Frequently asked questions
Readers & credentials

Readers

Basic Selling Information

1. **What are the benefits of aptiQ™ Readers?**
   - Streamlined multi-technology line-up reduces ordering confusion by selecting one type of reader to meet current and future needs.
   - Read highly secure aptiQ smart credentials using MIFARE® and MIFARE DESFire™ EV1 and proximity credentials
   - Easy to install with standard wiring, quick-connect wiring harness, and simplified mounting bracket
   - Aesthetically pleasing with modern shape and multiple color options to match any facility's décor
   - Priced competitively with industry leading single technology readers
   - Wiegand output allows the reader to interface with many common access control systems
   - Optional RS-485 connection provides more robust bi-directional OSDP communication
   - IP-65 Certified – performance in dusty or wet conditions
   - Keypad reader has an anti-microbial coating
   - Smart readers are NFC and aptiQmobile peer to peer capable

2. **What is the best way to migrate or transition from old proximity card technology to newer contactless smart technology?**
   The easiest and most cost effective plan for migration involves the use of multi-technology readers. Rather than replacing entire card populations immediately (typically administratively intense), customers can replace readers and migrate at their own pace. Once multi-technology readers have been installed the user can begin distributing secure contactless smart cards. A security office may choose to administer these new cards according to established policy.

3. **What does Multi-Technology mean when referring to a reader?**
   Multi-technology at Allegion means our readers are capable of reading more than one credential technology. Currently our readers are capable of reading both 125 kHz proximity technology and 13.56 MHz smart technology in the same reader. We also offer keypad and magnetic stripe options.

4. **What technology does aptiQ utilize/support?**
   MIFARE® and MIFARE DESFire™ EV1

5. **What readers are the aptiQ smart cards compatible with?**
   aptiQ smart cards using MIFARE® or MIFARE DESFire™ EV1 technology are currently compatible with the aptiQ smart and multi-technology reader family from Allegion (model #s: SM10, MT11, MT15, MTK15, MTMS15, MTMSK15).

6. **What are the benefits of multi-technology readers?**
   Benefits include easy migration to smart card technology from proximity, the ability to use multiple credential types in one facility, and the ability to transition at one's own pace from proximity to smart technology.

7. **Can my access control system support smart readers?**
   If the access control system can support a Wiegand reader or a Wiegand input, then yes. If it supports proximity readers and cards, it can support smart and multi-technology readers and cards.

8. **Which readers can be used with which cards?**
   Typically a proximity reader can read proximity cards and a smart card reader can read smart cards. There are also multi-technology readers that can read both smart and proximity cards. A multi-technology reader is ideal for transitioning from proximity technology to smart card technology at your own pace.

9. **Is there a "how-to order" guide for the aptiQ reader line?**
   Yes, the readers how-to-order guide can be found here. A credentials how-to-order guide is also available.

Reader and Credential Technologies

1. **Why choose smart technology over proximity?**
   There are many reasons to use smart over proximity cards, but the primary reasons are higher security and more memory.

2. **What is the difference between proximity and contactless smart card/reader technologies?**
   In using the two technologies purely for access control, there really are no visible differences for the user. With either technology the user simply presents a card to a reader and access is either granted or denied. The user is notified usually through both audible and visual means (beeper and LED). However, what cannot be seen may be of significant importance.

   The transaction between a typical proximity card and reader is a "license plate" transaction, meaning that as a card is presented to a reader, the card transmits a static number "in the clear" (through radio frequency communication a number is sent to and received by the reader). The number is the same every time the same card is presented. Conceivably, with the proper equipment, this number could be captured by someone skilled in RFID technologies and then replayed to the reader at a later time to gain unauthorized access.

   In comparison, a secure contactless smart card and reader transaction generally contains a much higher level of security. When a card is presented to the reader there is a question and answer session between the card and reader in order for each to authenticate the other. In very simple terms, the reader asks the card for its secret password, the card then asks the reader its mother's maiden name and so on. After this occurs (in less than ¼ second) the card and reader have "mutually authenticated" each other as belonging to one another. Access is either granted or denied by the access panel.

   During the transaction just described, the information actually transmitted between card and reader is encrypted or sent as a coded message. This is important in the event that someone or some device was illicitly attempting to capture the transmission of data. In that event, encrypted data will be much more difficult to use than the "license plate" unprotected data transmitted by a traditional proximity reader.

3. **Why was MIFARE DESFire™ EV1 created after MIFARE®?**
   NXP created MIFARE DESFire™ EV1 as the next generation in its technology platform (see www.MIFARE.net)

   MIFARE Classic
   The MIFARE Classic family is the pioneer and front runner in contactless smart ticket ICs operating in the 13.56 MHZ frequency range with read/write capability and ISO 14443 compliance. MIFARE Classic can be used for a variety of applications including access control, public transit, event ticketing, and more. MIFARE Classic uses 3DES (triple DES) to secure its data. 3DES (triple DES) is a specification for the encryption of electronic data which applies the Data Encryption Standard (DES) three times to each block.

   MIFARE DESFire EV1
   MIFARE DESFire™ EV1 was created as the next generation smart card technology by NXP. MIFARE DESFire EV1 offers a higher level of security because it uses 128 AES encryption. 128 AES is a specification for the encryption of electronic data using a 128 bit, symmetric key algorithm. MIFARE DESFire EV1 is ideal for service providers wanting to use multi-application smart cards in transport schemes, e-government or identity applications. It fully complies with the requirements for fast and highly secure data transmission, flexible memory organization and interoperability with existing infrastructure.

4. **What is iCLASS®?**
   iCLASS® is a proprietary smart card technology developed by HID that operates on ISO 15693.

5. **What is aptiQ?**
   aptiQ is a smart technology brand that operates on ISO 14443 and is based on an open architecture design built on smart technology using MIFARE® and MIFARE DESFire™ EV1. aptiQ smart technology enhances the intelligence of products in readers, credentials, and smart phone applications. aptiQ seamlessly interfaces and communicates with a variety of products, and provides a platform that easily adapts as new innovations enter the marketplace.

6. **What is the difference between ISO 14443 certification and ISO 15693?**
   ISO 14443 and ISO 15693 both apply to smart cards. The significant differences include the data transmission rates and the read ranges allowed by the respective standards. ISO 14443 transmits data up 4 times faster than ISO 15693 (ISO 14443 operates at 106K Baud data transfer speed, ISO 15693 operates at 26K Baud data transfer speed). In general, ISO 14443 cards have a shorter read range for security, but faster data transfer speeds than ISO 15693 cards.

Credentials

Basic Selling Information

1. **What is a credential?**
   A credential is anything that can identify you to a decision making system or device. A credential can be a mechanical key, personal identification number, biometric, magnetic stripe, a proximity card, or a smart card, among others.

2. **What is a proximity card?**
   A proximity card is a type of credential that is typically used for access control. A proximity card is a contactless integrated circuit device with an antenna and a chip that operates on a 125 kHz frequency. A proximity card becomes energized when it enters the RF field of the reader and transmits its static card data.

   From a technical standpoint, a proximity card has an antenna and chip set tuned to a 125 kHz frequency. When a proximity card is positioned in a 125 kHz RF field, the card will power up and repeatedly send out it's bit information by using FSK, ASK, or PSK techniques to manipulate the RF field. The reader will detect and interpret these filed manipulations into a bit stream for use in physical access identification. All data flows from the card to the reader. No information flows from the reader to the card. We do read FSK and ASK. We DO NOT read PSK.

3. **What is a contactless smart card?**
   A smart card is similar in construction to a proximity card. Both have an antenna and a chip. For a smart card, this chip is a microprocessor. A microprocessor is essentially a mini computer. Due to the added capability of a microprocessor, a smart card has the ability to store additional information and perform security functions. The common properties of proximity cards and smart cards are the same but smart cards have significantly more capability than proximity cards.

   From a technical standpoint, a smart card typically has an antenna and chipset tuned to a 13.56 MHz frequency. Unlike proximity cards, when a smart card is positioned in a 13.56 MHz RF field, the card will not automatically transmit data. A smart card will only respond to commands that originate from the reader. So, the reader must query the card for information to obtain a bit stream for use in physical access identification.

4. **Why is a smart card smart?**
   Smart cards are fast, secure, and have storage capability. Smart cards operate at a 13.56 MHz frequency which makes them faster than a proximity card. Mutual authentication, key diversification, and encryption are tools used to protect the information on a smart card. This type of security is not possible with a proximity card. Smart cards also offer storage; this means that in addition to access control information you are able to store additional information about the user including cashless vending, cafeteria services, transportation, biometric data, etc.

5. **What type of information can I keep on my smart card?**
   A smart card can store many different types of information and applications from banking, to transportation, to cashless vending, to healthcare, to biometrics, to cafeteria services, and more.

6. **Why choose smart card technology over proximity?**
   Smart cards are faster, more secure and have significantly more capability than traditional proximity cards. There are many reasons to use smart over proximity cards, but the primary reasons are higher security, more memory and cost savings.

7. **Why select smart credentials from Allegion?**
   Allegion has standardized on credential platforms that adhere to ISO standards. These are often called 'open' or 'non-proprietary' technologies. Who would choose to be locked in to one technology if they have a choice? Many large organizations have made an educated decision not to choose a proprietary card. In Europe, where smart cards are far more prevalent, proprietary cards have very little traction. Not only does choice mean a better financial value, it means a more secure and flexible offering than the competition.

8. **How does contactless smart card technology compare in price to traditional proximity systems?**
   A smart card has the ability to store more information than just a badge ID number. It can store multiple applications including cashless vending, library, transit and biometric templates to name a few. Smart cards also communicate using encryption and other data securing features. Even with the additional features, smart card technology is often as competitive or more competitive than proximity systems. Talk to your Electronic Sales Team representative for more specific pricing information.

9. **Can my access control system support smart cards?**
   If the access control system can support a Wiegand reader or a Wiegand output, then yes. If it supports proximity readers and cards, it can support multi-tech readers and smart cards.

10. **Does Allegion offer proximity cards compatible with HID® technology?**
    Yes. Allegion offers a complete line of proximity credentials and multi-technology credentials (proximity and smart card technology in the same credential) that are compatible with certain HID® proximity protocols. The cards are of comparable quality to those offered by HID and are compatible with HID® and XceedID proximity readers.

The Details

1. **Will I be able to use one aptiQ card to perform more than one application such as access control, food service payment, and cashless vending?**
   Yes. It's conceivable that you could employ multiple applications on a single card. In reality, a system might utilize one application for general access control, another for a biometric, and another for cashless vending.

   The aptiQ Alliance Program is working closely with application members and providers to ensure that a suite of products is available to Allegion credential customers.

2. **I have heard for several years that "smart card" technology will replace current card technologies and yet it hasn't happened. What, if anything, is changing this trend to smart cards?**
   Over the past few years contactless technology has evolved and semiconductor manufacturers are delivering much more competitive price points. Today you can purchase a contactless smart card with higher security for nearly the same price as a standard proximity card.

   Smart cards provide the flexibility to store multiple applications on a single card. This is becoming increasingly popular.

   Another very important reason that smart card adoption is taking hold is that during the summer of 2003 the U.S. government adopted standards for interoperability (some of this is still in process). The government is driving toward inter-department interoperability of secure credentials. This significant event is already spilling over into commercial security and will move the security industry toward open architecture systems, driving the adoption of standards for contactless technologies.

3. **What's a PIV card?**
   PIV stands for Personal Identity Verification. This card is based on a standard called FIPS 201-1 that specifies the architecture and technical requirements for a common identification standard for federal employees and contractors.

4. **What is a PIV-I card?**
   PIV-I stands for PIV-Interoperable. Federal contractors are not actually federal employees. Therefore, they cannot be issued a standard PIV card with federal information enrolled on it. If the contractor wants to use similar PIV cards for physical access, they may use PIV-I cards which have certain fields in the application set to maximum values (e.g 9999) indicating that the GUID is to be used for the physical access ID and not the standard FASC-N and Expiration Date fields.

5. **Can you deploy multiple technologies on the same credential? What type of reader is required?**
   We do offer multi-technology credentials. They are available with Proximity & MIFARE® and Proximity & MIFARE DESFire™ EV1 (aptiQ™). Multi-technology readers are required to read both proximity & smart (MT11, MT15, MTK15). Our multi-technology readers with mag stripe read mag stripe, proximity, and smart (MTMS15, MTMSK15). If you were to use one of our single frequency readers they will only read the matching frequency (PR10 reads proximity only and SM10 reads smart only).

Glossary of Terms

125 kHz: Radio waves operating at 125 thousand cycles per second. This technology has historically been the standard in proximity card/reader

128 Bit AES: A specification for the encryption of electronic data using a 128 bit, symmetric key algorithm

13.56 MHz: Radio waves operating at 13.56 million cycles per second allowing encrypted card and reader communication. This technology has historically been the standard in smart card/reader

26 Bit Format: The most common data format for RFID badges – consists of 4 components: Even Parity (1 bit), Facility Code (8 bits), Card Number (16 bits), and Odd Parity (1 bit)

3DES (TDEA): Triple DES is a specification for the encryption of electronic data which applies the Data Encryption Standard (DES) three times to each block

Access Control: The process of granting or denying specific requests to gain access to a logical system or a physical facility/location

Access Control Credential: A physical/tangible object, a piece of knowledge, or a facet of a person's physical being, that enables an individual access to a given physical facility or computer-based information system. Typically, credentials can be something you know (such as number or PIN), something you have (such as an access badge), something you are (such as a biometric feature) or some combination of these items. The typical credential is an access card, key fob, or other key

Amplitude Shift Key (ASK): A proximity card technology that communicates through amplitude shifting. The cards are commonly identified as GE/CASI or PROXLITE or OPENCLASS cards. XceedID readers support these cards and the default output format is 4002 optionally 4001

Anti-collision: The process built into an RFID system that protects multiple cards from being read at the same time when within the reader's RF field

Application Field: Areas in a smart card that house different applications and are protected by security keys

Application Programming Interface: A source code interface that is provided in order to support requests to be made by other computer programs and/or to allow data to be exchanged

Asymmetric Keys: Two related keys, a public and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification

Badge ID: The unique identifier for each card/credential within an access control system

Biometric: A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of a user. Facial images, fingerprints, and iris scan samples are all examples of biometrics

Biometric Information: The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns)

Biometric System: An automated system capable of the following:
-Capturing a biometric sample from an end user

-Extracting biometric data from that sample
-Comparing the extracted biometric data with data contained in one or more references
-Deciding how well they will match
-Indicating whether or not an identification of verification of identity has been achieved

Card Serial Number (CSN): A number issued by the manufacturer with no repeats. It can only be read and is sometimes called the Unique Identifier or UID – sizes of the CSN (4 to 8 bytes) varies according to the type of card technology. Any reader that conforms to the standard can read CSN

CE Mark: European certification that products meet RF interference standards

Contactless: A credential and reader system utilizing RFID technology to energize a microprocessor through and antenna to enable communication

Cryptographic Key (Key): A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm

Data0 (D0): One of two wires in Wiegand Communication Interface and represents the binary '0'

Data1 (D1): One of two wires in Wiegand Communication Interface and represents the binary '1'

Digital Signature: A series of numbers used as identification

Encryption: The reversible transformation of data from the original to a difficult to interpret format as a mechanism for protecting its confidentiality, integrity and its authenticity. Encryption requires use of an encryption algorithm and one or more encryption keys.

FCC Certification: US certification indicating that products meet RF interference standards

Federal Agency Smart Card Number (FASC-N): The data element that is the main identifier on the PIV card and is used by a physical access control system

FIPS 201: Federal Information Processing Standards Publication 201 is a United States federal government standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors in response to HSPD 12

Format: The way that the information (parity bits, facility codes, badge number) is organized on the credential

Frequency: The measure of the number of radio wave cycles completed in a specified period of time

Frequency Shift Key (FSK): A proximity card technology that communicates through frequency shifting. The cards are commonly identified as HID Prox, ISO-Prox, A WID, and Lenel Prox (to name a few) XceedID readers support these cards and output format and bit count is in the card

Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:

1. **One Way** – It is computationally infeasible to find any input that maps to any pre-specified output
2. **Collision Resistant** – It is computationally infeasible to find any two distinct inputs that map to the same output

HSPD 12: Homeland Security Presidential Directive 12 calls for a mandatory, government-wide standard for secure and reliable forms of ID issued by the federal government to its employees and employees of federal contractors for access to federally-controlled facilities and networks

Integrated Circuit Card- The simplest form of Smart Card that contains integrated components with simple memory (similar to an electromagnetic strip) and can complete simple verifications like PIN Codes or other basic hardware authentication

ISO 14443: A series of international, vendor-independent standards for proximity RFID that establishes guidelines for two types of Smart Cards (A & B) – the most common application, requires a read within 4 inches of the reader, and includes: Classic MIFARE, EV1, DESFire, and PIV

ISO 15693: A series of international, vendor-independent standards for vicinity RFID that establishes guidelines for Smart Cards that can read up to 1-1.5 meters – credentials include: ISO-X, iCLASS and Inside **XceedID only reports CSN on iClass and Inside

Key Fob: A specific form factor of credential that generally refers to a hard plastic disc that is carried on a key chain

Key Management: The process of controlling and managing the secret keys used in the cryptographic functions to encrypt data

Message Authentication Code: A piece of information that is used to authenticate a message

Microprocessor Card: A sophisticated form of a Smart Card with a secure microprocessor imbedded in plastic – contains full blown operating system (O/S), can do complex functions (cryptographic calculations, memory management, biometric verifications, etc.)

MIFARE®: A contactless and dual smart card chip technology produced by NXP that is fully compliant with the ISO 14443 standard

Modulation: The changing of radio waves in a specific manner in order to represent data

Multi-Technology Credential: A credential that contains two or more types of technology – ex. Proximity & Smart

Multi-Technology Reader: A reader with the ability to read two or more types of credential technologies – ex. Proximity & Smart

NFC (Near Field Communication): A wireless communication system that uses technology in Smart Phones to emulate ISO 14443 technology

Off-Card: Refers to data that is not stored within the card or to a computation that is not performed by the Integrated Circuit Chip (ICC) of the smart card

On-Card: Refers to data that is stored within the smart card or to a computation that is performed by the Integrated Circuit Chip (ICC) of the smart card

Personal Identification Number (PIN): A secret that a claimant memorizes and uses to authenticate his or her identity

Personal Identity Verification (PIV) Card: A physical artifact (e.g., identity card, smart card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer

readable and verifiable) – can include **CAC** (Common Access Card), **TWIC** (Transportation Worker Identification Credential), **FRAC** (First Responder Authentication Credential)

Phase Shifting Key (PSK): A proximity card technology that communicates through phase shifting. The cards are commonly identified Indala cards. XceedID does not support these cards

PKI-Card Authentication Key (PKI-CAK): An authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the Card authentication key of the PIV card and a contact or contactless reader

PKI-PIV Authentication Key (PKI-AUTH): A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the PIV authentication key of the PIV card and a contact reader

Proximity Credentials: Identification cards or badges that operate in the low frequency range (125kHZ)

Public Key: The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data

Public Key Infrastructure (PKI): A support service that provides the cryptographic keys needed to perform digital signature based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system

RS232 or RS485: Standards for serial communication lines that allow two way communication

Secret Key: A cryptographic key that must be protected from unauthorized disclosure to protect data encrypted with the key. The use of the term “secret” in this context does not imply a classification level; rather, the term implies the need to protect the key from disclosure or substitution

Secure Sector: The private area of non-volatile memory on a smart card – can be one large piece or divided up into many small areas. Access to the Secure Sector is protected by secret keys that are large numbers used with encryption algorithms. Any reader that attempts to access the Secure Sector must know the secret key

Smart Credentials: Identification cards or badges that operate in the high frequency range (13.56 MHz) and have additional memory for multiple applications and support the ability to read/write

Unique Identifier (UID): The unique number given to a credential at time of manufacture (see CSN)

Wiegand Communication Interface: A two wire communication interface between the reader and a controller or other device – the communication is one direction and only flows from the reader to the controller using two wire communications (DATA0 and DATA1)

Wiegand Data: The binary representation of card data that is converted to a number and is transmitted via the Wiegand Interface

Acronyms

3DES	Triple DES Encryption Standard
AES	Advanced Encryption Standard
AID	Application Identifiers
API	Application Programming Interface
ASK	Amplitude Shift Key
CAC	Common Access Card issued by the Department of Defense; PIV card
CAK	Card Authentication Key
CHUID	Cardholder Unique Identifier
CSN	Card Serial Number
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standard
FRAC	First Responders Authentication Credential
FSK	Frequency Shift Key
HSPD	Homeland Security Presidential Directive
MAC	Message Authentication Code
O/S	Operating System
PCI	PIV Card Issuer
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PSK	Phase Shift Key
RF	Radio Frequency
RFID	Radio Frequency Identification