will vary by card manufacturer, the volume of cards purchased, card material, and features. These are typically chip-enabled cards (see Section 3.6, below) that provide functions including encryption, integration with multi-identification factors such as biometric identifiers, and enhanced read range.

There is little visible difference between a 125 kHz card and a 13.56 MHz card. The user presents a card to a reader and access is either granted or denied; the user requires no operational knowledge. However, the back-end process for the 13.56 MHz card is considerably more complex. It should be noted that 125 kHz cards are faster and have a greater range than the 13.56 MHz cards, so users who are familiar with the 125 kHz cards will have to adjust to the slower features of the these cards.

The 13.56 Mhz standard was originally created as a ticketing solution for transport systems, and at the same time addressed the security issues in 125 kHz technology by enabling two-way communication between the card and reader. The key technology is a microcontroller chip embedded in the card, which provides much more storage capacity and enables stored data to be encrypted.

Well known examples of cards that use 13.56 MHz microcontroller technology include Mifare, DESFire, HID SEOS, and HID iClass. Table 3-8 summarizes the pros and cons of this ID type.

Table 3-8. Pros and Cons of 13.56 MHz Proximity Access Control Cards

Pros	Cons/Vulnerabilities
Convenient	Some Replay Resistance; vulnerable to known software settings
Rewriteable	More expensive than contact cards
Provides versatile interoperability	Requires firmware and software updates to protect against evolving threats
Available in 2k bit (256 byte), 16k bit (2K byte) or 32k bit (4K byte) memory configurations	

Pros	Cons/Vulnerabilities
Can be produced with visual security and anti-counterfeiting features such as holograms to quickly and easily identify genuine smart cards	
Stores credential numbers and biometrics	
Newer microcontroller chips include encryption and other means to secure the wireless transfer of data	

3.5 Biometrics

Biometrics can be added to an ACS for two-factor authentication. They can be used with both contact and contactless cards when the biometric is stored either in a database or on a chip integrated in an access control card. Biometric readers are available in formats to fit the biometric selected. Fingerprint, palm geometry, iris pattern, and facial recognition are popular formats. Figure 3-3 shows a fingerprint reader.

Figure 3-3. Access Control Reader with a Fingerprint Identifier

Source: IDEMIA Products, formerly MorphoAccess

This reader illustrates some of the features and capabilities that are available in the market, including:

- Tablet-like interface
- Media and messaging platform
- Video and audio IP intercom capability
- Anti-fraud: fake finger and duress finger
- Near Field Communication (NFC), iClass, Prox, MiFare, MiFare Plus, and DESFire
- IP65 weather resistant

Table 3-9 summarizes the pros and cons/vulnerabilities of this ID access control factor.

Table 3-9. Pros and Cons of Biometric Access Control Cards

Pros	Cons/Vulnerabilities
Provides another layer of security	The biometric is PII and must protected
A lost card cannot be used by an imposter to gain entry to a controlled area	Small populations of users may not have good biometric templates and may not be able to authenticate at the reader; thus a work-around (e.g. PIN) is needed for these users
Provides authentication instead of identification	Requires firmware and software updates
	Some biometrics are only contact (e.g., fingerprint, palm geometry)
	User might need a PIN to release the biometric if it is stored on a card
	There is no cryptographic protection of biometric between the card and the reader
	The transaction time to gain entry will increase
	Biometric reproductions can be made and may allow an unauthorized user access to a controlled area

3.6 Chip-Enabled Cards

With an embedded electronic chip, smart cards have the memory capacity to store large amounts of data plus the processing power to carry out functions such as data management, data encryption, and personal authentication. Smart cards can establish proof of trusted origin and confidentiality of stored and sent information, and can interact intelligently with a smart card reader and relying party system[2] such as a PACS or a Logical Access Control System established on an IT network.

For PACS, card holder record identifiers and card record identifiers are numbers that identify the appropriate card and user in the system. The card holder record of the relying party system provides authorizations (access privileges to locations). One or more authenticators, such as a PIN, biometric verification, or cryptographic protocol, may be required to allow the card holder to enter each specific area. An embedded integrated circuit chip can store very large identifiers; a common length is 128 bit.

The 128-bit Universally Unique Identifier (UUID) is sufficiently large that there is no need for a credential issuer to maintain a central registry. An identifier that may be generated without the need for a central registry of used values has the benefit of interoperability among all credential issuers using the same process regardless of issuing organization and geographic location.

Any PACS with the capability to process the large identifier will be able to register and allow use of such credentials.

[2] A **relying party** is "an entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system" (NIST SP 800-73-4).

Field tool kits exist that enable an issuer to revoke an issued credential from anywhere in the world, and easily prohibit the card holder from gaining access to any system where the credential is registered.

3.7 Federal Information Processing Standard (FIPS) 201 Technology

While PIV cards are not available to airports, many of their requirements have potential application in an airport PACS. FIPS 201 is an open system standard used for PIV and is designed to support any issuer and relying party. (An analogy is the use of EMV chips on credit cards; they work everywhere, no matter the issuer or merchant.) There is inherent use of Public Key Infrastructure (PKI) for this technology. In PKI, a Certification Authority algorithmically creates a key pair for (public and private) authenticating requests for access via a Registration Authority. Ideally, a PKI protects privacy, ensures electronic communication integrity, and verifies identities. This enables organizations to constrain who can use an issued card, and protects organizations from other issuers' cards.

NIST FIPS 140-2 defines the levels of hardware protection of cryptographic material within this framework.

FIPS 201 technology supports graduated levels of authentication, from least to most secure. This enables it to be tailored to the needs of the specific application. Appendix A describes the graduated levels of authentication within FIPS 201 compliant access control cards and federal programs that issue FIPS 201 technology cards.

> For more information on implementation of PIV-enabled PACS, see the Secure Technology Alliance's "A Quick Guide to Implementing Essential NIST SP 800-116 R1 Requirements."

An alternative to PIV is Commercial Identity Verification (CIV). CIV "leverages the PIV-I specifications, technology and data model without the requirement for cross-certification. Any enterprise can create, issue, and use CIV credentials according to requirements established within that enterprise's unique corporate environment" (Secure Technology Alliance, 2011). CIV is not widely used, likely due to the significant cost.

> For more information on CIV credentials, see the Smart Card Alliance's "The Commercial Identity Verification (CIV) Credential – Leveraging FIPS 201 and the PIV Specifications: Is the CIV Credential Right for You?"

3.8 Communications Protocols and Standards

The following sections summarize the communications protocols and associated standards for the various types of PACS cards and card technologies, and the relative pros and cons to be considered in selecting card solutions. There are essentially two types of communication protocol: Contact and Contactless.

Many card/credential types can support more than one type of communication protocol. For example, a PIV card is both contact and contactless. In addition, it is common when migrating legacy systems for a barcode (contact modality) to be available on a card with contactless capabilities.

3.8.1 Contact

Physical contact is required between the card/token and reader for communication to occur with contact cards. A broad range of features is available within the market, and newer versions of these cards and readers comply with ISO/IEC 7816, which defines standards for electronic identification cards (smart cards). However, many specific revisions of ISO/IEC 7816 exist and the user needs to confirm which year of the standard is required as the capabilities are additive.

The most common uses of contact technologies for security in the United States are the government PIV and TWIC programs.

Legacy contact communication technologies include:

- Barcodes scanned manually
- Magnetic stripe cards
- Wiegand wire technology
- OCR
- Optical Memory

It should be noted that secondary authentication factors, such as PINs entered manually, are independent of the communication protocol.

3.8.2 Contactless

Physical contact is not required between the card/credential and reader for communication to occur with contactless cards. Common forms of contactless communication protocols are discussed in the sections below.

Essentially, there two main types: proximity and vicinity. For each type, both proprietary and standards-based protocols exist. However, for this document, we will focus on proprietary proximity, standards-based proximity, and standards-based vicinity. Most of the proprietary technologies are now considered legacy. Alternatives to proximity and vicinity are also discussed below.

3.8.2.1 Proprietary Proximity

For this communication protocol, the card/credential must be in relatively close proximity to the reader for communication to occur. The read range is typically 5–7 cm.

Many of these cards in use in the United States are based on the legacy proprietary HID ISO Prox 125 MHz specifications. Outside the United States, there are alternative standards.

Pros of proprietary proximity include good read range, speed, lightweight protocol, availability of suppliers for cards and readers, and readers have a wide range of features, including prompting.

Cons of proprietary proximity include one-way communication, low data rates, little or no security, and easy duplication. In addition, the cards cannot hold more than a small amount of information.

These cards can be used with a PIN or even biometrics. However, the card cannot carry a biometric and would require central storage of the biometric.

3.8.2.2 Standards-Based Proximity

For this communication protocol, the card/credential must still be in relatively close proximity to the reader for communication to occur, but its range is slightly shorter range, at 3–5 cm.

Standards-based proximity also differs from proprietary in that its cards are based on ISO/IEC 14443, which operates at 13.56 MHz.

Pros of this technology include connection speed and having many suppliers for cards and readers. Typically, these cards are equipped with a built-in chip, which allows the local storage of large amounts of data that could be used for biometrics or alternative security. Additionally, readers have a wide range of features, including optional security features, and the low read range minimizes sniffing.

One con is that many of the cards and readers comply with ISO/IEC 7816, which defines standards for electronic identification cards, so the user will need to confirm which specific revision year of the standard is required, as the capabilities are additive. Also, features vary with manufacturer card types, and these features may increase card and reader costs and require specific card readers.

Current deployments for standards-based proximity communication based on ISO 14443 include PIV, TWIC, and commercially available branded cards, such as Mifare, DESFire, HID SEOS, and HID iClass.

3.8.2.3 Standards-Based Vicinity

While proximity cards require the card/credential to be relatively close to the reader for communication to occur, vicinity communication allows for a greater distance between the card/credential and the reader. This communication protocol is based on ISO/IEC 15693, which defines standards for electronic identification cards.

Pros of this technology include connection speed. Additionally, readers have a wide range of features, including optional security features.

Cons include that many specific revisions of ISO/IEC 15693 exist, and the user needs to confirm which year of the standard is required as the capabilities are additive. Additionally, in the United States there are limited suppliers for the readers, and the 70-cm read range has unintended consequences such as doors opening as a cardholder walks by.

This communication protocol is not widely used for airport access control, with the exception of vehicle access.

3.8.2.4 Proprietary Ultra-High Frequency (UHF)

UHF radio transmissions include the band from 300 to 3000 MHz (1 m – 10 cm). Proprietary UHF modalities include all UHF wireless cards. This modality is primarily used for inventory control in warehouses and supply chain applications.

The pros of this modality are that 900 MHz reads through walls and obstructions, and has a longer effective range.

The cons are that proprietary UHF can be read at 30 m, which introduces a significant risk of opening the wrong access control door, has very limited capabilities on chips, and there are no cryptographic security mechanisms.

This technology has limited deployment in airport access control.

3.8.2.5 Near Field Communications (NFC)

NFC is widely used on smartphones for commercial applications, such as ApplePay, and also at airport boarding gates to show boarding passes in electronic form. While NFC is a communications protocol and not an access control mode per se, it is of increasing interest because smartphones could be allowed for access control in the future. Potential NFC modalities include all wireless card readers that use NFC.

Pros of NFC include the ability to enable mobile smartphones to act as smart card devices for PACS. Several ACS manufacturers are offering such solutions, but there are security challenges to overcome, and the solutions have not been adopted as expected.

Cons include the ability of a pair of smartphones to be used in a relay setup to attack a system and the inherent capability to modify the behavior of a smart phone far more easily than a chip on a smart card. Because of this, caution is advised.

This technology has limited deployment in airport access control.

SECTION 4: ACCESS CONTROL CARD AND SYSTEM CONSIDERATIONS

The following sections describe topics for consideration as access control cards and systems are upgraded.

4.1 Installation Considerations

While few installation issues are specific to the access medium itself, several card-related issues can arise when a new technology is installed (particularly one with biometric features). Topics to consider include:

- Re-enrollment of the entire user population, including all internal and external stakeholders
- Training of all users on the daily use, care, and maintenance of the card and the reader
- Training of system operators on the added software capabilities of a more robust technology, including media audits and report generation
- Tracking of all maintenance and error reports to determine the nature of any recurring issues (such as faulty or hidden design or installation problems, media failure, false accept/false reject patterns, forensic searches, or misuse by employees)
- Identification of users whose biometric may exhibit characteristics that are difficult to recognize (such as certain gender, ethnic, or physical attributes or anomalies that may require an alternate biometric or other accommodation)
- Identification of design and installation issues at locations where improper lighting, camera angles, or reflections at different times of day may affect the visual biometrics (such as iris scan or facial recognition)
- Failure of third-party interfaces

4.2 Printing Capabilities

Card printing is dependent upon the material from which it is made. PVC and polymers are the materials most used for access cards. They are inexpensive and widely available in standard sizes, and there are many inexpensive printers for this card material. PVC, however, does not exhibit tolerance for typical abuse, such as being placed in a wallet or used as an ice scraper. These situations often crack the card and render it unusable.

Generally, cards are a mixture of layers including PVC, polyethylene terephthalate film (PETF) and polyethylene terephthalate (PET) polymers to achieve best results under ISO/IEC 7810 tests for resistance to bending, flame, chemicals, temperature, and humidity. These polymer cards are more durable, but also more expensive, but they are better suited for high wear applications, and environmentally demanding situations (e.g., marine environment with salt in the air). They also hold up better when placed in a wallet.

Polycarbonate is extremely durable. Many new state driver's licenses are now polycarbonate, which ensures 10 years of use. It also brings additional costs, specifically around printing and general manufacturing issues.

ABS is rarely used in access control card technologies. ABS is used as an abbreviation for two different plastics. One is Acrylonitrile Butadiene Styrene wherein the Acrylonitrile crosslinks the Styrene for

toughness and the Butadiene supplies a rubber-like consistency. There are a variety of grades with different proportions of ingredients and additives for different properties.

Table 4-1 shows a breakdown of the most common card materials and substrates. Most access control cards are multi-layer laminates; each has different physical and operational characteristics.

Table 4-1. Common Card Materials and Substrates

	PVC	ABS	Polycarbonate	PETF	PET
Temperature Stability	80° C Max	100° C Max	168° C Max	200° C Max	75° C Max
Mechanical Characteristics	Ages vary quickly	Mechanically strong	High stability	Very high stability	Becomes brittle quickly
Typical Applications	Access control, bank cards, SIMS	SIMS	Identity cards	Identity cards, bank cards, transit fare cards	Identity cards, transit fare cards
Printability	Easy to print locally	Easy to print locally; supports high print quality and direct and reverse-transfer printing	Specialized printing techniques; laser engraving	Offset printing on laminated sheets	Offset printing on laminated sheets
Counterfeit Resistance	Easy to copy, clone, and alter	Delaminate to alter	Most resistant to copy, clone, and alter	Will not delaminate; high resistance to copy, clone, and alter	Delaminate to alter
Relative Unit Cost	Lowest in short term, until replacement needed	Low	High but long lasting in most situations	Moderate	Moderate

Card manufacturer warranties should be examined in detail when determining card requirements.

4.3 Avoiding Card Selection Pitfalls

The card selection process involves a thorough assessment and evaluation of system-wide PACS issues over a significant period, requiring a significant amount of information gathering before a fully informed decision can be made. Poor planning in this regard poses the risk of leading to a security system that fails to work properly and potentially allows breaches or failures. However, detailed pre-planning with all stakeholders before the technology selections are made, along with a willingness to review and revise those decisions when necessary, is more likely to lead to a successful outcome.

Questions to be addressed to improve project planning and to avoid surprises in selection and installation include:

- **Who?** Identify stakeholders, along with their interests and involvement.
- **Why?** Organize the elements of "who" into an effective planning team to define operational requirements. What are the goals and objectives (not technical specifications)? Is this a need or a wish-list item?
- **What?** Identify the functionalities needed to meet user requirements.
- **When?** Is this a critical time-sensitive decision or can it be absorbed into other shared capital projects?
- **Where?** Are these cards to be used airport-wide or in specific locations such as new and/or external facilities?

After those questions are answered, next steps include:

- Identify all necessary resources including manpower, expertise, information sources (DHS, TSA, and Safe Skies FAST), support equipment, and supplies
- Build a comprehensive team of people with suitable skills and knowledge, including operational personnel
- Conduct an assessment of existing legacy systems and third-party integration requirements
- Identify all direct and ancillary costs and capital expenses (including planning, design, implementation, and maintenance costs)
- Conduct a risk assessment including all realistic threats, vulnerabilities, and consequences
- Develop strategies and specific actions to minimize risks of selected card technologies

Project management procedures should be in place that maintain the technical integrity of card specifications from the time they are developed through technology selection, procurement, and installation. These procedures should call for proof testing of even small changes in card features, characteristics, and formats with actual PACS hardware, and under conditions as that are close as possible to actual airport operating conditions, before a card is committed to production. Factory testing before cards are shipped in actual PACS equipment shipment, when feasible, can assure that the installation process will proceed with a high level of confidence.

While proper planning will hopefully mitigate most issues, smaller issues could be easily overlooked and result in major problems. Some examples of specific lessons learned by airports through selection and implementation of new card technology include:

- Cards are often issued with card holders, clasps (for affixing a card to clothing), lanyards (for wearing a card around the neck), or transparent pocket armbands (for display outside clothing). These accessories should be considered in specifying and selecting access cards.
- If access control cards are to be attached to lanyards or straps, which may require punched holes or thru-card fasteners, first confirm that the card can be safely punched at all. If so, verify that the area to be punched/bored does not impact the card's interior electronic circuits (i.e., the contactless antenna). Also ensure that contact badge (e.g., mag stripe) holders allow the badge to be used without removing it from its holder.
- Because 125 kHz proximity cards can be cloned, it is recommended these access control cards be kept in an RFID-blocking sleeve. This can be an inconvenience for the user to remove the card from the sleeve to gain access, but the sleeve reduces the threat of the card being cloned.

- With higher frequency proximity cards, a dielectric plate may need to be placed on the back of the reader because of the shorter read range and presence of metal near the reader.
- Airline or other tenant corporate cards could interfere with airport-issued cards. Such cards may have to be kept separate or taken out of the badge holder when an airport-issued card is presented to a reader.

4.4 Credentials and Assurance Considerations

Airports should expect increased focus on IT security. While NIST Special Publications are not mandatory for commercial US airports, they do embody best practices for securing federal facilities, and merit emulation by airports. A good place to start for establishing information security requirements is NIST SP 800-63 Digital Identity Guidelines, which defines levels of security assurance for various credential and token implementations. This is valuable guidance for specifying PACS security provisions, including ACS hardware (reader specifications) and card technology selection.

This framework allows an identity provider to indicate to a service provider how much trust is behind each authentication event. Service providers, based on their own needs and assessment of risks, determine what level of assurance they require in an authentication event in order to allow the user access. Assurance is separated into two concepts:

- The strength of the processes used to identify the user at the time of user registration (i.e., the concept of identity assurance). In the context of this guidance document, this refers to the assurance that the person enrolled in the PACS is the person whose enrollment is authorized.
- The strength of the authentication method(s) used in each authentication instance (i.e., the concept of authentication assurance). In the context of this guidance document, this information helps the airport determine the number and type of authentication factors preferred or required for their PACS.

There are three levels of identity assurance in this framework, expressed as a value from 1 to 3. Likewise, there are three levels of authentication assurance, expressed as a value from 1 to 3. The relying party—the airport operator, if it is the service provider—determines what levels are required to allow access to their service. The levels of each type of assurance selected or preferred do not have to correspond. For instance, an airport may choose to comply with level 3 in identity assurance, yet feel level 2 is sufficient in authentication assurance.

> See the full NIST SP 800-63 Digital Identity Guidelines, comprising four documents, at: https://pages.nist.gov/800-63-3/.

SECTION 5: FUTURE TRENDS

5.1 Technology Trends

A dominant trend in airport access control is the expectation that the use of biometrics will become mandatory rather than voluntary.

Industry experts suggest that although biometric upgrades will occur, the most practical approach would be to implement them during the next scheduled upgrades at each airport in its regular system life cycle. All US commercial airports already have a regulatory-compliant system in place; some are very new, while others are now reaching the end of their operational life cycles, which is often more than 7–8 years, and is often reflective of progressively more advanced technology. The planners/designers of new facilities will need to maintain a level of flexibility and expandability to account for still-unanticipated new technologies and/or regulatory requirements in the next series of life cycles for all security-related systems, including IT, fiber distribution, terminal expansion, and future outlying facilities, including multiple regional airports.

Fingerprint technologies are widely available, though alternate biometric technologies such as iris scan, facial recognition, hand geometry, and voice recognition have considerably improved and are also in place, but can be less convenient in the high-intensity airport operational environment. Nonetheless, they may be appropriate for certain limited applications such as cash operations, high-value storage, critical infrastructure locations, or certain types of tenant facilities, some of which may justify two-factor authentication. Airlines have begun the use of biometrics to validate certain categories of passengers; for example, using facial recognition for boarding passes, or touchless fingerprint for high-speed verification.

Technologies such as biometrics, and many IT technologies, pose challenges to the protection of a person's private information. There are legitimate concerns about the possible misuse of biometric data. ACS using biometrics will increasingly be required to have policies regarding how biometric data will be collected, stored, accessed, and used, and limit the distribution of biometric data for any reason beyond the stated purposes. Appropriate managerial and technical controls, such as data encryption, will be required to protect the integrity of biometric data whenever it is transported over a network.

Multifactor authentication is increasingly common in PACS deployments to provide higher levels of assurance of the identity of the person seeking access to a secure area. A card reader with a keypad is a common tool used in areas where policies require two-factor authentication for physical access requests.

Smartphones are now ubiquitous among passengers and airport personnel for both professional and personal use. They are already being used by passengers for boarding gate access at airports worldwide. Properly configured and secured, it is possible for smartphones to take the place of electronically enabled ACS cards at airports when a visible means of identification, such as a printed card, is provided for SIDA requirements.

There is an IT industry trend to move away from passwords because of their inherent weaknesses and the growing attention to their particular vulnerabilities to hacking and cyber-attacks recurring worldwide. Google, Microsoft, Amazon, Visa, Samsung, Aetna, and other technology leaders have formed The Fast ID Online (FIDO) Alliance, an open industry association focused on developing authentication standards to help reduce the world's reliance on passwords. The FIDO Alliance currently has published three sets of specifications for simpler, stronger authentication: FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF), and FIDO2, which

includes the W3C's Web Authentication (WebAuthn) specification and FIDO Client to Authenticator Protocol (CTAP).

> FIDO Alliance activities can be followed at: https://fidoalliance.org/

Complementing the FIDO Alliance, whose members are not airport specific, are efforts by the International Air Transport Association (IATA) to accelerating implementation of its One ID biometric identity initiative. IATA represents the air carriers, for whom expeditious passenger processing is a high priority. One ID seeks to use fingerprint, iris, or facial recognition technology to reduce the need for repetitive identity checks at airports and create a seamless, end-to-end passenger process.

> More information on One ID is available on the IATA website:
> https://www.iata.org/whatwedo/passenger/Pages/one-id.aspx

Smartphones are becoming increasingly enabled for security applications. Many airlines now accept electronic boarding passes at the gate, but TSA still requires government-issued photo IDs at the screening checkpoints. Over time, there will likely be efforts to enable smartphones to replace physical photo ID media and to serve as access control media, and possibly eliminate the need for access control cards for persons having trusted smartphones.

5.2 TSA Cybersecurity Roadmap 2018

Rapidly growing concerns regarding advances in technology have brought significantly greater government and industry attention to both physical security and its extensive reliance on cybersecurity. In late 2018, TSA issued its Cybersecurity Roadmap to assist industry in broadening its cybersecurity efforts in the transportation sector (specifically aviation and airports) by implementing what it refers to as a four-pillar strategy. This is not a regulatory or mandated approach, but is presented as a collaborative approach to apply the Cybersecurity Strategy to transportation modes and customize them for outcome-specific threat reductions.

> **TSA Roadmap:**
> https://www.tsa.gov/sites/default/files/documents/tsa_cybersecurity_roadmap_adm_approved.pdf.

Airport operators should seek to understand this overall Cybersecurity Strategy in the longer term. The core, initially, is the TSA Pillar I for Risk Identification. As the TSA strategy crosses all elements of the Transportation Systems Sector for aviation, this document addresses its impacts on airports.

The TSA website maintains links of TSA public statements and congressional testimony on identified security concerns and events.

> **TSA Public Statements:** https://www.tsa.gov/news/press/testimony
> **TSA Congressional Testimony:** https://www.tsa.gov/news/speeches.

REFERENCES

Martin, Zack. “PIV-I, CIV circling the drain.” *SecureIDNews*, March 9, 2015, accessed September 10, 2019, https://www.secureidnews.com/news-item/piv-i-civ-circling-the-drain/2/

Miller, Mark. “Wiegand for Dummies.” *Telaeris*, November 10, 2014, accessed September 20, 2019. https://telaeris.com/blog/wiegand-for-dummies/

Norman, Thomas L. Electronic Access Control, 2nd ed. Oxford: Butterworth-Heinnemann, 2017

ProxSource. “Types of Access Control Cards.” Accessed August 8, 2019, http://www.proxsource.com/resources/types-of-access-control-cards/

Secure Technology Alliance. “The Commercial Identity Verification (CIV) Credential—Leveraging FIPS 201 and the PIV Specifications.” Last modified October 2011, accessed September 10, 2019, https://www.securetechalliance.org/publications-the-commercial-identity-verification-civ-credential-leveraging-fips-201-and-the-piv-specifications/

Smith, David. “Definition: Wiegand.” Last updated August 2007, accessed July 1, 2019. https://whatis.techtarget.com/definition/Wiegand

Techopedia. “Magnetic Stripe.” Accessed October 8, 2019, https://www.techopedia.com/definition/20581/magnetic-stripe

ADDITIONAL RESOURCES

[FIPS140] FIPS Publication 140-2, Security Requirements for Cryptographic Modules, NIST.

[ISO10373] ISO/IEC 10373, Identification Cards—Test Methods. Part 1—Standard for General Characteristic Test of Identification Cards, ISO, 1998. Part 3—Standard for Integrated Circuit Cards with Contacts and Related Interface Devices, ISO, 2001. Part 6—Standard for Proximity Card Support in Identification Cards, ISO, 2001.

[ISO14443] ISO/IEC 14443-1:2000, Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards, ISO, 2000.

[ISO7810] ISO/IEC 7810:2003, Identification Cards—Physical Characteristics, ISO, 2003.

[ISO7811] ISO/IEC 7811, Identification cards – Recording technique. Part 6—Magnetic stripe -- High coercivity, ISO, 2008. Part 7—Magnetic stripe – High coercivity, high density, ISO, 2004.

[ISO24727] ISO/IEC 24727, Identification cards – Integrated circuit card programming interfaces. Part 2—Generic card interface, ISO, 2008. Procedures for the authentication protocols for interoperability, ISO, 2010.

[SP 800-63] NIST Special Publications 800-63-3, Digital Identity Guidelines; SP 800-63A, Enrollment and Identity Proofing; SP 800-63B, Authentication and Lifecycle Management; and SP 800-63C, Federation and Assertions; NIST, June 2017 or as amended.

[SP 800-73] NIST Special Publication 800-73-3, Interfaces for Personal Identity Verification, NIST, February 2010 or as amended.

[SP 800-76] NIST Special Publication 800-76-2, Biometric Specifications for Personal Identity Verification, NIST, July 2013 or as amended.

[SP 800-78] NIST Special Publication 800-78-3, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST, December 2010 or as amended.

[SP 800-79] NIST Special Publication 800-79-1, Guidelines for the Accreditation of Personal Identity Verification Card Issuers, NIST, June 2008 or as amended.

[SP 800-116] NIST Special Publication 800-116, A Recommendation for the use of PIV Credentials in Physical Access Control Systems (PACS), NIST, November 2008 or as amended.