
A SMART CARD ALLIANCE ACCESS CONTROL COUNCIL RESOURCE

# Access Control Reader and Credential Architecture and Engineering Specification for Non-Government Facilities: Contactless Smart Card 13.56 MHz High Frequency Technology

Version Number: 1.1
Publication Date: April 2015
Publication Number: ACC-15001

**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.

# *Access Control Reader and Credential A & E Specification: Annotated Version*

## *[Insert Project Name]*

***Specification for Architects, Consultants, and Engineers***

***Access Control A&E Specification ___[insert date]___***

# Contactless Smart Card 13.56 MHz High Frequency Technology [Sample] A & E Guide Specification for Architects, Consultants, and Specifying Engineers

This document contains sample guide specifications for 13.56 MHz contactless smart card technology products. The document is written using industry standard formatting and language (e.g., Construction Specification Institute (CSI) Division 28 – Electronic Safety and Security Section 28 13 Electronic Security System), and is designed for use by architects, consultants, and specifying engineers who are preparing bid specifications for physical access control, building control, and security systems for non-government facilities.

The Microsoft Word version of these specifications may be copied into the appropriate sections of a complete bid specification by using the "cut and paste" method. This document is designed to be used as a "whole specification;" where choices should be made and where project-specific information should be inserted are indicated in the specification in [brackets].

[Note that this document is the "annotated version." As an educational resource for the specifier, the annotated specification includes links to commentary that describes or defines terminology and content included in the specification; these links are shown as an underlined number in brackets (e.g., [1]). When using the document in a specification, the unannotated Microsoft Word version should be used.]

These specifications do not guarantee performance. Performance is the result of many factors, including, but not limited to, how the system is deployed, what environment it is being deployed into, and how it is used.

This document is specific to the requirements for use of modern secure smart card technology in physical access control system (PACS) applications in non-government facilities. It focuses on the card-to-reader operations and is intended to work with a wide variety of commercial PACS. The specification assumes the card data model is designed in accordance with the specific PACS being implemented. Successful security deployments are a shared responsibility by all involved in the solution supply chain. Proper installations not only involve the specification but also include the responsibilities of the manufacturer, integrator and end user to deploy, operate and maintain the solution. These responsibilities should be clearly defined in the project documentation and associated processes and procedures.

Products covered are focused on PACS applications and include reference to commercially available products. Access control credentials and accessories are also included. This specification does not endorse any specific product or service. Product or service references are provided as examples.

Note that this specification was developed to be used for commercial, non-government PACS implementations. The specification does not apply to and should not be used for federal facilities.

This specification is maintained by the Smart Card Alliance Access Control Council. As with any specification, the Smart Card Alliance anticipates that there may be questions and interpretations that arise when using this specification. Please send all correspondence to ACCA&E@smartcardalliance.org.

These "Section 16720 Smart Card Access Control System" specifications (the "Form Specifications") are general in nature and solely for illustration. The Form Specifications are not intended for any specific application or use and project specific considerations must be taken into account in the architect's or engineer's preparation of actual system specifications. The Smart Card Alliance makes no representation or warranty with respect to these Form Specifications and nothing contained herein shall create, or be inferred to create, any express or implied warranty by the Smart Card Alliance. These Form Specifications are intended solely for the purpose of reflecting general guidelines for smart card physical access control system specifications. The architect or engineer preparing the actual smart card specifications should therefore refer to and confirm actual manufacturer's specifications. The Smart Card Alliance assumes no liability with respect to, arising from, or arising out of the Form Specifications or any use thereof.

# *1 Alarm and Access Control Equipment [1] [2]*

**A. Contactless Access Control Smart Card Reader [3]:** Provide contactless smart card reader or equivalent where shown on the drawings. Smart card readers shall be "single-package" type, combining the reader, electronics and antenna in one package [4], in the following configurations:

**1. Smart Card Reader Security**

a. Reader shall implement features to protect security keys if the keys are stored in the reader. [33]

b. Reader needs to be compatible with the security features of the access credential and controller.

c. The reader shall have features that sense and report tampering. [20]

d. The power and data connections from the reader to the physical access control system (PACS) should be tamper-protected and supervised.

**2. Smart Card Reader, Mullion Mounting (Optional Single-Gang Mounting Kit)**

a. Provide mullion or “single-gang” mounting style contactless smart card readers for door frame mounting, non-metal wall mounting, non-metal vehicle stanchions and non-metal pedestals, and where shown on plans. To prevent adverse effects on read-range and reader performance, if the reader is mounted on metal, appropriate precautions (such as insulating spacers) should be considered to ensure acceptable performance. (Consult manufacturer’s recommendations.)

b. The reader optional single-gang mounting kit shall be designed for USA, European and Asian electrical back boxes having a mounting hole spacing of 52-60mm.

c. The reader material shall conform to the current version of UL 94 for flame resistance and UL 508 for UV resistance suitable for indoor or outdoor usage and be sealed to an IP rating of [insert rating] [5].

d. The reader shall conform to the current version of UL/C 294, and shall be FCC and CE certified.

e. The reader shall operate in the 13.56 MHz high frequency band and shall conform to the current version of the following ISO/IEC Standards [select one or more]: [6] [7] [8]

1) ISO/IEC 14443 parts 1 thru 3 A/B (read/write)

2) ISO/IEC 14443 parts 1 thru 4 A/B (read/write)

3) ISO/IEC 15693 (read/write)

f. The reader shall comply fully with ISO/IEC 14443 parts 1, 2, 3, and 4 and/or ISO/IEC 15693 parts 1 thru 3 open card standards to fully enable interoperability among suppliers of similar products.

g. The reader shall have an approximate read range of no more than 100 mm when used with an access control credential conforming with ISO/IEC 14443 Part 1 Class 1 [9] and approximate read range of 1 m when used with ISO/IEC 15693 access control cards.

h. The reader shall require that a card, once read, must be removed from the RF field before it will be read again, to prevent multiple reads from a single card presentation and anti-passback errors. [10]

i. The reader shall be capable of reading access control data from any ISO/IEC 14443 part 3 and/or part 4 compliant contactless card or other form factor, and transmitting the data in Wiegand, serial (RS-232, RS-485) or other format to the PACS. [11] [12]

j. The reader shall be capable of reading access control data from any ISO/IEC 15693 card or other form factor, and transmitting the data in Wiegand, serial (RS-232, RS-485) or other format to the PACS. [11] [12]

k. The reader shall be capable of writing to any ISO/IEC 14443 part 4 compliant smart card or other form factor as required by the application.

l. The reader shall provide functionality for the following communication ports [11]:
   1) Wiegand port, for connection to standard access control panels [OR]
   2) RS232, RS422, or RS485 port, for connection to PCs or access control systems, either individually or on a multi-drop bus [OR]
   3) ISO/IEC 7811 Clock & Data ABA track 2 emulation port, for connection to standard control panels requiring magnetic stripe interface [13] [OR]
   4) Internet Protocol (IP) (e.g, TCP or UDP) [OR]
   5) Secure wireless

m. The reader shall have visual indication to show, at a minimum, whether power is on, whether the card is being read, and whether access is granted/denied [14].
   1) Visual displays shall be low power, be visible in the ambient environment, and be able to meet Americans with Disabilities Act (ADA) requirements.

n. The reader shall have an audible indicator, such as an audio transducer capable of producing tone sequences for various status conditions (at a minimum, to indicate whether access is granted/denied). [15]

o. Reader shall support modern cryptographic standards for secure communications between the card and the reader. [17] [18] [19]

p. The reader shall have features that sense and report tampering. [20]

q. The reader shall have the ability for its firmware and keys to be updated in the field in a secure fashion. [21]

r. The reader shall be warranted in compliance with the warranty statement provided in the specification.

s. Color shall be [insert color; e.g., black, silver].

t. [Insert specific brand and model if desired] product series, or equivalent, compatible with selected cards or other form factors.

**3. Keypad Smart Card Reader, Mullion Mounting (Optional Single-Gang Mounting Kit)**

a. Provide mullion or "single-gang" mounting style contactless readers for door frame mounting, non-metal wall mounting, non-metal vehicle stanchions and non-metal pedestals, and where shown on project plans. To prevent adverse effects on read-range and reader performance, if the reader is mounted on metal, appropriate precautions (such as insulating spacers) should be considered to ensure acceptable performance. (Consult manufacturer's recommendations.)

b. The reader single-gang mounting kit shall be designed for USA, European and Asian electrical back boxes having a mounting hole spacing of 52-60mm.

c. The reader shall be constructed high quality flame resistant and UV resistant material suitable for indoor or outdoor usage and be sealed to an IP rating of [insert rating]. [5]

d. The reader shall conform to the current version of UL/C 294, and shall be FCC and CE certified.

e. The reader shall operate in the 13.56 MHz high frequency band and shall conform to the current version of the following ISO/IEC Standards [select one or more]: [6] [7] [8]

1) ISO/IEC 14443 parts 1 thru 3 A/B (read/write)

2) ISO/IEC 14443 parts 1 thru 4 A/B (read/write)

3) ISO/IEC 15693 (read/write)

f. The reader shall comply fully with ISO/IEC 14443 parts 1, 2, 3, and 4 and/or ISO/IEC 15693 parts 1 thru 3 open card standards to fully enable interoperability among suppliers of similar products.

g. The reader shall have an approximate read range of no more than 100 mm when used with an access control credential conforming with ISO/IEC 14443 Part 1 Class 1 [9] and approximate read range of 1 m when used with ISO/IEC 15693 access control cards.

h. The reader shall require that a card, once read, must be removed from the RF field before it will be read again, to prevent multiple reads from a single card presentation and anti-passback errors. [10]

i. The reader shall be capable of reading access control data from any ISO/IEC 14443 part 3 and/or part 4 compliant contactless smart card or other form factor, and transmitting the data in Wiegand, serial (RS-232, RS-485) or other format to the PACS. [11] [12]

j. The reader shall be capable of reading access control data from any ISO/IEC 15693 card or other form factor, and transmitting that data in Wiegand, serial (RS-232, RS-485) or other format to the PACS. [11] [12]

k. The reader shall be capable of writing to any ISO/IEC 14443 part 4 compliant smart card or other form factor as required by the application. [34]

l. The reader shall provide functionality for the following communication ports [11]:
   1) Wiegand port, for connection to standard access control panels [OR]
   2) RS232, RS422, or RS485 port, for connection to PCs or access control systems, either individually or on a multi-drop bus [OR]
   3) ISO/IEC 7811 Clock & Data ABA track 2 emulation port, for connection to standard control panels requiring magnetic stripe interface [13] [OR]
   4) Internet Protocol (IP) (e.g, TCP or UDP) [OR]
   5) Secure wireless

m. The reader shall have visual indication to show, at a minimum, whether power is on, whether the card is being read, and whether access is granted/denied [14].
   1) Visual displays shall be low power, be visible in the ambient environment and be able to meet Americans with Disabilities Act (ADA) requirements.

n. The reader shall have an audible indicator, such as an audio transducer capable of producing tone sequences for various status conditions (at a minimum, to indicate whether access is granted/denied). [15]

o. Reader shall support modern cryptographic standards for secure communications between the card and the reader. [17] [18] [19]

p. The reader shall have features that sense and report tampering. [20]

q. The reader shall have a keypad which outputs keyed-in data in a format compatible with the PACS. [22] [23]

r. The reader shall have the ability for its firmware and keys to be updated in the field in a secure fashion. [21]

s. The reader shall be warranted in compliance with the warranty statement provided in the specification.

t. Color shall be [insert color; e.g., black, silver].

u. [Insert specific brand and model if desired] product series, or equivalent, compatible with selected cards or other form factors.

[SELECT B, C or D for the ACCESS CREDENTIAL section. [7]]

**B. ACCESS CREDENTIALS – (Cards Supporting Standard ISO/IEC 14443 through Part 3) [7] [28]**

Provide [specify quantity] ISO/IEC 14443 compliant contactless credentials with the following features or form factors:

**1. Credential Security Features [16]**

a. Access credential shall have a cryptographically-sound mutual authentication mechanism based on an open, recognized and public symmetric cryptographic algorithm (three-key TDES or AES) or asymmetric cryptographic algorithm (RSA or ECC). [29]

b. In the case of a symmetric key credential, it shall be diversified using a method that is non-reversible and incorporates a unique, reliable identifier (for example, the non-alterable chip individual serial number). [30]

c. In the case that secure messaging is required between the card and reader, a secure messaging method shall be utilized to provide confidentiality of the data communications between the reader and the credential using an open, recognized and public symmetric cryptographic algorithm (three-key TDES or AES) or asymmetric cryptographic algorithm (RSA or ECC). This messaging method shall be designed to prevent simple cryptographic attacks like man-in-the-middle and replay attacks. [31]

v. Message authentication, such as cryptographic message authentication code (CMAC), shall be used to protect the integrity of the data transmitted from the card. [32]

2. **Access Card [24]**

   a. Access cards shall be used with ISO/IEC 14443 access readers to gain entry to access controlled portals (e.g., doors, gates, turnstiles) and to hold information specific to the user.

   b. The card shall operate in the 13.56 MHz high frequency band only.

   c. The card shall comply fully with the current version of ISO/IEC 14443 part 1 class 1, part 2, and part 3A or 3B, open card standards to enable interoperability among suppliers of products using the same chip sets and must be compatible with the specified access control reader.

   d. The card shall conform fully to the current version of ISO/IEC 14443 Part 3 – Initialization and Anti-collision Protocol and must be capable of identifying multiple credentials in a single field and selecting one credential to work with.

   e. The card shall meet the current version of ISO/IEC 7810 card specifications for length, width, thickness, flatness, card construction and durability, and shall be in a form suitable for direct two-sided dye-sublimation or thermal transfer printing on the specified card printer.

   f. Presentation of the card to the access control reader in accordance with ISO/IEC 14443 shall result in an accurate reading of the card. [24]

   g. The card shall be warranted in compliance with the warranty statement provided in the specification. [25]

   h. Provide [specify quantity] ISO/IEC 14443 compliant access control cards, compatible with the specified readers.

   i. The card must be capable of being worn and displayed by personnel. Contactless smart cards should not be slot-punched; a sleeve or other form of carrier should be used. [26]

   j. The card shall be available with or without a magnetic stripe, with security taken into consideration. [27]

3. **Access Key Fob**

   a. Access fobs shall be used with ISO/IEC 14443 access readers to gain entry to access controlled portals (e.g., doors, gates, turnstiles) and to hold information specific to the user.

   b. The fob shall operate in the 13.56 MHz high frequency band only.

c. The fob shall comply fully with the current version of ISO/IEC 14443 part 1 class 1, part 2, and part 3A or 3B, open card standards to enable interoperability among suppliers of products using the same chip sets and must be compatible with the specified access control reader.

d. The fob shall conform fully to the current version of ISO/IEC 14443 Part 3 – Initialization and Anti-collision Protocol and must be capable of identifying multiple credentials in a single field and selecting one credential to work with.

e. The key fob shall be constructed of durable material, and shall be suitable for placement on a key ring.

f. Presentation of the fob to the access control reader in accordance with ISO/IEC 14443 shall result in an accurate reading of the fob. [24]

g. Provide [specify quantity] ISO/IEC 14443-compliant key fobs compatible with the specified readers.

h. The key fob shall be warranted in compliance with the warranty statement provided in the specification. [25]

C. **ACCESS CREDENTIALS – (Cards Supporting Standard ISO/IEC 14443 through Part 4) [7] [28]**

Provide [specify quantity] ISO/IEC 14443 compliant contactless credentials with the following features or form factors:

**1. Credential Security Features [16]**

a. Access credential shall have a cryptographically-sound mutual authentication mechanism based on an open, recognized and public symmetric cryptographic algorithm (three-key TDES or AES) or asymmetric cryptographic algorithm (RSA or ECC). [29]

b. In the case of a symmetric key credential, it shall be diversified using a method that is non-reversible and incorporates a unique, reliable identifier (for example, the non-alterable chip individual serial number). [30]

c. In the case that secure messaging is required between the card and reader, a secure messaging method shall be utilized to provide confidentiality of the data communications between the reader and the credential using an open, recognized and public symmetric cryptographic algorithm (three-key TDES or AES) or asymmetric cryptographic algorithm (RSA or ECC). This messaging method shall be designed to prevent simple cryptographic attacks like man-in-the-middle and replay attacks. [31]

d. Message authentication, such as cryptographic message authentication code (CMAC), shall be used to protect the integrity of the data transmitted from the card. [32]

**2. Access Card [24]**

a. Access card shall be used with ISO/IEC 14443 access readers to gain entry to access controlled portals (e.g., doors, gates, turnstiles) and to hold information specific to the user.

b. The card shall operate in the 13.56 MHz high frequency band only.

c. The card shall comply fully with the current version of ISO/IEC 14443 parts 1, 2, 3, and 4 open card standards to enable interoperability among suppliers of products using the same chip sets and must be compatible with the specified access control reader.

d. The card shall conform fully to the current version of ISO/IEC 14443 Part 3 - Initialization and Anti-collision Protocol and must be capable of identifying multiple credentials in a single field and selecting one credential to work with.

e. The card shall conform to the current version of ISO/IEC 7816, part 4 command set.

f. The card shall meet the current version of ISO/IEC 7810 card specifications for length, width, thickness, flatness, card construction and durability, and shall be in a form suitable for direct two-sided dye-sublimation or thermal transfer printing on the specified card printer.

g. Presentation of the card to the access control reader in accordance with ISO/IEC 14443 shall result in an accurate reading of the card. [24]

h. The card shall be warranted in compliance with the warranty statement of the specification. [25]

i. Provide [specify quantity] ISO/IEC 14443 compliant access control cards, compatible with the specified readers.

j. The card must be capable of being worn and displayed by personnel. Contactless smart cards should not be slot-punched; a sleeve or other form of carrier should be used. [26]

k. The card shall be available with or without a magnetic stripe, with security taken into consideration. [27]

### 4. Access Key Fob

a. Access fobs shall be used with ISO/IEC access readers to gain entry to access controlled portals (e.g., doors, gates, turnstiles) and to hold information specific to the user.

b. The fob shall operate in the 13.56 MHz high frequency band only.

c. The fob shall comply fully with the current version of ISO/IEC 14443 parts 1, 2, 3, and 4 open card standards to enable interoperability among suppliers of products using the same chip sets and must be compatible with the specified access control reader.

d. The fob shall conform fully to the current version of ISO/IEC 14443 Part 3 – Initialization and Anti-collision Protocol and must be capable of identifying multiple credentials in a single field and selecting one credential to work with.

e. The key fob shall conform to the current version of ISO/IEC 7816, part 4 command set.

f. The key fob shall be constructed of durable material, and shall be suitable for placement on a key ring.

g. Presentation of the fob to the access control reader in accordance with ISO/IEC 14443 shall result in an accurate reading of the fob. [24]

h. Provide [specify quantity] ISO/IEC 14443-compliant key fobs compatible with the specified readers.

i. The key fob shall be warranted in compliance with the warranty statement of the specification. [25]

## D. ACCESS CREDENTIALS [7] – ISO/IEC 15693

Provide [specify quantities] ISO/IEC 15693 compliant contactless credentials with the following features or form factors:

### 1. Credential Security Features [16]

a. Access credential shall have a cryptographically-sound mutual authentication mechanism based on an open, recognized and public symmetric cryptographic algorithm (three-key TDES or AES) or asymmetric cryptographic algorithm (RSA or ECC). [29]

b. In the case of a symmetric key credential, it shall be diversified using a method that is non-reversible and incorporates a unique, reliable identifier (for example, the non-alterable chip individual serial number). [30]

c. In the case that secure messaging is required between the card and reader, a secure messaging method shall be utilized to provide confidentiality of the data communications between the reader and the credential using an open, recognized and public symmetric cryptographic algorithm (three-key TDES or AES) or asymmetric cryptographic algorithm (RSA or ECC). This messaging method shall be designed to prevent simple cryptographic attacks like man-in-the-middle and replay attacks. [31]

**2. Access Card [24]**

a. Access cards shall be used with ISO/IEC 15693 access readers to gain entry to access controlled portals (e.g., doors, gates, turnstiles) and to hold information specific to the user.

b. The card shall operate in the 13.56 MHz high frequency band only.

c. When multiple cards are in the reader field, the reader shall respond in a manner that is compatible with the PACS controller.

d. The card shall meet the current version of ISO/IEC 7810 card specifications for length, width, thickness, flatness, card construction and durability, and shall be in a form suitable for direct two-sided dye-sublimation or thermal transfer printing on the specified card printer.

e. Presentation of the card to the access control reader in accordance with ISO/IEC 15693 shall result in an accurate reading of the card. [24]

f. The card shall be warranted in compliance with the warranty statement of the specification. [25]

g. Provide [specify quantity] ISO/IEC 15693 compliant access control cards, compatible with the specified readers.

h. The card must be capable of being worn and displayed by personnel. Contactless smart cards should not be slot-punched; a sleeve or other form of carrier should be used. [26]

i. The card shall be available with or without a magnetic stripe, with security taken into consideration. [27]

**3. Access Key Fob**

a. Access fobs shall be used with ISO/IEC 15693 access readers to gain entry to access controlled portals (e.g., doors, gates, turnstiles) and to hold information specific to the user.

b. The fob shall operate in the 13.56 MHz high frequency band only.

c. When multiple cards are in the reader field, the reader shall respond in a manner that is compatible with the PACS controller.

d. The key fob shall be constructed of durable material, and shall be suitable for placement on a key ring.

e. Presentation of the fob to the access control reader in accordance with ISO/IEC 15693 shall result in an accurate reading of the fob. [24]

f. Provide [specify quantity] ISO/IEC 15693-compliant key fobs compatible with the specified readers.

g. The key fob shall be warranted in compliance with the warranty statement of the specification. [25]

END

# *A&E Guide Specification Commentary*

The commentary in this section is intended to provide an educational resource for the specifier. The questions and answers are linked to the appropriate item in the guide specification and provide definitions or additional detail describing the specified feature.

Note that this specification was developed to be used for commercial, non-government PACS implementations. The specification does not apply to and should not be used for federal facilities.

### 1. What is a smart card-based PACS?

A physical access control system (PACS) that uses smart card credentials (contact or contactless) and smart card readers for access control is considered a smart card-based PACS.

Smart cards are increasingly accepted as the credential of choice for securely controlling physical access. Standards-based smart ID cards can authenticate a person's identity, enable the determination of the person's appropriate level of access in conjunction with the PACS, and admit the cardholder to a facility. Appropriate use of contact or contactless smart card technology in the PACS design enables security professionals to implement the strongest possible security policies.

More than one application can be carried on a single smart ID card, enabling users to access physical and logical resources without carrying multiple credentials. Access rights can be changed dynamically, depending on perceived threat level, time of day, or other appropriate parameters. Information technology departments can record and update privileges from one central location. Human resources departments can process employees quickly, granting or withdrawing all access rights immediately in a single transaction. The organization as a whole incurs lower maintenance costs.

Additional information on the use of smart cards for physical access control can be found in the Smart Card Alliance white paper, *Using Smart Cards for Secure Physical Access*, available at http://www.smartcardalliance.org/publications-secure-physical-access-report/.

### 2. How should an organization plan for implementing a smart card-based physical access control system?

Identifying and analyzing the organization's application requirements is the first step in planning for and implementing a smart card-based PACS. Additional critical considerations include the following:

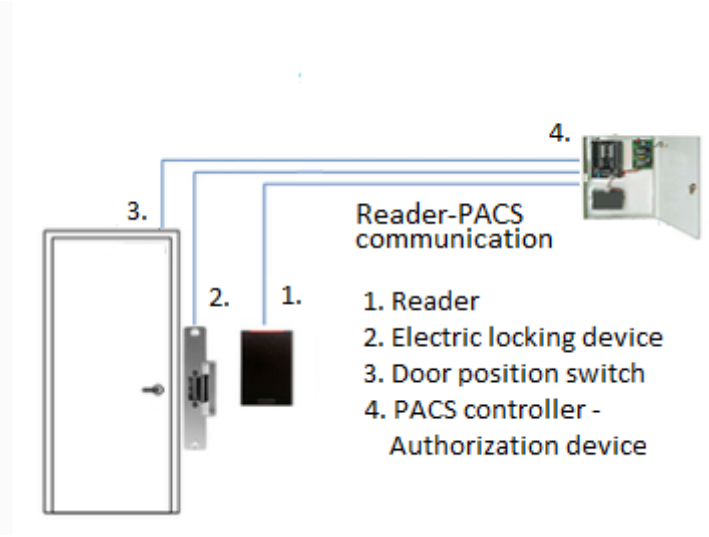
- User interface, performance, and security requirements.
- The required level of integration with other enterprise applications.
- Selection of a system architecture that meets security requirements cost effectively.
- Selection of an appropriate credential technology.
- Credential life-cycle management.
- Migration. When migration is planned carefully, organizations can implement new functionality while accommodating legacy systems.

Once the smart card credential has been specified, the appropriate smart card reader can be identified and specified.

### 3. What is a reader?

A reader is a device that can access data (e.g., a unique identifier) stored in the chip of a smart card, format the data, and send the data to a PACS for authorization. Readers can be separate from or combined with PACS controllers. The card issuer must be capable of producing and personalizing cards that are compatible with the PACS, and each identifier must be unique.

This section describes readers that are separate from the PACS controller (as shown in the following diagram). (Combined reader-controller devices are described in question 4.) Three critical requirements apply to reader selection.




First, the reader must be matched to both the technology of the card and the capabilities of the PACS. Matching means that the reader and card must both interface using the same frequency (e.g., 13.56 MHz), the same standard (e.g., ISO/IEC standard 14443 or 15693), and the same protocol for communication. (See questions 7 and 11 for additional information.) In deployments that specify cryptographic techniques for card, reader, or mutual authentication, key algorithms must be specified as well as an agreement of how to distribute and store the cryptographic keys. In addition, the issuing system must be capable of encoding cards according to the PACS specification and protecting the identifiers and keys used. Security requirements require careful consideration before a system is deployed.

Second, the reader must be capable of transmitting the data that is read from the card to the PACS. A common standard for the reader-to-PACS interface is Wiegand. Wiegand is a widely used simplex (one way) reader-to-PACS technology. Most PACS use Wiegand to receive data from a card reader. In non-Wiegand, or duplex (bi-directional) deployments, the reader must be specified with the appropriate communication protocol. (See question 11.)

The third requirement is reader power. Most PACS provide power to the readers. The reader must either be capable of operating with the power provided by the PACS or be powered separately. Both distance from the controller and reader cabling affect how much power is available at the reader location. The reader manufacturer's specification for power available at the reader must be followed.

### 4. What is meant by "single package type?"

A reader that combines all components, processor, electronics and antenna in one package is a single package type reader. One benefit of using such a reader is that installation is very simple: the reader is contained in a common housing that can be mounted directly on a door frame.

These readers require an antenna and a processor. In addition, readers that can capture a second authentication factor, such as a PIN, must include a keypad. The keypad should be activated only after a card has been presented. Readers with biometric capability also require a sensor that can capture a live biometric sample (e.g., fingerprint, iris, palm vein) and convert the captured data to a biometric template. The template can be used for on-reader or on-card comparison.

### 5. What is an IP rating or NEMA rating?

Indoor and outdoor electronic products and mechanical devices are commonly exposed to people, dirt, and moisture. The case, cabinet, or covering on any electrical or mechanical product protects the device. Case design, which includes such elements as vent holes and the placement of screws and fastening devices, determines how much protection the case provides against intrusions ranging from dirt, dust, and insects to sprayed, dripped or directed moisture and poking fingers.

An *ingress protection* (IP) rating classifies and rates the degree of protection provided against intrusion. IP is the industry standard term created by the International Electrotechnical Commission (IEC). The IEC assigns a 2-digit rating (defined in Standard 60529). The first digit identifies the degree of protection afforded both to the product or device from the intrusion of objects (e.g., fingers, paper clips, dirt) and to the user from hazardous parts or mechanisms inside the product. The second digit identifies the degree of protection against liquids. For example, IP54 indicates that the device is protected from dust and protected from splashing water in any direction. (For a full definition of all numbers and levels that apply to outdoor products, refer to IEC Standard 60529.)

The National Electrical Manufacturers Association (NEMA) rating is a second, equally important rating that defines the types of environments in which an electrical enclosure can be used. The United States typically uses NEMA rating codes. IP codes are more common on devices used internationally.

Access control panels or readers may carry a NEMA rating or an IP rating or both. While the presence of both ratings may be confusing, any rating indicates that at some point in the design process, the product was submitted for testing to a third-party authority that assigned the number.

### 6. What is the advantage of 13.56 MHz contactless smart cards vs. other technologies (e.g., prox, magnetic stripe, bar code)?

A simple comparison of how the different technologies read data from access cards reveals the strengths and weaknesses of each:

- Magnetic stripe cards. Magnetic stripe card readers free-read the data encoded on Track 1, 2, or 3 of the card according to ISO/IEC Standard 7811 using a standard magnetic read head and decipher the data.
- Smart cards using card serial numbers. Smart card readers used with access cards using card serial numbers modulate a signal according to ISO/IEC Standard 14443-2 (at 13.56 MHz), perform anti-collision processing according to ISO/IEC14443-3, and then free-read the card serial number.

- Proximity cards. Proximity card readers modulate a signal (typically 125 kHz; e.g., amplitude shift keying (ASK), frequency shift keying (FSK), phase-shift keying (PSK)), then decode the data (e.g., Manchester Phase Encoding) and decipher it.
- Smart cards using cryptography. Smart card readers using cryptographic authentication modulate a signal according to ISO/IEC 14443-2 (at 13.56 MHZ), perform anti-collision processing according to ISO/IEC 14443-3, use additional ISO/IEC 14443-4 compliant command sets to send commands to the card, use secret keys to perform authentication, read the data, and decipher encrypted data.

The use of contactless smart cards in a PACS offers numerous benefits. The cards are reliable and inexpensive. The card body is durable; the card is passive (no battery), with a low cost of ownership. In addition, the output from the card reader can be communicated in several different ways, making it quite flexible. Typical reader-to-PACS interface options include Wiegand and clock/data. Bidirectional communication options include USB, serial (RS232, RS485), and Internet protocols (e.g., TCP, UDP).

Contactless smart cards also provide the following support for strong data protection:

- A tamper-resistant contactless chip
- Read/write protection for stored information
- High security encryption capability
- Challenge-response mutual authentication capability
- Unique serial numbers
- Biometrics support that can provide a one-to-one match

Contactless smart cards provide on-card intelligence:

- Can process information as well as store it
- Provide support for multiple applications
- Can support update of card information and applications without issuing new cards
- Can support using a public key infrastructure and encryption.

Contactless smart cards are convenient:

- Portable, easy-to-use form factor
- High speed access for high throughput
- Useable in harsh or dirty environments (relying on the RF interface)
- Fast identity authentication

Smart cards that incorporate cryptographic authentication provide strong data security, using cryptographic algorithms, secret keys, and mutual authentication. They are compliant with ISO/IEC standards 14443A, 14443B, 15693, and 7816, making them widely interoperable. Memory storage is increasing as products mature (with cards now available with 64–128K+ bytes of memory). Finally, the cards can support applications in addition to physical access, including logical access, payment, and other applications requiring identity authentication.

### 7. How do I choose between the three choices: ISO/IEC 14443 parts 1 thru 3 A/B (read/write); ISO/IEC 14443 parts 1 thru 4 A/B (read/write); ISO/IEC 15693 (read/write)?

New access control system implementations use ISO/IEC 14443 or ISO/IEC 15693 contactless smart card technologies. ISO/IEC 14443 and ISO/IEC 15693 technologies share the following important features and benefits:

- 13.56 MHz frequency of operation. This frequency can be used throughout the world for contactless applications.
- Read/write capability. This allows user information to be stored and updated on the card (for example, a PIN or biometric template) and helps eliminate the need to access a host computer or database during use.
- Ability for manufacturers to implement security features. Although neither standard specifies security, features such as Data Encryption Standard (DES), Triple DES, and Advance Encryption Standard (AES) are commonly available.
- Support for card-to-reader authentication.
- Ability for vendors to develop readers that incorporate additional security capabilities, such as keypads and biometric sensors.

The key differentiators between ISO/IEC 14443 and ISO/IEC 15693 are the operational ranges, speed (data transfer rates), and extent and maturity of features and applications that use the technologies. The following table compares key features of contactless smart cards and proximity cards.

***Comparison of Standards-Based Contactless Smart Cards and Proximity Cards***

| Features | Proximity | ISO/IEC Standard 14443 | ISO/IEC Standard 14443 parts 1–3 | ISO/IEC Standard 14443 parts 1–4 | ISO/IEC Standard 15693 |
|---|---|---|---|---|---|
| Frequency | 125 KHz | 13.56 MHz | 13.56 MHz | 13.56 MHz | 13.56 MHz |
| Operational range | Up to 1 m (~3 ft), dependent on reader type | Up to 4–10 cm (~2-4 in) | Up to 4–10 cm (~2-4 in) | Up to 4–10 cm (~2-4 in) | Up to 1–1.5 m (~5 ft) |
| Encryption and authentication functions[§] | None | MIFARE®, DES/3DES, AES, RSA[#], ECC | Supplier-specific command set (e.g., MIFARE® Classic) | MIFARE® Plus, DES/3DES, AES, RSA[#], ECC | Supplier-specific protocols, DES/3DES |
| Memory capacity range | None | 1K–128K bytes (depending on card) | 1K–128K bytes (depending on card) | 1K–128K bytes (depending on card) | 256 and 2K bytes |
| Read/write ability | No | Read/write | Read/write | Read/write | Read/write |
| Data transfer rate (Kb/sec) | Not relevant due to small data packet | 106-848 | 106-848 | 106-848 | Up to 26.4 |
| Anti-collision | No | Yes | Yes | Yes | Yes |

| Features | Proximity | ISO/IEC Standard 14443 | ISO/IEC Standard 14443 parts 1–3 | ISO/IEC Standard 14443 parts 1–4 | ISO/IEC Standard 15693 |
|---|---|---|---|---|---|
| Capable of card-to-reader authentication | No | Yes | Yes | Yes | Yes |
| Hybrid card capability[&] | No | Yes | Yes | Yes | Yes |
| Contact interface support | No | Yes | Yes | Yes | No |

[*] ISO/IEC 14443 uses the standard ISO/IEC 7816 for common application-level functions.

[§] The ISO standard does not specify security functions. MIFARE® is a trademark of NXP Semiconductors.

[#] RSA-based encryption and authentication may not be available on all cards due to power consumption, execution time or key length constraints.

[&] Hybrid smart cards have two chips, one supporting the contact interface and one supporting the contactless interface. Dual-interface cards have one chip supporting both contact and contactless interfaces.

### 8. What do I need to specify if I want to have NFC-enabled mobile phones used for access as a credential?

NFC technology is a low power wireless link that can transfer data between two devices that are located a few centimeters apart. NFC requires no pairing code. When two NFC-enabled devices touch each other, data transfer is initiated automatically.

NFC devices are compatible with ISO/IEC Standard 14443. Use of an ISO/IEC14443-compliant reader makes it technically possible for any NFC-enabled mobile device to be used as a credential carrier in a bring-your-own-device (BYOD) environment. Note that the credential data stored on the mobile device and transmitted to the reader must be supported by the PACS panel to which the reader is connected. NFC is available in mobile devices with a variety of operating systems.

Policies that govern how the credential is entered, stored, and maintained in the mobile device must be created by the individual organization.

### 9. What is ISO/IEC 14443 Part 1 Class 1?

ISO/IEC Standard 14443 consists of four parts. ISO/IEC 14443 Part 1 covers the card's physical characteristics. (Note that ISO/IEC 14443 uses the term *proximity card* to refer to a contactless smart card.)

The proximity integrated circuit card (PICC) classes define a combination of antenna dimensions and loading effects. For example, a Class 1 PICC is a proximity card whose antenna is located inside a zone defined by two concentric rectangles. The outer rectangle is 81 x 49 mm, while the inner rectangle is 64 x 34 mm.

The standard allows for considerable freedom in the location and dimensions of antennas in proximity cards, which in practice results in large differences in the working ranges of different card implementations with the same proximity coupling device (the card reader). This can lead to problems in some applications. (For additional information, see *ISO /IEC standard 14443 Part 1 2008: Identification cards — Contactless integrated circuit cards — Proximity cards —Part 1: Physical characteristics AMENDMENT 1: Additional PICC classes*.)

### 10. Describe how the card and reader should work together to prevent multiple reads which can result in anti-passback errors. Why is this needed?

When the card is activated by the reader using the ISO/IEC 14443 standard, the reader and card may perform a mutual authentication. (See question 29). Once the authentication is completed, the reader will read the specified data, such as the card identifier. Once the reader has received the card identifier, the reader must end the session and stop reading the card. This prevents the reader from re-reading and re-sending the card identifier to the PACS multiple times during one card presentation/access request. If multiple cards are present within the read range, the reader should start the authentication process and initiate a new session with the next card.

An access reader should prevent multiple reads; each time the card data is sent to the access control panel (or server), the system processes the data on the card. Multiple reads may corrupt the historic data logs, degrade system performance, result in overflowing buffers and potentially enable a denial of service attack on the access system.

In addition, in deployments where anti-passback is activated, a PACS prevents someone who has already entered a facility from passing an access card to another person outside the facility (the PACS equivalent of "buddy punching" in a time and attendance system).

When the same card identifier is read multiple times at the same reader, the system may interpret this as a passback attempt and generate an alarm. Some systems prevent this alarm from being generated by requiring the door through which the person has entered to open and close before the person is considered to have passed through.

### 11. What communication protocol or format can / should be used between the reader and the PACS?

Communication between the reader and the PACS can rely on either a standards-based one-way protocol and format, which many PACS and associated access control panels (access controllers) can support natively (i.e., Wiegand, ISO/IEC 7811 Clock & Data ABA Track 2), or two-way communications, either standards-based or proprietary. If communication is bi-directional, it is important to be sure that the PACS and any PACS hardware that interfaces with the reader can support the selected format and protocol and are configured appropriately.

Two-way communication typically relies on RS-485 or TCP/IP protocols for communication; the associated data protocol can vary. For example, Open Supervised Device Protocol (OSDP) can be used over either an RS-485 or a TCP/IP connection. The two-way validation process can be performed initially through external secure modules, after which a one-way protocol (such as Wiegand) can support any legacy PACS requirements. Alternatively, the secure validation and authentication mechanisms can both use the two-way communication link between the reader and the PACS hardware. In this case, it is critical to select appropriate readers and ensure that the access control hardware, firmware, and software can work with the readers both to perform validation and respond to access requests.

### 12. Should the reader support both ISO/IEC 14443 and ISO/IEC 15693?

Which ISO/IEC standards readers need to support depends on the user credential population. Typically, an enterprise chooses to standardize on either ISO/IEC 14443 or ISO/IEC 15693 for their credential population. If a mixed credential population must be accommodated, then the reader must support both.

### 13. When would ISO/IEC 7811 Clock & Data ABA Track 2 emulation be required?

A PACS using legacy card-reader technology such as magnetic stripe can be upgraded to use modern smart cards that offer cryptographic protection for the credential data stored in the card and prevent counterfeiting. Use of these cards increases confidence in the claimed identity of the presented card to a level that is not possible with the legacy technologies.

Such an upgrade can be achieved by emulating the data model and transferring legacy card data to a smart card that performs a cryptographic authentication before the card releases any data (see question 29). The card should enable the reader to access the stored data only after the authentication process is completed successfully. The reader reads and sends the card data to the PACS using the same clock and data protocol as the legacy magnetic stripe reader. This approach offers a smooth, cost-effective upgrade that requires no PACS modification.

### 14. What types of visual indicators should the reader include and what do they show?

Types of visual indicators include an LED or LED bar (on/off), a bi-color indicator (red/green), or a tri-color indicator (red/green/amber). Visual indicators show the physical access control system (PACS) response to the person who presents a card to the reader, at a minimum indicating whether access is denied or granted. Some applications also use screens or other displays to provide instructions (e.g., hold card in field, enter PIN).

### 15. How are audible indicators used?

Audible indicators are typically PACS defined and indicate simply that the card is read or a button is pushed for ADA compliance. Audible indicators are almost never used to provide any other feedback on standard PACS card readers.

### 16. What security features need to be considered?

Required security features depend on the type of card and desired use. There are, at a minimum, three security options: plain (no security), plain with cryptographic protection (MAC) that authenticates communication messages (the message comes from an authenticated source), and full encrypted communication.

The following are some key security terms:

- *Hash*: a function that maps a small bit string of arbitrary length to a fixed-length bit string. A hash can meet security requirements if it is a one-way action (it is computationally infeasible to find any input that maps to a pre-specified output) and collision resistant (it is computationally infeasible to find two unique inputs that map to the same output).
- *Symmetric algorithm*: An algorithm that generates a secure key for use in authentication. In symmetric key implementations, the secure key is shared among trusted parties to provide secure authentication means. The risk inherent in symmetric key implementations is that the credential and reader keys can be shared. Additional information on key management can be found at http://csrc.nist.gov/groups/ST/toolkit/key_management.html.
- *Asymmetric algorithm*: An algorithm that generates a secure private key that is mathematically linked to a public key. Asymmetric cryptography is the basis of public key infrastructure (PKI) implementations and has the advantage of keeping the subscriber's private key secure in a cryptographic module that does not allow the private key to be

exported from the module. The subscriber's public key is meant to be shared and is sent with a digitally signed message, for example.

PACS applications that are not operating in the FIPS 201-compliant systems required by the Federal government typically do not use asymmetric keys and PKI. FIPS 201 technology can be used for commercial PACS applications without requiring the Federal policies, simplifying implementation. (Additional information on the use of FIPS 201 standards for commercial applications can be found in the Smart Card Alliance white paper, *The Commercial Identity Verification (CIV) Credential–Leveraging FIPS 201 and the PIV Specifications*, available at http://www.smartcardalliance.org/publications-the-commercial-identity-verification-civ-credential-leveraging-fips-201-and-the-piv-specifications/)

### 17. What types of security functions are needed in communications between the card and reader?

Card–reader communications are susceptible to several types of attack:

- Replay
- Relay
- Man in the middle
- Data sniffing
- Denial of service

Card–reader communications should be designed to avoid these attacks.

In a *replay* attack, the portion of the card–reader communication that authenticates the card is captured and replayed for the reader in an attempt to achieve access without presenting the actual credential. To protect against replay attacks, card–reader communications should require message serialization and encryption so that each message has a pseudo-random component that cannot be replayed.

In a *relay* attack, an attacker reads a card and relays the card information to a reader. Neither the reader nor the card know they are not communicating directly. The attacker may store the communications traffic to attempt to break any encryption. The attacker may also try to alter some messages or retransmit some messages. To protect against relay attacks, card–reader communications should include a timeout to combat relay delay. The communications should be encrypted (and use encryption best practices) to prevent alteration of the messages. The communications should also include functionality to avoid replay attacks.

*Man-in-the-middle* attacks are similar to relay attacks; however, rather than the attacker interposing between the card and reader, the attacker is present in the reader field at the same time as the card. The attacker attempts to corrupt the card transmission or otherwise prevent the reader from receiving card communications and instead presents the information itself. To protect against man-in-the-middle attacks, communications should be encrypted to prevent alteration of the messages. The communications should also include functionality to avoid replay attacks.

In *data sniffing* attacks, a nearby reader attempts to read (and record or relay) communications between the card and the reader. The retrieved information can be used to break the encryption or be stored for future playback. To protect against data sniffing attacks, communications should be encrypted. If data is encrypted using symmetric key methods, the key should be diversified based on a shared secret as well as card-specific data. This approach ensures that if the encrypted communications from a single card are decrypted, communication with other cards is not imperiled. Asymmetric encryption is also acceptable. The communications should also include functionality to avoid replay attacks.

In *denial of service* attacks, an attacker prevents the card and reader from communicating properly. Denial of service can be achieved by flooding the reader field with noise at the correct communications frequency (jamming) or occupying all of the reader's resources by not allowing communications to cease. Counter mechanisms can include spread-spectrum communications or frequency hopping, but smart card communications generally do not implement these features. To reduce the chance of denial of service attack on the access system, once the reader has activated the card and received the card identifier data, the reader must end the session and stop reading the card. This prevents the reader from re-reading and re-sending the card identifier to the PACS multiple times during one card presentation/access request. Each time the card data is sent to the access control panel (or server), the system processes the data on the card. Multiple reads may corrupt the historic data logs, degrade system performance, overflowing buffers and potentially enable a denial of service attack on the access system.

A good discussion of PACS threat vectors can be found in the document, Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (EPACS), available at http://www.idmanagement.gov/documents/piv-e-pacs.

### 18. What security features do smart card-based PACS have?

Since the objective of a PACS is to authorize access to privileged areas appropriately, the initial safeguard against attack is the process by which the smart card is issued. The card should be issued based on sound criteria for verifying an individual's identity. It must be strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation, be able to be rapidly authenticated electronically, and be issued only by reliable providers.

Smart card-based PACS can include additional security features. Card and reader interaction can include the following protection measures:

- Anti-collision avoidance and card selection.
- Reader establishment of communication with the card.
- Mutual authentication, which assures both the card and the reader that they are communicating with an authenticated device (see question 29).
- Message data confidentiality. The message data is encrypted from card-to-reader and reader-to-card.
- Exchange and verification of secret key (symmetric keys).
- Option to use a public key infrastructure (PKI) for authentication.
- The reader requests the data from the card.
- Readers can perform processing for stronger authentication or transmit data to the PACS infrastructure (controllers and applications servers).
- Credential number processing. A method should be used to assure non-duplication of credential numbers, and these numbers should be stored securely in binary format . The credential numbers should not be parsed; if they are, compensating controls should be included to avoid credential number collisions.

Use of secure communication protocols represents an additional line of defense. The typical levels of security supported by secure communications protocols are mutual authentication, integrity, data origin authentication, and confidentiality. A smart card-based PACS can perform the following:

- Validate digital signatures
- Recognize invalid digital signatures
- Recognize certificate/private key mismatch
- Reject expired credentials
- Perform revocation checks

In addition, the PACS infrastructure (application software and access control hardware) can be protected by applying encryption to communications circuits, using strong passwords, and encrypting PIN codes stored in the database server. No one should be able to access cardholder PINs through an application or through the database server.

### 19. What are modern cryptographic standards for secure communications between the card and reader and how do I select which to use?

Cryptographic techniques can be used to secure communications between both hardwired and wireless devices. When the two devices are a smart card and a reader, the encryption techniques often have to be applicable to both contact and contactless communications between the card and the reader. The technology used may be different than the technology used for communication elsewhere in a PACS. Many smart cards support more than one cryptographic standard, for backward compatibility or interoperability with a variety of PACS, or to accommodate the performance strength objectives of the application. Either symmetric or asymmetric encryption keys can be used.

Some popular symmetric encryption standards (algorithms) used or being embraced for use between a smart card and a reader in a PACs are listed in the following table.

| Name | Key Size | Key Type | Block Size | Stream Size |
|---|---|---|---|---|
| Crypto-1* | 48 bits | – | – | 48 bits |
| DES (Data Encryption Standard)** | 56 bits (+8 parity bits) | Symmetric | 64 bits | – |
| 3DES (Triple Data Encryption Standard)§ | 56, 112, or 168 bits | Symmetric | 64 bits | – |
| AES (Advanced Encryption Standard)# | 128, 192, or 256 bits | Symmetric | 128 bits | – |

* Crypto1 is a proprietary encryption algorithm created by NXP Semiconductors specifically for MIFARE® cards (e.g., those used in the Oyster card and CharlieCard). It was published in 2008 and provides low security.

** DES, originally published as FIPS 46 in 1977, is now considered unsecure for many applications and was withdrawn as a standard by NIST.

§ 3DES (or TDES) was published as FIPS 46-3 in 1999 and withdrawn by NIST in 2005. It applies the DES algorithm three times to each data block. It increases the key size without having to create a new cipher algorithm. The three keys can be the same or different. NIST considers the option with three different keys (3KDES) to be appropriate through 2030.

# AES was published as FIPS 197 in 2001. NIST considers AES to be appropriate beyond 2030.

### 20. What types of features on the reader sense and report tampering?

Readers are by necessity located on the non-secure side of an access control point. Because the reader is a collecting device for the credential information, PINs, and biometric data that are used for access authorization, adversaries often view the reader as a primary point of attack. It is therefore important for the reader be able to detect and communicate any attempts to tamper with it.

The reader cover, reader mounting, and card-reader communication are treated as three separate tampering areas. Each uses a separate tamper detection method. When tampering is detected (for example, a reader cover is removed or a reader is removed from the mounting surface or disconnected), a tamper event is created. Most modern PACS have the capability to communicate tamper events to the appropriate system operator as alarm messages. In many cases, a tamper event will cause the PACS to activate video equipment to support operator assessment.

Monitoring the reader cover is the first line of defense against tampering. The reader cover should be monitored by a device that contacts the PACS if tampering occurs. The second tamper detection area is the reader mounting. This area should also be monitored to detect tampering and send messages to the PACS. Although plunger switches are commonly used in these areas as tamper detection devices, some readers offer optical tamper circuits for the cover and plunger or magnetic tamper detection devices for the wall mounting. The third area that should be monitored is reader-to-PACS communication. The PACS should detect any communication interruption and reader substitution.

Tampering alarm messages should be covered by security policies and treated as priority alarms. Because any tamper event should be treated as a hostile event, policies must be defined to allow reader maintenance and replacement. And regardless of how tampering is detected, the tamper devices must be compatible with the PACS capabilities to receive and process the output generated by the device.

### 21. How are reader firmware and keys updated securely?

Ideally, PACS smart card readers use uniquely formatted files that are encrypted using symmetric or asymmetric cryptography and are either loaded at the time of manufacture or after installation using either a bidirectional interface (e.g., RS232, RS485, TCP/IP) or contactless programming cards. Keys can be stored in the reader or in the controller in a uniquely encrypted key store.

### 22. What types of keypads should be considered?

A variety of keypads are available. Which keypad is appropriate depends on the application.

Keypads typically are configured in one of two configurations: the telephone number pad (the number one is in the upper left corner), and the calculator pad (the number one is in the lower left corner). Most keypads for access control are in the telephone format. A scrambled format is also available from a limited number of vendors. Section 508 of the Americans with Disabilities Act requires keypad devices to include accommodations to aid the vision impaired (e.g., Braille markings or a single dot on the center key).

Keypads can be designed with keys that depress for tactile feedback, or they can use piezoelectric technology that is sensitive to a touch on the keypad surface. Membrane or piezo keypads can be designed to withstand outdoor or wash-down conditions.

Keypads can be combined with card readers. Keypad communication is then generally sent over the same interface as reader communication. However, if the keypad is a standalone keypad, it often

uses a Wiegand interface. Wiegand is a one-way interface that allows the control panel to change the color of an LED indicator. Some keypads output a digital signal for each keystroke, while others buffer multiple keystrokes and output a binary representation of the number entered.

The keypad output format must be compatible with the capabilities of the access control panel.

### 23. What are examples of keypad data formats?

The keypad can be used in two ways: to send primary access credential data or to send secondary PIN data. Credential data is considered primary data because that data is used to reference access control lists, while PIN data is used to authenticate the credential data itself. PIN authentication may not be required in all situations; whether it is required is generally determined by a facility risk assessment. Keypads communicate with the PACS system using a Wiegand interface (SIA standard), clock/data interface (ABA standard), proprietary serial protocol, or OSDP protocol (a developing standard).

Regardless of the interface or protocol used, the keypad can send each keystroke independently or buffer multiple keystrokes and output a binary version of the resulting number. When communicating over a Wiegand interface, for example, the data sent for each key may be in 4-bit bursts (4 bits are all that are needed to identify one of the 12 keys on the typical keypad: 0-9, *, and #), 8-bit bursts (which provide some bit error checking), or some other proprietary format.

A keypad that buffers keystrokes has to be able to match the number of keystrokes buffered with the capacity to communicate the resulting number using the configured Wiegand data format. For instance, a 34-bit format, composed of 2 parity bits, a fixed 16-bit facility code, and a 16-bit buffer output, has a maximum decimal equivalent of 65,535. Therefore, the keypad would only be able to buffer 4–5 digits (not all 5-digit combinations can be output using this format). Keypads can typically be configured for one of a variety of formats, to support short or long numbers.

### 24. What should be considered for performance best practices for card-to-reader use and communication?

The 13.56 MHz high frequency contactless interface is more sensitive to local disturbances than the legacy 125 kHz low frequency technologies.

One consideration is the location of the reader. A weak RF field causes the card and reader to make several attempts to establish a session for communication. When the attempt to establish a session fails, a new attempt is made, at a slower transmission rate. RF interference, such as from nearby airports, fluorescent light fixtures, or elevator equipment may reduce the strength of the RF field between the reader and card and cause intermittent card-to-reader communication failures. The presence of metal in the immediate area of the reader can also distort data transmitted between the reader and card. In some cases, this effect can be mitigated by relocating the reader or turning it to face a different direction. Simple RF field strength indicators are available that can show the installer the available field strength for each reader.

In addition, in many readers there is one area where the card is most likely to quickly establish a session with the reader. Training can teach cardholders where to position the card best in relationship to the reader, improving overall satisfaction with the system.

### 25. How should the specification handle warranties of different equipment?

The following sample language can be used to specify warranty terms in the system specification.

1. The contractor shall guarantee the system including all components, parts, and assemblies, in its entirety to be free from mechanical and electrical defects for a period of at least twelve (12) months (parts and labor), commencing upon date of acceptance by owner. A qualified factory-trained service representative shall provide warranty service.
2. The contractor shall make available to the owner a complete maintenance contract proposal after initial warranty period. The proposal shall include:
    a. Response to emergency service requests on site, if required.
    b. Replacement or repair of defective components as required.
    c. Manufacturer's recommended preventive maintenance.
    d. Second year, 3- and 5-year maintenance contract with the price shown for each year and all payment terms and conditions.
3. The service contract shall be optional, and the owner shall have the right to accept or reject the contract and accept only the warranty service as described above, at no additional cost.
4. The contractor's warranty shall cover all costs associated with the troubleshooting, repair, and replacement of defective work, including costs of labor, transportation, lodging, materials, and equipment.
5. The warranty shall not cover any damage to material or equipment caused by accident, misuse, or unauthorized modification or repair by the owner.

### 26. What do I need to consider if the access card is to be slot-punched?

Contactless smart cards should not be slot-punched.

### 27. What other technologies should I consider having the access card support?

Using a smart card as an access card enables systems that can interact with smart card technology to obtain reliable identity information. This identity information can then be used by a variety of applications that require authoritative information, such as time and attendance systems for office buildings, work areas, or construction sites, or applications at cafeterias, where authorization can be managed simultaneously with a payment transaction. Smart cards can provide the identity information, and the third-party application can then process the payment transaction. Smart cards can also be used as secure storage, for processing balances and similar financial information, provided that the containers on the smart card are compatible with the applications.

Other candidate technologies are technologies used for different or legacy applications that are physically resident in the card body but do not interact with the smart card chip, such as a magnetic stripe, a one- or two-dimensional barcode, or a 125 kHz legacy proximity antenna, which can be embedded in the card. Any technology under consideration should be reviewed to determine whether it is supported by standards and whether providers make comparable products that work with the technology.

### 28. How do cards that support ISO/IEC 14443 through Part 3 differ from cards that support ISO/IEC 14443 through Part 4?

*[Note that ISO/IEC Standard 14443 refers to 13.56 MHz contactless smart cards as "proximity cards;" this should not be confused with 125 KHz proximity cards that use different technology and are not covered by the ISO/IEC 14443 standard.]*

ISO/IEC 14443 Part 3 specifies initialization and anti-collision–electrical interface and transmission protocols. Part 3 does not include the command set that would be used in card applications. ISO/IEC 14443 Part 3 supports the following:

- Polling for proximity cards or objects (PICCs) entering the field of a proximity coupling device (PCD)
- The byte format, the frames, and the timing used during the initial phase of communication between PCDs and PICCs
- The initial Request and Answer to Request command content
- Methods to detect and communicate with one PICC among several PICCs (anticollision)
- Other parameters required to initialize communications between a PICC and PCD
- Means to ease and speed up the selection of one PICC among several PICCs based on application criteria

ISO/IEC 14443 Part 4 specifies the transmission protocol. ISO/IEC 14443 Part 4 cards support the standardized T=CL protocol. Typically ISO/IEC 14443 Part 4 cards provide higher levels of functionality including organization, security, and commands for data interchange.

Cards that support ISO/IEC Part 4 specify the following:

- Content of command-response pairs exchanged at the interface
- Means to retrieve data elements and data objects in the card
- Structure and content of historical bytes to describe operating characteristics of the card
- Structure for applications and data in the card, as seen at the interface when processing commands
- Methods to access files and data in the card
- A security architecture defining access rights to files and data in the card
- Means and mechanisms for identifying and addressing applications in the card
- Methods for secure messaging
- Methods to access the algorithms processed by the card (the algorithms are not described)

The specific types of applications to be implemented will determine whether the contactless smart card must support ISO/IEC 14443 through Part 3 or through Part 4.

### 29. What is mutual authentication?

Mutual authentication is a process that enables two entities to authenticate each other before exchanging information. Mutual authentication means that the reader authenticates the card, and the card authenticates the reader, thus ensuring that only legitimate components are involved.

### 30. What is key diversification?

Key diversification means that each card has its own security key, derived from a master key. The key is not the same for all credentials in a system. Key diversification protects against disclosure of a master key.

### 31. What is secure messaging?

In this case, secure messaging enables data and commands transmitted between the card and reader to be both integrity protected and encrypted.

### 32. What is message authentication?

Message authentication (MAC) provides assurance that a message coming from an authenticated source has not been modified.

### 33. How should the reader protect security keys?

The reader should protect security keys against being read in any form other than the intended one. It should not be possible to read keys back from the reader hardware or from reader communications. In the case of high security cards, it should not be possible to eavesdrop the keys from the reader.

## *Publication Acknowledgements*

This white paper was developed by the Smart Card Alliance Access Control Council to provide a tool for architects, engineers, consultants, integrators, manufacturers and end users to incorporate smart card-based physical access control cards and readers into specifications for non-government PACS implementations.

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 Access Control Council members for their contributions. Participants involved in the development of this white paper included: Advanced Card Systems, Ltd.; Allegion; AMAG Technology, Inc.; Booz Allen Hamilton; CH2M HILL; Eid Passport Inc.; GSA; HID Global; HP Enterprise Services; Identification Technology Partners, Inc.; Identiv; IDmachines; IQ Devices; NXP Semiconductors; Oberthur Technologies; Quantum Secure Inc.; Roehr Consulting; Secure Mission Solutions; Stanley Security Solutions; Tyco Software House; U.S. Department of State; XTec, Inc.

The Smart Card Alliance thanks **Steve Rogers**, IQ Devices, who was the member project lead, and the Council members who participated in the project team to write the document, including:

- **Dave Adams**, HID Global
- **Don Campbell**, Eid Passport
- **Sal D'Agostino**, IDmachines
- **Tony Damalas**, Stanley Security
- **Frazier Evans**, Booz Allen Hamilton
- **Dave Helbock**, XTec, Inc.
- **Stafford Mahfouz**, Tyco Software House
- **Cathy Medich**, Smart Card Alliance
- **Robert Merkert**, Advanced Card Systems
- **Steve Rogers**, IQ Devices
- **Greg Russell**, Eid Passport
- **Adam Shane**, AMAG Technology
- **Lars Suneborn**, Smart Card Alliance
- **Joe Tassone**, Identiv
- **Mike Zercher**, NXP Semiconductors
- **Rob Zivney**, ID Technology Partners

The Smart Card Alliance also thanks Access Control Council members who participated in the review of the white paper including:

- **Bob Dulude**, HID Global
- **Jeremy Earles**, Allegion
- **Walter Hamilton**, ID Technology Partners
- **Daryl Hendricks**, GSA
- **Russ Kent**, HP Enterprise Services
- **Lolie Kull**, HP Enterprise Services
- **Mike Kelley**, Secure Mission Solutions
- **Ahmed Mohammed**, Oberthur Technologies
- **Roger Roehr**, Roehr Consulting
- **Mark Steffler**, Quantum Secure
- **Brian Stein**, CH2M HILL
- **Mike Sulak**, U.S. Dept. of State

## *Trademark Notice*



## *About the Smart Card Alliance Access Control Council*

The Smart Card Alliance Access Control Council is focused on accelerating the widespread acceptance, use, and application of smart card technology for physical and logical access control. The group brings together, in an open forum, leading users and technologists from both the public and private sectors and works on activities that are important to the access control community and that will help expand smart card technology adoption in this important market. The Council works on projects to stimulate the use of smart card technology for access control.