Schlage

Electronic security

Readers & Credentials

Datasheets

Master Index

ALLEGION™

aptiQ™

FIPS 201-1 compliant readers

Overview

aptiQ® smart and multi-technology readers by Allegion have been approved by the U.S. Government under HSPD-12 for FIPS 201-1 compliance as PIV transparent readers. PIV compliance is available on six reader models, including the SM10 smart mini-mullion, MT11 multi-technology mullion, MT15 multi-technology single gang, MTK15 multi-technology single gang with keypad, MTMS15 multi-technology magnetic stripe and MTMSK multi-technology magnetic stripe with keypad.

aptiQ multi-technology readers are a unique and critical component of successful security upgrades in all sectors of the government. FIPS 201-1 is a Federal Information Processing Standard ("FIPS") developed by the National Institute of Standards and Technology ("NIST") to satisfy the requirements of HSPD-12, a Homeland Security Presidential Directive. One of the main objectives of HSPD-12 is to ensure government-wide interoperability for information technology and security through the implementation of a range of federal standards and product requirements. FIPS 201-1 seeks to improve identification and authentication of Federal employees and contractors for access to the federal facilities and information systems.

aptiQ FIPS 201-1 PIV compliant readers are available with multiple data output formats, which provide unprecedented versatility within the PIV & PIV-I specification.

In addition to reading approved FIPS 201-1 PIV & PIV-I credentials, aptiQ smart and multi-technology readers are also compatible with many standard proximity and leading smart card technologies (see specifications). The ability to read multiple existing card types and PIV & PIV-I cards simultaneously is a tremendous benefit to those agencies looking to transition seamlessly from older proximity technologies to new, mandated PIV & PIV-I credentials. A mixed population of old prox credentials and new PIV & PIV-I credentials is unavoidable during the government's multi-year upgrade path to FIPS 201-1 compliance.

Features and benefits

- Compatibility: compatible with industry standard magnetic stripe technology (tracks 1, 2, or 3) and 125 kHz and 13.56 MHz contactless technologies
- Read range: up to 6 inches (proximity), up to 2 inches for PIV & PIV-I credentials
- Tri-state LED (red, green, amber): visual indicator and audio feedback representing status and activity information
- Tamper detection
- Environment: accommodates interior, exterior, metal and non-metal installation environments

Additional features

- Compliance: compatible with applicable ISO standards
- Compatible with all access control systems that support Wiegand format
- Warranty: limited lifetime against defective workmanship and materials
- Additional technologies supported
  - Magnetic stripe
    - Track 1, 2, or 3
  - Proximity
    - Schlage
    - XceedID®
    - HID® Proximity (certain formats)
    - GE/CASI ProxLite™
    - AWID® Proximity
  - Smart card (secure sector only)
    - Schlage
    - aptiQ® using MIFARE® Classic
    - aptiQ using MIFARE DESFire™ EV1
    - FIPS 201-1/PIV & PIV-I
  - Smart card (card serial number only)
    - DESFire® application HID iClass®
    - Inside contactless PicoTag™

Ordering information

- **SM10** - Smart mini-mullion reader
- **MT11** - Multi-technology mullion reader
- **MT15** - Multi-technology single gang reader
- **MTK15** - Multi-technology single gang reader with keypad
- **MTMS15** - Multi-technology magnetic stripe reader
- **MTMSK15** - Multi-technology magnetic stripe reader with keypad

aptiQ PIV readers have been approved by the GSA lab as compliant with FIPS 201-1 and the appropriate PIV credentials.

Please see individual data sheets for each reader for more specific technical information.

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

aptiQ™

Credential Compatibility Guide

125 kHz STANDARD PROXIMITY

XceedID™	LenelProx®
Schlage	HID®
GE/CASI®	AWID®

For added security, customers can choose to disable proximity functionality once the transition from proximity to contactless smart cards is complete.

13.56 MHz CONTACTLESS SMART

		Secure Format	Configurable Format	Card Serial Number Only†
ISO 14443	aptiQ™ MIFARE®	🔒		
	MIFARE® CSN[†]		🔧	
	aptiQ™ MIFARE DESFire™ EV1 with PACSA	🔒		
	MIFARE DESFire™ EV1		🔧	
	FIPS 201-1/PIV II US Government (ie Oberthur® and Gemalto®) must order PIV compliant readers	🔒	🔧	
	DESFire®		🔧	CSN ONLY
ISO 15693	HID iCLASS®			CSN ONLY
	Infineon my-d®			CSN ONLY
	Inside PicoTag™			CSN ONLY
	Texas Instruments Tag-it™		🔧	
	ST Microelectronics®		🔧	

Functionality for FIPS 201/PIV II is in default configuration.

Ingersoll Rand
Security Technologies

877-671-7011 · securitytechnologies.ingersollrand.com

004245 04/13

ALLEGION™

aptiQ™

FIPS 201-1 compliant readers

Overview

aptiQ® smart and multi-technology readers by Allegion have been approved by the U.S. Government under HSPD-12 for FIPS 201-1 compliance as PIV transparent readers. PIV compliance is available on six reader models, including the SM10 smart mini-mullion, MT11 multi-technology mullion, MT15 multi-technology single gang, MTK15 multi-technology single gang with keypad, MTMS15 multi-technology magnetic stripe and MTMSK multi-technology magnetic stripe with keypad.

aptiQ multi-technology readers are a unique and critical component of successful security upgrades in all sectors of the government. FIPS 201-1 is a Federal Information Processing Standard ("FIPS") developed by the National Institute of Standards and Technology ("NIST") to satisfy the requirements of HSPD-12, a Homeland Security Presidential Directive. One of the main objectives of HSPD-12 is to ensure government-wide interoperability for information technology and security through the implementation of a range of federal standards and product requirements. FIPS 201-1 seeks to improve identification and authentication of Federal employees and contractors for access to the federal facilities and information systems.

aptiQ FIPS 201-1 PIV compliant readers are available with multiple data output formats, which provide unprecedented versatility within the PIV & PIV-I specification.

In addition to reading approved FIPS 201-1 PIV & PIV-I credentials, aptiQ smart and multi-technology readers are also compatible with many standard proximity and leading smart card technologies (see specifications). The ability to read multiple existing card types and PIV & PIV-I cards simultaneously is a tremendous benefit to those agencies looking to transition seamlessly from older proximity technologies to new, mandated PIV & PIV-I credentials. A mixed population of old prox credentials and new PIV & PIV-I credentials is unavoidable during the government's multi-year upgrade path to FIPS 201-1 compliance.

Features and benefits

- Compatibility: compatible with industry standard magnetic stripe technology (tracks 1, 2, or 3) and 125 kHz and 13.56 MHz contactless technologies
- Read range: up to 6 inches (proximity), up to 2 inches for PIV & PIV-I credentials
- Tri-state LED (red, green, amber): visual indicator and audio feedback representing status and activity information
- Tamper detection
- Environment: accommodates interior, exterior, metal and non-metal installation environments

Additional features

- Compliance: compatible with applicable ISO standards
- Compatible with all access control systems that support Wiegand format
- Warranty: limited lifetime against defective workmanship and materials
- Additional technologies supported
  - Magnetic stripe
    - Track 1, 2, or 3
  - Proximity
    - Schlage
    - XceedID®
    - HID® Proximity (certain formats)
    - GE/CASI ProxLite™
    - AWID® Proximity
  - Smart card (secure sector only)
    - Schlage
    - aptiQ® using MIFARE® Classic
    - aptiQ using MIFARE DESFire™ EV1
    - FIPS 201-1/PIV & PIV-I
  - Smart card (card serial number only)
    - DESFire® application HID iClass®
    - Inside contactless PicoTag™

Ordering information

- **SM10** - Smart mini-mullion reader
- **MT11** - Multi-technology mullion reader
- **MT15** - Multi-technology single gang reader
- **MTK15** - Multi-technology single gang reader with keypad
- **MTMS15** - Multi-technology magnetic stripe reader
- **MTMSK15** - Multi-technology magnetic stripe reader with keypad

aptiQ PIV readers have been approved by the GSA lab as compliant with FIPS 201-1 and the appropriate PIV credentials.

Please see individual data sheets for each reader for more specific technical information.

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ▪ LCN ▪ SCHLAGE ▪ STEELCRAFT ▪ VON DUPRIN

ALLEGION™

Multi-Technology Readers

Overview

All XceedID® Multi-Technology Readers contain both 125 kHz proximity and 13.56 MHz smart card capability in one unit, making them the most flexible readers in the industry. With the ability to simultaneously read smart and proximity cards, customers are protected from obsolescence in the transition from proximity technology to contactless smart card technology. Even if customers want to continue using proximity technology today, these multi-technology readers offer economical migration to the latest in smart card technology on their budget or timeline.

The smart capability of the multi-technology reader provides higher security when used with a smart credential . Each message between the card and the reader is digitally signed using Message Authentication Coding to ensure the integrity of the data. Additionally, smart reader technology can be used in various applications, including logical access, cashless vending, and cafeteria services.

These readers are compliant with all applicable ISO standards (14443).

Features & Benefits

- Multiple Color Options
- Modular design allows for easy, upgradeable changes in the field
- Manufactured with high-quality UV resistant materials
- Tri-state LED (red, green, amber) provides a visual indicator and audio feedback representing status and activity information
- Accommodates interior, exterior, metal, and non-metal installation environments
- Security/Key Management: several options to ensure the greatest choice between “open” or high credential security
- Lifetime limited warranty against defective workmanship and materials

Base Part Number	XF1100	XF1500	XF 2100	XF 2110
Technology	Multi-Technology 125 kHz Proximity Technology 13.56 Mhz Smart Technology			
Mount	Mullion Reader	Wall Mount Reader	Mid-Range Wall Mount	Mid-Range Wall Mount
FIPS 201 Compliant Model	Yes			
Frequency	125 kHz and 13.56 MHz			
Standard Default Configuration	75 bit PIV			
Standards	ISO 14443 and ISO 15693			
Physical Dimensions (HWD)	5.85″ x 1.72″ x 1.14″ 14.9 cm x 4.3 cm x 2.9 cm	5.1″ x 3.25″ x 0.76″ 12.9 cm x 8.3 cm x 1.9 cm	5.85″ x 4.5″ x 1.45″ 14.9 cm x 11.4 cm x 3.7 cm	5.85″ x 4.5″ x 1.45″ 14.9 cm x 11.4 cm x 3.7 cm
Weight	0.6 lbs		1.1 lbs	
Certifications	FCC Certification Canadian FCC Certification UL 294 Listed R&TTE Directive (15 EU Countries) CE Mark			
Voltage Range	6-16 VDC	5-16 VDC	6-16 VDC	8-16 VDC
Power Supply	Linear DC			
Average Current Requirement	95 mA DC	110 mA DC	95 mA DC	120 mA DC
Peak Current Requirement	254 mA DC	160 mA DC	218 mA DC	215 mA DC
Maximum Read Range*				
125 kHZ:	up to 5″ (12.7cm)	Up to 4.5″ (11.4cm)	up to 6″ (15.24cm)	up to 6″ (15.24cm)
13.56 MHz:	ISO 14443: up to 1.5″ (3.8cm)		ISO 14443 MIFARE Standard: up to 3″ (7.62cm) ISO 14443 DESFire: up to 2.5″ (6.35cm) ISO 15693: up to 6″ (15.24cm)	ISO 14443 MIFARE Standard: up to 3″ (7.62cm) ISO 14443 DESFire: up to 2.5″ (6.35cm) ISO 15693: up to 6″ (15.24cm)
Cable Specification	18 AWG, 5 Conductor Stranded/Shielded			
System Interfaces	Wiegand			
Operating Temperature	-31 to 151F (-35 to 67C)			
Color Options	Black (standard), Gray (optional)			
Additional Technologies Supported**	Schlage Smart and Proximity XceedID Smart and Proximity MIFARE® Secure Sector MIFARE® CSN aptiQ™ Smart Cards using MIFARE DESFire™ EV1 with PASCA DESFire® EV1 CSN (configurable) DESFire® CSN HID® Proximity protocols		HID iClass® CSN Inside Contactless PicoTag® CSN, GE/CASI ProxLite® ST Microelectronics® CSN Texas Instruments Tag-It® Serial Number Phillips I-Code® CSN AWID® Proximity LenelProx®	

** CSN = Card Serial Number

* Maximum read range depends on credential type/form factor and installation conditions

Note: Support for certain technologies requires configuration.

XceedID®

Proximity Card Readers

Overview

XceedID® offers a full line of proximity readers that provide an attractive and cost-effective solution for facilities already using proximity technology or looking to upgrade from more traditional technologies. XceedID proximity readers provide the convenience of 125 kHz proximity technology, and are compatible with most industry leading proximity credentials. These readers are ideal for applications utilizing legacy proximity systems or credentials, as they can easily be integrated into existing 125 kHz access control systems.

Proximity Readers by XceedID operate on a Wiegand interface, are compatible with all industry leading proximity credentials, and are also completely ISO compliant.

Features & Benefits

- Manufactured with high-quality UV resistant materials
- Tri-state LED (red, green, amber) provides visual indicator and audio feedback representing status and activity information
- Accommodates interior, exterior, metal, and non-metal installation environments
- Limited lifetime warranty against defective workmanship and materials

Base Part Number	XF1050	XF1550	XF 2110P-K
Technology	Proximity 125 kHz Proximity Technology		
Mount	Mini-Mullion Reader	Wall Mount	Mid-Range (wall mountable)
FIPS 201 Compliant Model	Not Applicable		
Frequency	125 kHz		
Standards	ISO 14443	ISO 14443 and 15693	
Physical Dimensions (HWD)	4.2″ x 1.72″ x 1.0″ 10.7 cm x 4.3 cm x 2.5 cm	5.1″ x 3.25″ x 0.76″ 12.9 cm x 8.3 cm x 1.9 cm	5.85″ x 4.5″ x 1.45″ 14.9 cm x 11.4 cm x 3.7 cm
Weight	0.6 lbs		1.1 lbs
Certifications	FCC Certification Canadian FCC Certification UL 294 Listed R&TTE Directive (15 EU Countries) CE Mark		
Voltage Range	5-16 VDC		
Power Supply	Linear DC		
Average Current Requirement	110 mA DC		55 mA DC
Peak Current Requirement	160 mA DC		167 mA DC
Maximum Read Range*	Up to 4.5″ (11.4cm)		Up to 6.0″ (15.24 cm)
Cable Specification	18 AWG, 5 Conductor Stranded/Shielded		
System Interfaces	Wiegand		
Operating Temperature	-31 to 151F (-35 to 67C)		
Color Options	Black (standard) Gray (optional)	Black (standard)	Black (standard) Light Gray (optional) Gray (optional)
Additional Technologies Supported	Schlage Proximity XceedID™ Proximity HID® Proximity protocols GE/CASI ProxLite® AWID® Proximity LenelProx®		

* Maximum read range depends on credential type/form factor and installation conditions

Ingersoll Rand
Security Technologies

877-671-7011 • securitytechnologies.ingersollrand.com

XceedID®

Smart Card Readers

Overview

Contactless Smart Card Readers allow your facility to meet the requirements of today while planning for the future. Operating on 13.56 MHz frequency, these Contactless Smart Card Readers by XceedID® provide one of the most advanced identification reader technologies available today. The combination of Contactless Smart Card Readers and smart credentials provides more security, more speed, and more data storage than the more common systems of today.

All Contactless Smart Card Readers by XceedID provide advanced security by supporting all applicable ISO standards (14443). Rather than using open transmission protocols, Schlage smart card readers utilize high security data. Each message between the card and the reader is digitally signed using Message Authentication Coding (MAC) to ensure the integrity of the data.

These readers are an excellent choice for an entirely new installation that does not need to support legacy technology and will simplify administration and strengthen campus security. Additionally, smart reader technology can be used in various applications, such as logical access, cashless vending, and cafeteria services.

Features & Benefits

- Industry standard 13.56 MHz contactless smart card technology
- Compliant with ISO standards
- Manufactured with high-quality UV resistant materials
- Tri-state LED (red, green, amber) provides a visual indicator and audio feedback representing status and activity information
- Accommodates interior, exterior, metal, and non-metal installation environments
- Security/Key Management: several options to ensure the greatest choice between “open” or high credential security
- Lifetime limited warranty against defective workmanship and materials

Base Part Number	XF1060MF	XF1200	XF1560	XF 2200	XF 2210
Technology	13.56 Smart Technology				
Mount	Mini-Mullion Reader	Mullion Reader	Wall Mount Reader	Mid-Range Wall Mount	Mid-Range Wall Mount
FIPS 201 Compliant Model	N/A	Yes	N/A	Yes	Yes
Frequency	13.56 MHz				
Standard Default Configuration	N/A	75 bit PIV	75 bit PIV	75 bit PIV	75 bit PIV
Standards	ISO 14443	ISO 14443 and 15693			
Physical Dimensions (HWD)	4.2″ x 1.72″ x 1.0″ 10.7 cm x 4.3 cm x 2.5 cm	6.07″ x 1.72″ x 1.14″ 15.4 cm x 4.4 cm x 2.9 cm	5.1″ x 3.25″ x 0.76″ 12.9 cm x 8.3 cm x 1.9 cm	6.10″ x 4.55″ x 1.27″ 15.5 cm x 11.6 cm x 3.2 cm	6.10″ x 4.55″ x 1.27″ 15.5 cm x 11.6 cm x 3.2 cm
Weight	0.45 lbs	0.6 lbs	0.6 lbs	1.6 lbs	1.1 lbs
Certifications	FCC Certification Canadian FCC Certification UL 294 Listed R&TTE Directive (15 EU Countries) CE Mark				
Voltage Range	5-16 VDC				
Power Supply	Linear DC				
Average Current Requirement	50 mA DC	65 mA DC	110 mA DC	70 mA DC	110 mA DC
Peak Current Requirement	85 mA DC	80 mA DC	160 mA DC	105 mA DC	140 mA DC
Maximum Read Range*	Up to 2″ (5.1 cm)	Up to 4.0″ (10.2 cm)	Up to 4.5″ (11.4cm)	Up to 4.5″ (11.4cm)	Up to 4.5″ (11.4 cm)
Cable Specification	18 AWG, 5 Conductor Stranded/Shielded				
System Interfaces	Wiegand				
	N/A	RS-485	N/A	RS-485	RS-485
Operating Temperature	-31 to 151F (-35 to 67C)	-31 to 149F (-35 to 65C)	-31 to 151F (-35 to 67C)	-31 to 149F (-35 to 65C)	-31 to 149F (-35 to 65C)
Color Options	Black (standard) Gray (optional)				
Additional Technologies Supported**	MIFARE® Secure Sector MIFARE® CSN DESFire™ CSN HID iClass® CSN Inside Contactless PicoTag® CSN ST Microelectronics® CSN Texas Instruments Tag-It® Serial Number Phillips I-Code® CSN	aptiQ™ Cards using MIFARE® DESFire EV1 with PACSA MIFARE® Secure Sector MIFARE® CSN DESFire™ CSN HID iClass® CSN Inside Contactless PicoTag® CSN ST Microelectronics® CSN Texas Instruments Tag-It® Serial Number Phillips I-Code® CSN			

** CSN = Card Serial Number
* Maximum read range depends on credential type/form factor and installation conditions
Note: Support for certain technologies requires configuration.

Ingersoll Rand
Security Technologies

877-671-7011 • securitytechnologies.ingersollrand.com

CRM2 and CRP2

Enrollment readers

Overview

The CRM2 magnetic stripe credential enrollment reader and the CRP2 Proximity Credential Enrollment Reader are designed to allow easy enrollment of credentials into the Schlage Express access control system. These compact readers eliminate the need for manual data entry, and provide error-free identification and security throughout the workplace. The plug and play functionality provided via a convenient USB connection allows either of these readers to seamlessly integrate with the Schlage Express software. Additionally, the reader allows for keystrokes to be added before and after the card's data, providing flexibility and data customization.

Note: Compatible with Schlage Express version 4.0 and higher

Features and benefits

- CRM2
  - Magnetic stripe reader
  - Reads data from any data track location on the card
  - USB connectivity
  - Plug-and-play functionality
- CRP2
  - Proximity reader
  - USB connectivity
  - Plug-and-play functionality

CRP2 specifications

Typical maximum read range	1.0" – 3.0" (2.5 – 7.6 cm) dependent upon proximity card type and environmental conditions
Dimensions (H x W x D)	3 $^{3}/_{8}$" x 2" x 0.6"
Weight	0.45 lbs (12.7g)
Power supply and interface	USB self-powered
Indicators	Tri-state LED, beeper
Transmit frequency	125 kHz
Operating temperature range	-22° to 150°F (-30° to 65°C)
Operating humidity range	5% to 95% relative humidity, non-condensing
Storage temperature range	-40° to 185°F (-40° to 85°C)
Certifications	FCC, United States; CE Mark Europe, C-tic Australia, RoHS
Warranty	One year for material/workmanship and defects

CRM2 specifications

Desktop dimensions (H x W x D)	3.674" x 1.325" x 1.193" (93.32 x 33.65 x 30.3 mm); Optional base: 3.375" x 3.5" x 0.5" (86 x 89 x 13 mm)
Desktop weight	4.6 oz (136 g); Base: 13 oz (369 g)
Media thickness	0.015" (0.127 mm) to 0.038" (1.14 mm)
Slot width	0.040" (1.0 mm)
Swipe speed	3 to 60 inches per second, bi-directional
Power supply and interface	USB: self-powered; RS-232 [DB9F] model: 5V supplied by either PS/2 keyboard pass-through or USB power tap
Indicators	Tri-state LED, beeper
Operating temperature range	32° to 131°F (0° to 55°C)
Operating humidity range	5% to 95% relative humidity, non-condensing
Storage temperature range	-22° to 158°F (-30° to 70°C)
Cable length	6 foot articulated cable
Operating life	1,000,000 cycles minimum
Warranty	One year for material/workmanship and defects

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

© 2015 Allegion
005132, Rev. 08/15
www.allegion.com/us

ALLEGION™

SCHLAGE®

KP212, KP232 and KP2000

KP212 and KP232

Mullion mounted keypad series

The mullion keypad series is a standalone solution and is ideal for controlling electrified door hardware such as electric strikes or electromagnetic locks. The sleek design allows easy installation, mounting directly to mullion. Designed with backlit keys and weather resistant, they are well suited for both indoor and outdoor applications.

The mullion stile readers can be programmed to accept up to 120 user codes, are equipped with a Form C, dry contact relay and can be released by using a momentary request-to-exit switch.

The KP232 is designed to meet most residential, commercial, and industrial single door access control needs, and has two inputs and four outputs and factory set access control. The KP232 is a back-to-back keypad application, coming with two keypads. One keypad must be wired on the inside of the door and one must be wired on the outside of the door, creating an in and out reader setup.

KP2000

Single gang flush mount

The KP2000 series single gang flush mount keypads manage up to 500 users and provide complete access control functionality including monitoring door position, controlling locking hardware, triggering propped or forced alert or alarm shunt output. Other applications for the KP2000 series keypads include: controlling electronic devices such as handicapped doors, gate controls, alarm systems, ATM vestibules, and other types of machinery requiring momentary or latched outputs.

You can select between two modes of functionality with the KP2000 series keypads. They can operate most Wiegand access system controllers, or as standalone access control devices.

The KP2000 Series comes in two different styles: the “e” style and the “eM” style. The “e” style keypad uses hardened backlit keys while the “eM” style uses a durable metal keypad including Braille alpha-numeric keys. The KP2000 series can be used in interior and exterior applications. The flush-mount keypads are constructed to meet your aesthetic needs while ensuring long-term durability and high-quality performance.

Features and benefits

- KP212 and KP232
  - Up to 120 users
  - Illuminated hardened keys
  - Sounder
  - Doorbell relay
  - Weather resistant
  - Programmable 00-99 second relay activation time
  - Remote trigger input (REX)
  - Bell output (timed or continuous)
  - Applications:
    - Heavy traffic
    - Indoor/outdoor
- KP2000
  - Features and benefits on back

Reader specifications

Feature set	KP212	KP232	KP2000E	KP2000EM
Mounting	Mullion	Mullion	Single gang/flush	Single gang/flush
Users	120	120	500	500
PIN length	1-6 digits	1-6 digits	1-10 digits	1-10 digits
Duty cycles	Medium	Medium	Medium	Heavy-duty
Back light	Yes	Yes	Yes	No
Keys	Hard plastic	Hard plastic	Heavy-duty plastic	Heavy-duty metal with braille
Weather resistant	Indoor/outdoor	Indoor/outdoor	Indoor/outdoor	Indoor/outdoor
Doorbell key	Yes	Yes	No	No
Wiegand output	No	No	No	No
Remote trigger (REX)	Yes	Yes	Yes	Yes
Access control functionality	Programmable relay activation time (0-99 seconds). Perfect for electric or magnetic locks requiring momentary control.	4 dedicated relay outputs (lock release, door forced, door propped and alarm shunt . Plastic keypad acts as controller. Metal keypad communicates to controller.)	Monitors DPS, controls various electronic hardware, triggers door propped, forced door alert or alarm shunt	Monitors DPS, controls various electronic hardware, triggers door propped, forced door alert or alarm shunt
Relays	2 relays (main and aux)	Main, prop door, forced door and alarm shunt relay	2 Form C	2 Form C
Outputs	2 independent (configurable)	4 independent (dedicated)	2 independent	Programmable
Finish	Aluminum	Aluminum and plastic	Aluminum	Aluminum
UL 294	No	No	Yes	Yes

- KP2000 features
  - 500 users
  - Door position input
  - Request-to-exit input
  - 2 Form C SPDT relay outputs – default for access control function
  - Sounder for key press and alert conditions
  - Option for secure installation with control electronics in protected area
  - Widest array of user type options including single use and two man rule
  - 10-30 VDC and 12-24 VAC operation
  - Over-voltage protection for reliable operation
  - Single-gang flush mount design
  - Indoor/outdoor use
  - Keypad programmable
  - Key press feedback via sounder and yellow LED
  - Built-in assignable sounder
  - Bi-color red/green LED indicates relay status

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

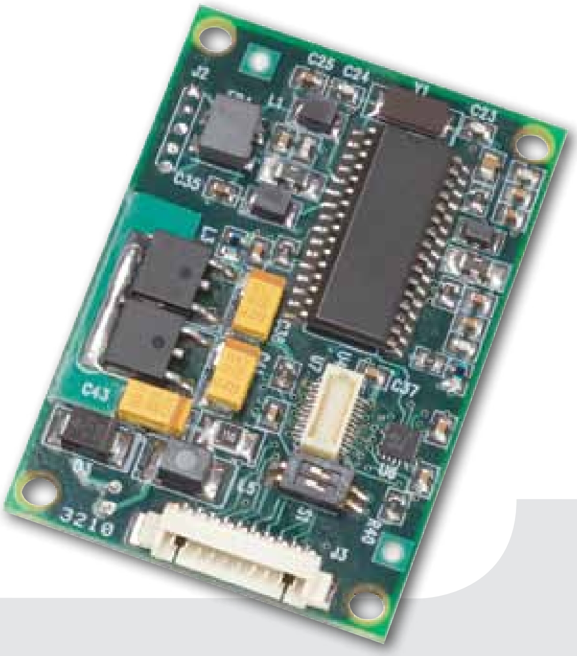
aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

© 2015 Allegion
005000, Rev. 08/15
www.allegion.com/us

aptiQ™

OEM100 Module



Overview

The OEM100 module is an embeddable RFID reader component useful for manufacturers creating custom RFID products.

The OEM100 module contains both 125 kHz proximity, 13.56 MHz contactless smart card capability and supports ISO Standard 14443 technologies.

The OEM100 module provides compatibility with certain HID® proximity protocols GE/CASI ProxLite®, AWID®, LenelProx, and many 13.56 MHz technologies including aptiQ™ smart cards featuring MIFARE DESFire™ EV1 and MIFARE®.

By offering 125 kHz and 13.56 MHz technology in a single compact reader module, the Ingersoll Rand OEM100 module gives a product the flexibility to be used in many of the most popular credential technology environments.

Features & Benefits

- 125 kHz frequency
- 13.56 MHz frequency
- Supports the most popular proximity and smart card formats on the market today

Ingersoll Rand
Security Technologies

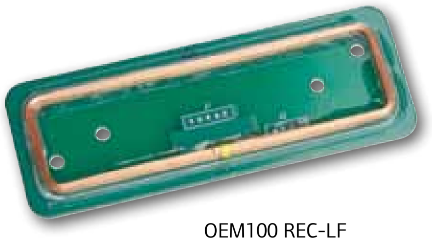
OEM100 Specifications

Dimensions	Main Logic Board Antenna Board #1 HG Rectangular Antenna Board #2 Square	1.4″ x 2.05″ x 0.315″ (35.6mm x 52.1mm x 8mm) 1.35″ x 3.6″ x 0.2″ (34.3mm x 91.4mm x 5.1mm) 2.85″ x 2.83″ x 0.2″ (72.4mm x 71.9mm x 5.1mm)
125kHz Technologies	GE/CASI ProxLite® HID® Proximity AWID® Proximity LENEL® Proximity	
13.56MHz Technologies	ISO 14443 aptiQ™ featuring MIFARE DESFire™ EV1 (with PACSA enabled) ISO 14443 Secure MIFARE® Classic ISO 14443 PIV (FASC-N output options) ISO 14443 PIV-1 (GUID output options) CSN for HID iClass®, ISO 15693, ISO 14443	

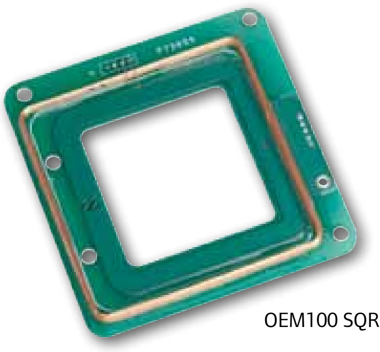
Card	**Card Type**	**Read Range**
125kHz	ASK, FSK	Up to 4.5″(11.4 cm)
13.56MHz	ISO 15693	Up to 3.0″ (7.6 cm)
13.56MHz	ISO 14443A MIFARE® Standard	Up to 2.0″ (5.1 cm)
13.56MHz	ISO 14443A aptiQ™ smart cards featuring MIFARE DESFire™ EV1	Up to 1.5″ (3.8 cm)

Electrical Specifications	Operating Temperature: -31 to 149 F (-35 to 65 C) Frequency: 125kHz and 13.56MHz Voltage Input: 5-16V Average System Current: 95 mAmps (180 mAmps max) Communication: Wiegand, RS485, or UART-TTL

ANTENNA OPTIONS:



OEM100 REC-LF



OEM100 SQR-LF

ORDERING INFORMATION

OEM100 REC-LF - OEM100 Module + HG Antenna (Rectangular Antenna)

OEM100 SQR-LF - OEM100 Module + OEM Antenna (Square 2x2 Antenna)

Ingersoll Rand
Security Technologies

SCHLAGE

SEKPDWG and SEKPDMWG

Electronic keypads

Overview

The fully encapsulated electronic keypad can be used by itself or next to another reader device for additional security. Its stainless steel construction is ideal for indoor or outdoor applications. The two designs, single gang box or the mullion mount style, give it the diversity needed for any application.

Features and benefits

- Field selectable keypad configurations
- SEKPDWG mounts directly to a single gang electrical box
- SEKPDMWG mounts to any mullion style frame
- No moving parts to replace

Specifications	
Dimensions	SEKPDWG: 5.125" x 3.375" x .437" SEKPDMWG: 7.125” x 1.75” x .75”
Power supply	5-12 VDC (field selectable)
Operating temperature	-40º F to 160º F
Weight	SEKPDWG: 16 oz SEKPDMWG: 4.4 oz
Material	316L stainless steel
Standby current draw	SEKPDWG: 5V-20mA, SEKPDMWG: 5V-20mA

Ordering information

- **SEKPDWG** - Single gang style keypad
- **SEKPDMWG** - Mullion style keypad
- **SEKPD8B** - Mullion style keypad (8 bit)

Note: Specify 5V or 12V

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

004252, Rev. 08/15
www.allegion.com/us

ALLEGION™

SCHLAGE®

SERIII-W

Scramble keypad

Overview

The SERIII scramble keypad is a keypad reader designed to prevent onlookers from detecting the PIN code being entered. The LED's display a randomly allocated set of numbers from 0 to 9. The position of the numbers change every time the keypad is activated. Only the user standing directly in front of the keypad can see the scrambled digits.

Features and benefits

- Very narrow viewing angle of the lighted, scrambled digits
- The membrane keypad is extremely durable
- Random allocation of digits ensures even wear to the keys
- Individual PIN codes can be up to 9 digits in length
- The SERIII has a weatherproof rating of IP65
- An audible alarm signals when a button is depressed
- Robust polycarbonate enclosure
- The unit is equipped with power-up diagnostics and self-test routine
- The SERIII is provided with Wiegand communication protocol
- Over 3.6 million unique permutations are available
- Terminal connection on the rear of the unit

Specifications

Dimensions	5.39" x 4.17" x 2.05"
Input voltage	8 - 12 VDC
Input current	500mA max.
Operating temperature	5º F to 122º F
Weight	16.76 oz
Cable distance (Wiegand)	500' with 22AWG 6 conductor stranded with overall shield

Ordering information

- **SERIII-W-GR** - Scramble keypad (gray)
- **SERIII-W-BLK** - Scramble keypad (black)

- **SMK-2-GR** - Scramble keypad surface mount kit (gray)
- **SMK-2-BLK** - Scramble keypad surface mount kit (black)
- **SSMK-2-ADA** - Scramble keypad surface mount kit (ADA compliant)

- **PMK-2-GR** - Panel mount kit (gray)
- **PMK-2-BLK** - Panel mount kit (black)
- **SPMK-2-GR** - Panel mount kit with steel back box (gray)
- **SPMK-2-BLK** - Panel mount kit with steel back box (black)

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

SMR10 and SMR20

Magnetic stripe readers

Overview

The SMR10 and SMR20 stripe readers have a slim, mullion style design. The die cast metal housing makes it ideal for indoor or outdoor applications. The SMR20 has a 12 position membrane style keypad.

Features and benefits

- Rugged metal housing
- All stainless steel hardware is standard
- Audiovisual indication provides two LED's (red/green) and beeper sounds
- Static discharge protection
- Accepts low or high coercivity-magnetic cards
- Standard track 2 encoding (track 1 and 3 are available)
- One security screw mounting
- Supports Wiegand or Clock & Data interface formats via dip switches

Specifications

Dimensions (W x H x L)	1.95" x 1.3" x 5.5"
Power requirements	5 or 12 VDC
Power consumption	20 mA at 12 VDC
Operating temperature	-40° F to 170° F
Weight	10 oz
Cable distance	500' with 18AWG 6 conductor stranded with overall shield

Ordering information

- **SMR10-5V-BLK** - 5 VDC standard, magnetic stripe card reader (black)
- **SMR10-5V-BG** - 5 VDC standard, magnetic stripe card reader (beige)
- **SMR10-12V-BLK** - 12 VDC magnetic stripe card reader (black)
- **SMR10-12V-BG** - 12 VDC magnetic stripe card reader (beige)
- **SMR20-5V-BLK** - 5 VDC standard, magnetic stripe card reader with keypad (black)
- **SMR20-5V-BG** - 5 VDC standard, magnetic stripe card reader with keypad (beige)
- **SMR20-12V-BLK** - 12 VDC magnetic stripe card reader with keypad (black)
- **SMR20-12V-BG** - 12 VDC magnetic stripe card reader with keypad (beige)

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

ALLEGION™

SCHLAGE®

SMR5

Magnetic stripe reader

Overview

The SMR5 Mercury magnetic stripe reader has a slim, mullion style design. The die cast metal housing makes it ideal for indoor or outdoor applications.

Features and benefits

- Rugged metal housing
- All stainless steel hardware is standard
- Audiovisual indication provides multicolor LED (red/green) and beeper sounds
- Static discharge protection
- Accepts low or high coercivity-magnetic cards
- Standard track 2 encoding (track 1 and 3 are available)
- One security screw mounting
- Supports Wiegand or Clock & Data interface formats

Specifications

Dimensions (W x H x L)	1.95" x 1.3" x 5.5'
Power requirements	5 or 12 VDC
Power consumption	20 mA at 12 VDC
Operating temperature	-40º F to 170º F
Weight	10 oz
Cable distance	500' with 18AWG 6 conductor stranded with overall shield

Ordering information

- **SMR5-5V-BLK** - 5 VDC magnetic stripe card reader (black)
- **SMR5-5V-BG** - 5 VDC magnetic stripe card reader (beige)
- **SMR5-12V-BLK** - 12 VDC magnetic stripe card reader (black)
- **SMR5-12V-BG** - 12 VDC magnetic stripe card reader (beige)

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

ALLEGION™

aptiQ™

MT20

Multi-technology enrollment reader with ENGAGE™ technology

Overview

The aptiQ™ MT20 USB multi-technology enrollment reader with ENGAGE™ technology is designed to simplify your enrollment process. The MT20 simplifies the enrollment of proximity, smart or mobile credentials in an access control system by using a computer's USB connection. The MT20 does not require software to operate when using a USB connection and will function on any operating system. When using the ENGAGE Web Application, the MT20 will automatically output the data in the expected format. The USB connection emulates a keyboard and will keystroke the facility code and badge ID from the credential to the cursor's location on the screen.

The MT20 is compatible with aptiQ smart credentials (MIFARE® Classic and MIFARE DESFire™ EV1), aptiQmobile™ credentials and most proximity credentials.

Features and benefits

- Use your computer and the ENGAGE web app to easily enroll credentials in your access control system
- Recognizes aptiQ smart credentials (MIFARE® Classic and MIFARE DESFire™ EV1), aptiQmobile credentials and most proximity credentials
- Limited Lifetime Warranty

Model	MT20
Reader type	USB
Software and operating system requirements	N/A - USB
Bit formats recognized	26A, 32X, 34N, 34S, 35C, 37X, 37H, 40X
Technologies supported	Schlage Proximity XceedID™ Proximity HID® Proximity GE/CASI ProxLite® AWID® Proximity LenelProx® Schlage MIFARE® Secure Sector XceedID™ MIFARE® Secure Sector aptiQ™ Smart Cards using MIFARE DESFire™ EV1 with PACSA DESFire® CSN HID iClass® CSN Inside Contactless PicoTag® CSN ST Microelectronics® CSN Texas Instruments Tag-It® Serial Number Phillips I-Code® CSN
Physical dimensions (l x w x h)	5.56" x 2.00" x .695"
Operating temperatures	0 to 40 C
Weight	4.1 oz
Power supply	Connect to powered USB port or via USB power supply
Interface	USB
Current requirement	160 mA
Default configuration	CE-401-073, for use with ENGAGE web applicaton
Octal output	CE-401-061, for use with SMS Express
FC/BID output	CE-401-060 (SUSB89 default,) for use as keystroke emulator
BID only	CE-401-069, for use as keystroke emulator

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

ALLEGION™

aptiQ™

aptiQ®

Multi-technology readers

Overview

aptiQ multi-technology readers by Allegion are designed to simplify your access control solutions. Transition your system from proximity to smart card technology at your own pace without having to change out readers as new technologies are available. aptiQ readers handle all applicable ISO standards (14443A, 14443B, 15693), are FIPS 201-1 compliant and are versatile enough to read 125kHz proximity and 13.56MHz contactless smart cards in a single unit. aptiQ multi-technology readers interface with aptiQ smart credentials (MIFARE® Classic and MIFARE DESFire™ EV1) and can read the card serial numbers of a variety of smart cards from other manufacturers, making your next upgrade in technology simple and seamless. Additionally, aptiQ readers are already NFC compatible and able to communicate with NFC-enabled phones whenever you're ready to take that step.

aptiQ multi-technology readers use an open architecture platform designed to work with industry standards and common access control system interfaces. Multiple aptiQ reader form factors are designed to fit a variety of placement needs, with an attractive modern design which will complement any facility's architecture and décor. aptiQ readers are very easy to install with the quick-connect design and a standard wiring color scheme that most technicians are already accustomed to. But if you do have questions, you'll never worry about lack of service or assistance. As always, our knowledgeable sales and support staff is ready to assist you with any design or technology questions you may have.

Note: Magnetic stripe multi-technology readers also available.

Features and benefits

- Accommodates interior, exterior, metal, and non-metal installation environments
- Recognizes most proximity credentials, and aptiQ smart credentials (MIFARE® Classic and MIFARE DESFire™ EV1)
- FIPS 201-1 compliant
- NFC compatible, reads aptiQmobile™ credentials
- Quick-connect design for easy installation
- Simple wiring – color scheme is identical to most readers in the market
- Easy-to-install mounting bracket
- Tri-state LED (red, green, amber) visual indicator and audio feedback representing status and activity information, easily discernible for the audibly or visually impaired
- Wiegand output for simple interface with most access control panels
- Multiple reader cover color options
- Limited lifetime warranty
- Multi-technology readers may also be ordered with RS-485 capability

Model*	PR10	SM10	MT11	MT15	MTK15
Reader type	Proximity mini-mullion*	Smart mini-mullion*	Multi-technology mullion	Multi-technology single gang	Multi-technology single gang keypad
Frequency	125 kHz	13.56 MHz	13.56 MHz and 125 kHz		
FIPS 201-1 compliant	No	Yes			
Standard default PIV output	N/A	75 bit PIV**			
Standards	N/A	ISO 14443A, 14443B, 15693			
Certifications	FCC Certification • IC Certification • UL 294 Listed • R&TTE Directive (15 EU Countries) • CE Mark • IP65				
Voltage range	5-16 VDC				
Power supply	Linear DC				
Current requirement (at 12 VDC and 25 C; mAmps)	Avg. 65 mA Peak 110 mA	Avg. 95 mA Peak 195 mA	MT11 Avg. 100 mA Peak 170 mA MT11-485 Avg. 115 mA Peak 145 mA	MT15 & MT15-485 Avg. 120 mA Peak 200 mA	MTK15 and MTK15-485 Avg. 120 mA Peak 230 mA
Read range	Proximity: Up to 3" (7.5 cm)	MIFARE: Up to 3" (7.5 cm) DESFire EV1: Up to 2" (5.1 cm)	Proximity: Up to 5" (12.7 cm) MIFARE: Up to 4" (10 cm)	Proximity: Up to 5" (12.7 cm) MIFARE: Up to 4" (10 cm)	DESFire EV1: Up to 2" (5.1 cm) PIV credential: Up to 2.5" (6.5 cm)
Cable specification	18 AWG, 5 conductor stranded/shielded				
System interfaces	Wiegand	Wiegand / Clock & Data	Wiegand / Clock & Data / RS-485*** (OSDP)		
Cabling distance	Wiegand output: 500 ft. (152 m)				
Physical dimensions (H x W x D)	4.26" x 1.72" x 0.81" 10.8 cm x 4.4 cm x 2.1 cm	4.26" x 1.72" x 0.81" 10.8 cm x 4.4 cm x 2.1 cm	5.91" x 1.72" x 0.81" 15 cm x 4.4 cm x 2.1 cm	5.1" x 3.25" x 0.76" 12.9 cm x 8.3 cm x 1.9 cm	5.1" x 3.25" x 0.76" 12.9 cm x 8.3 cm x 1.9 cm
Operating temperatures	-40º to 158ºF (-40º to 70ºC)				
Weight	4.1 oz	3.9 oz	5.7 oz	9.1 oz	9.3 oz
Material	PBT Polymer				
Technologies supported in default mode					
Schlage Proximity	■		■	■	■
XceedID™ Proximity	■		■	■	■
HID® Proximity	■		■	■	■
GE/CASI ProxLite®	■		■	■	■
AWID® Proximity	■		■	■	■
LenelProx®	■		■	■	■
aptiQmobile		■	■	■	■
Schlage MIFARE®		■	■	■	■
XceedID MIFARE®		■	■	■	■
aptiQ smart cards using MIFARE™ Classic		■	■	■	■
aptiQ smart cards using MIFARE DESFire™ EV1		■	■	■	■
DESFire® CSN		■	■	■	■
HID iCLASS® CSN		■	■	■	■
Inside Contactless PicoTag® CSN		■	■	■	■
ST Microelectronics® CSN		■	■	■	■
Texas Instruments Tag-It® CSN		■	■	■	■
Phillips I-Code® CSN		■	■	■	■

Color options

■	Black (standard)	■	Cool tone gray
□	Cream	■	Warm tone brown

* Some features and benefits listed on the front may not be applicable to the smart-only and proximity-only readers.

** Other output options available through configuration.

*** RS-485 model numbers include "-485" after the original model number. For example, MT11-485 is the RS-485 version of the multi-technology mini-mullion reader. Multi-drop, Open Standard Device Protocol (OSDP).

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

aptiQ™

aptiQ®

Multi-technology magnetic stripe readers

Overview

aptiQ multi-technology magnetic stripe readers by Allegion are designed to simplify your access control solutions. Transition your system from an existing population of magnetic stripe cards to more secure smart card technology at your own pace. aptiQ multi-technology readers are versatile enough to read magnetic stripe, 125 kHz proximity, and 13.56MHz contactless smart cards in a single unit, handle all applicable ISO standards (14443A, 14443B, 15693), and are FIPS 201-1 compliant. aptiQ multi-technology magnetic stripe readers interface with aptiQ smart credentials (MIFARE® Classic and MIFARE® DESFire™ EV1), and can read the card serial numbers of a variety of smart cards from other manufacturers, making your next upgrade in technology simple and seamless. Additionally, aptiQ readers are already NFC compatible and able to communicate with NFC-enabled phones whenever you're ready to take that step.

aptiQ multi-technology magnetic stripe readers use an open architecture platform designed to work with industry standards and common access control system interfaces. And with an attractive modern design they'll complement any facility's architecture and décor. aptiQ readers are very easy to install with the quick-connect design and a standard wiring color scheme that most technicians are already accustomed to. But if you do have questions, you'll never worry about lack of service or assistance. As always, our knowledgeable sales and support staff is ready to assist you with any design or technology questions you may have.

Features and benefits

- Accommodates interior, exterior, metal, and non-metal environments
- Recognizes magnetic stripe credentials, most proximity credentials, and aptiQ smart credentials (MIFARE® Classic and MIFARE DESFire™ EV1)
- FIPS 201-1 compliant
- NFC compatible, reads aptiQmobile™ credentials
- Quick-connect cable for easy installation
- Simple wiring – color scheme is identical to most readers in the market
- Easy-to-install mounting bracket
- Tri-state LED (red, green, amber) visual indicator and audio feedback representing status and activity information, easily discernible for the audibly or visually impaired
- Wiegand or RS-485 output for simple interface with most access control panels
- Multiple reader cover color options
- Limited lifetime warranty
- Magnetic stripe track 2 default, tracks 1 and 3 configurable

Model	MTMS15	MTMSK15
Reader type	Multi-technology magnetic stripe	Multi-technology magnetic stripe with keypad
Frequency	13.56MHz, 125 kHz, and magnetic stripe	13.56MHz, 125 kHz, and magnetic stripe
FIPS 201-1 compliant	Yes	Yes
Standard default PIV output	75 bit PIV*	75 bit PIV*
Standards	ISO 14443A, 14443B, 15693	ISO 14443A, 14443B, 15693
Certifications	FCC certification · IC certification · UL 294 Listed · R&TTE directive (15 EU countries) · CE mark · IP65	FCC certification · IC certification · UL 294 Listed · R&TTE directive (15 EU countries) · CE mark · IP65
Voltage range	5-16 VDC	5-16 VDC
Power supply	Linear DC	Linear DC
Current requirement (at 12 VDC and 25 C; mAmps)	MTMS15 and MTMS15-485 Avg. 120mA Peak 200mA	MTMSK15 and MTMSK15-485 Avg. 120mA Peak 230mA
Read range	Proximity: up to 5" (12.7 cm) MIFARE: up to 4" (10 cm) DESFire EV1: up to 2" (5.1 cm) PIV credential: up to 2.5" (6.5 cm)	Proximity: up to 5" (12.7 cm) MIFARE: up to 4" (10 cm) DESFire EV1: up to 2" (5.1 cm) PIV credential: up to 2.5" (6.5 cm)
Cable specification	18 AWG, 5 conductor stranded/shielded	18 AWG, 5 conductor stranded/shielded
System interfaces	Wiegand / Clock & Data / RS-485** (OSDP)	Wiegand / Clock & Data / RS-485** (OSDP)
Cabling distance	Wiegand output: 500 ft (152 m)	Wiegand output: 500 ft (152 m)
Physical dimensions (H x W x D)	4.43” x 5.17” x 1.15” 11.25 cm x 13.13 cm x 2.92 cm	4.43” x 5.17” x 1.15” 11.25 cm x 13.13 cm x 2.92 cm
Operating temperatures	-31º to 151ºF (-35 to 67ºC)	-31º to 151ºF (-35 to 67ºC)
Weight	8.9 oz	9.5 oz
Material	PBT polymer	PBT polymer
Technologies supported in default mode		
Magnetic stripe (tracks 1, 2, or 3)***	■	■
Schlage Proximity	■	■
XceedID® Proximity	■	■
HID® Proximity	■	■
GE/CASI ProxLite®	■	■
AWID® Proximity	■	■
LenelProx®	■	■
Schlage MIFARE®	■	■
XceedID MIFARE®	■	■
aptiQmobile	■	■
aptiQ smart cards using MIFARE® Classic	■	■
aptiQ smart cards using MIFARE DESFire™ EV1	■	■
DESFire® CSN	■	■
HID iClass® CSN	■	■
Inside Contactless PicoTag® CSN	■	■
ST Microelectronics® CSN	■	■
Texas Instruments Tag-It® CSN	■	■
Phillips I-Code® CSN	■	■

Color options

■	Black (standard)	■	Cool tone gray
□	Cream	■	Warm tone brown

* Other output options available through configuration.

** RS-485 model numbers include “-485” after the original model number. For example, MTMS15-485 is the RS-485 version of the multi-technology mini-mullion reader. Multi-drop, Open Standard Device Protocol (OSDP).

*** By default, the MTMS15 and MTMSK15 readers will read track 2 of the magnetic strip. If you require the ability to read track 1 or track 3, please contact technical support at 1-877-671-7011 for configuration options.

† Lead time may apply for non-standard colors

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

009209, Rev. 08/15
www.allegion.com/us

aptiQ™ advantages

When you choose aptiQ readers and credentials from Allegion, you're making the right decision. We offer unique advantages that help your business thrive and make doing business easier.

24 HOUR shipments

Standard orders of cards and readers are shipped in 24-48 hours.

FAIR pricing

No upcharges for services that should come standard...like CardTrax™ and our standard composite material cards that eliminate warping from high-heat printers.

QUALITY assurance

Quality control measures, advanced equipment and technology, and a no-fault replacement policy protect your investment.

WARRANTY limited lifetime[1]

Know you're protected against defects in materials and workmanship under normal use and service.

OPEN architecture

We secure our access control application sector, but the rest of the sectors are open for you to work with any company you choose.

MOBILE solutions today

With aptiQmobile™, your customers can use their NFC-enabled smart phone just like an ID card, and in many cases without replacing your existing readers.

aptiQ advantages

CARDTRAX
card number tracking services

Ensure facility code and badge ID combinations are unique and never duplicated on any other cards we make. Compatible with Corporate 1000™.

SECURE
highest encryption available

aptiQ credentials using MIFARE DESFire™ EV1 offer our highest level of security through the use of mutual authentication, key diversification, and encryption.

CUSTOM
programming

Program any smart cards and readers with your custom key format and proprietary bit format.

ENGRAVING
permanent laser

Permanently label ISO and clamshell cards with badge ID information, logos, pictures and text.

Use aptiQ readers along with aptiQ credentials

- Simple lineup with only 7 SKUs but all of the technology options you need
- Available in Wiegand and RS-485
- All readers are FIPS 201-1 by default
- Multi-technology allows for easy transitions from one technology to the next
- Create your own reader label with the custom reader label program
- Color options and custom covers available

[1] Warranty periods different for networked reader keypads, networked magnetic striped read heads, and magnetic stripe credentials.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises 27 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

010353, Rev. 05/14
www.allegion.com/us

ALLEGION™

aptiQ™

FIPS 201-1 compliant readers

Overview

aptiQ® smart and multi-technology readers by Allegion have been approved by the U.S. Government under HSPD-12 for FIPS 201-1 compliance as PIV transparent readers. PIV compliance is available on six reader models, including the SM10 smart mini-mullion, MT11 multi-technology mullion, MT15 multi-technology single gang, MTK15 multi-technology single gang with keypad, MTMS15 multi-technology magnetic stripe and MTMSK multi-technology magnetic stripe with keypad.

aptiQ multi-technology readers are a unique and critical component of successful security upgrades in all sectors of the government. FIPS 201-1 is a Federal Information Processing Standard ("FIPS") developed by the National Institute of Standards and Technology ("NIST") to satisfy the requirements of HSPD-12, a Homeland Security Presidential Directive. One of the main objectives of HSPD-12 is to ensure government-wide interoperability for information technology and security through the implementation of a range of federal standards and product requirements. FIPS 201-1 seeks to improve identification and authentication of Federal employees and contractors for access to the federal facilities and information systems.

aptiQ FIPS 201-1 PIV compliant readers are available with multiple data output formats, which provide unprecedented versatility within the PIV & PIV-I specification.

In addition to reading approved FIPS 201-1 PIV & PIV-I credentials, aptiQ smart and multi-technology readers are also compatible with many standard proximity and leading smart card technologies (see specifications). The ability to read multiple existing card types and PIV & PIV-I cards simultaneously is a tremendous benefit to those agencies looking to transition seamlessly from older proximity technologies to new, mandated PIV & PIV-I credentials. A mixed population of old prox credentials and new PIV & PIV-I credentials is unavoidable during the government's multi-year upgrade path to FIPS 201-1 compliance.

Features and benefits

- Compatibility: compatible with industry standard magnetic stripe technology (tracks 1, 2, or 3) and 125 kHz and 13.56 MHz contactless technologies
- Read range: up to 6 inches (proximity), up to 2 inches for PIV & PIV-I credentials
- Tri-state LED (red, green, amber): visual indicator and audio feedback representing status and activity information
- Tamper detection
- Environment: accommodates interior, exterior, metal and non-metal installation environments

Additional features

- Compliance: compatible with applicable ISO standards
- Compatible with all access control systems that support Wiegand format
- Warranty: limited lifetime against defective workmanship and materials
- Additional technologies supported
  - Magnetic stripe
    - Track 1, 2, or 3
  - Proximity
    - Schlage
    - XceedID®
    - HID® Proximity (certain formats)
    - GE/CASI ProxLite™
    - AWID® Proximity
  - Smart card (secure sector only)
    - Schlage
    - aptiQ® using MIFARE® Classic
    - aptiQ using MIFARE DESFire™ EV1
    - FIPS 201-1/PIV & PIV-I
  - Smart card (card serial number only)
    - DESFire® application HID iClass®
    - Inside contactless PicoTag™

Ordering information

- **SM10** - Smart mini-mullion reader
- **MT11** - Multi-technology mullion reader
- **MT15** - Multi-technology single gang reader
- **MTK15** - Multi-technology single gang reader with keypad
- **MTMS15** - Multi-technology magnetic stripe reader
- **MTMSK15** - Multi-technology magnetic stripe reader with keypad

aptiQ PIV readers have been approved by the GSA lab as compliant with FIPS 201-1 and the appropriate PIV credentials.

Please see individual data sheets for each reader for more specific technical information.

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

© 2015 Allegion
004256, Rev. 08/15
www.allegion.com/us

ALLEGION

aptiQ

Reader accessories

for aptiQ® readers

Overview

aptiQ multi-technology readers by Allegion are designed to simplify your access control solutions. A variety of accessories and replacement parts are available to ensure your readers are always performing well.

Reader covers

Replacement reader covers can be used to replace faded or cracked covers and to change the color of your readers along with any updates to the facility's décor. We offer four color options — black, cream, cool tone gray, and warm tone brown.

Cosmetic backplate covers

While replacing legacy readers with aptiQ readers, the footprint of the legacy reader may be larger than that of the new reader. Cosmetic backplate covers accommodate this issue. Available in three sizes, our cosmetic backplate covers are designed to cover holes and unpainted areas that you do not wish to invest time and money to repair.

Quick-connect cable

The quick connect cable allows the installer to connect the necessary reader wires without the hassle of a reader case hanging off the other end. Simply connect the wiring harness and plug the reader in, it's that easy. Every reader already comes with a quick-connect cable, but you can order the cable separately if you need extras.

Other accessories

Following repeated use, the magnetic stripe read head in a reader can wear down. We offer a replacement magnetic stripe read head for our aptiQ multi-technology magnetic stripe readers.

Reader mounting backplates are designed as a quick mounting bracket for a simplified installation process. Every reader comes with a reader backplate, but you can also order these separately if you need replacements and extras.

Reader covers

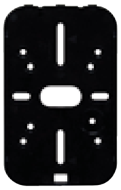
Color options

■	Black (standard)	■	Cool tone gray
□	Cream	■	Warm tone brown

Cosmetic backplate covers

Quick-connect cable

Part number	Black	23846520	23846553	23846587	23846611	24064149	24064198
	Brown	23846546	23846579	23846603	23846637	24064156	24064206
	Gray	23846538	23846561	23846595	23846629	24064172	24064222
	Cream	23920648	23920655	23920598	23920606	24064164	24064214
Corresponding reader model		PR10 and SM10	MT11	MT15	MTK15	MTMS15	MTMSK15
Reader type		Mini-mullion	Mullion	Single gang	Single gang with keypad	Magnetic stripe	Magnetic stripe with keypad
Dimensions		4.26" x 1.72" x 0.81"	5.91" x 1.72" x 0.81"	5.1" x 3.25" x 0.76"	5.1" x 3.25" x 0.76"	4.43" x 5.17" x 1.15"	4.43" x 5.17" x 1.15"
Material		PNT polymer	PNT polymer	PNT polymer	PNT polymer	PNT polymer	PNT polymer



Part	Cosmetic backplate cover		Quick connect cable/ pigtail – 18 inch	Magnetic stripe read head	Mounting backplate	
Part number	Mini-mullion/ mullion	CP-11	23846462	21074009	Mini-mullion	23846355
					Mullion	23846397
	Single gang	CP-15			Single gang	23846439
	Mid range	CP-21			Magnetic stripe	24152654
Dimensions	Mini-mullion/ mullion	6.70" x 2.50"	N/A	N/A	5.1" x 3.25" x 0.76"	
	Single gang	5.65" x 3.85"				
	Mid-range	6.45" x 5.50"				

Color options

⬛	Black (standard)	■	Cool tone gray
□	Cream	■	Warm tone brown

Allegion, the Allegion logo, and aptiQ, are trademarks of Allegion plc, its subsidiaries and/or affiliates in the United States and other countries. All other trademarks are the property of their respective owners.

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

© 2015 Allegion
009621, Rev. 08/15
www.allegion.com/us

Reader Conversion Chart

Legacy model to aptiQ™ model

The new line of contactless readers from Ingersoll Rand Security Technologies simplifies your decision-making and ordering process. The new models provide increased performance, have a modern design, and offer a variety of technological capabilities with smart, proximity, and multi-technology options. Use the chart below to easily identify which new reader is the best replacement for each legacy reader.

Legacy Models (Schlage/XceedID)				Model Conversion		
Model #	Description			Model #	Description	
(S)XF1050	Proximity Mini-Mullion		▶	PR10	XceedID Proximity Mini-Mullion	
(S)XF1060MF	Smart Mini-Mullion		▶	SM10	aptiQ™ Smart Mini-Mullion	
(S)XF1100 (S)XF1200	Multi-Technology Mullion Smart Mullion		▶	MT11	aptiQ™ Multi-Technology Mullion	
(S)XF1500 (S)XF1550 (S)XF1560 (S)XF2100 (S)XF2200	Multi-Technology Single Gang Proximity Single Gang Smart Single Gang Multi-Technology Mid-Range Smart Mid-Range		▶	MT15	aptiQ™ Multi-Technology Single Gang	
(S)XF2110 (S)XF2110P-K (S)XF2210	Multi-Technology Mid Range with Keypad Prox Mid-Range with Keypad Smart Mid-Range with Keypad		▶	MTK15	aptiQ™ Multi-Technology Single Gang with Keypad	

aptiQ™ Smart Technology from Ingersoll Rand enhances the intelligence of products through a secure, open architecture design 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.

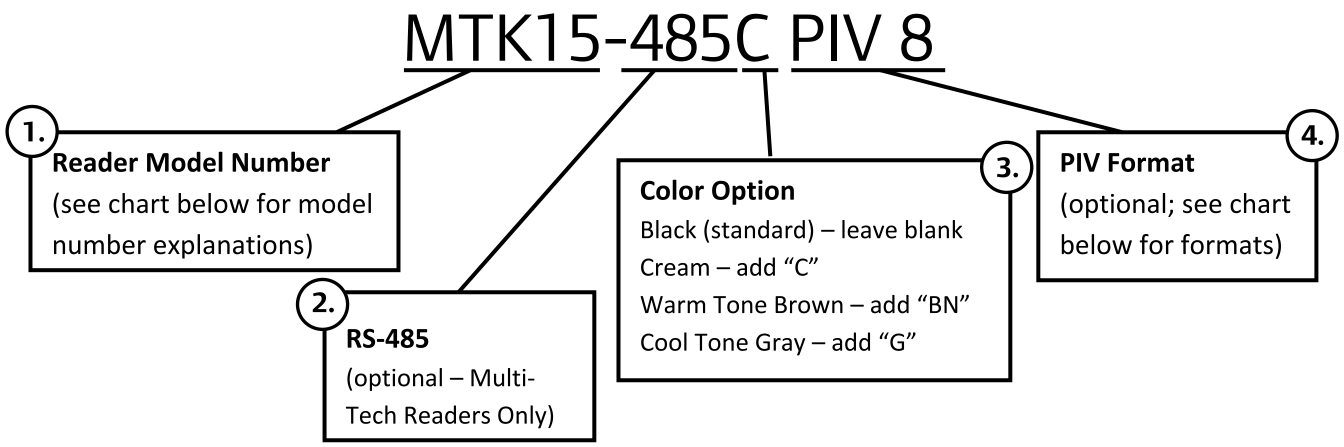
Reader Order Guide

This guide has been designed to assist you in determining the appropriate information to use when ordering reader products from Ingersoll Rand Security Technologies. This is not meant to substitute a purchase order, and a valid purchase order must be submitted to order reader products. If you have any questions, or need additional assistance, please contact your Ingersoll Rand Security Technologies Sales Professional.

Build Your Reader Part Number

Follow the steps below to build the full part number for the reader you wish to order. Use the sample below to determine how to write your part number on your PO.

Sample Part Number:



MTK15-485C PIV 8

1. **Reader Model Number** (see chart below for model number explanations)

2. **RS-485** (optional – Multi-Tech Readers Only)

3. **Color Option**
Black (standard) – leave blank
Cream – add "C"
Warm Tone Brown – add "BN"
Cool Tone Gray – add "G"

4. **PIV Format** (optional; see chart below for formats)

1. Choose Your Reader Model

Ingersoll Rand Security Technologies offers readers in a variety of technologies and form factors. Please see the chart below to determine which reader you would like to order.

Reader Model Number	Model Description
PR10	**Proximity Mini-mullion Reader:** Compact proximity reader, designed to fit in small spaces, or to be mounted to a door mullion.
SM10	**Smart Mini-mullion Reader:** Compact smart reader, designed to fit in small spaces, or to be mounted to a door mullion.
MT11	**Multi-technology Mullion Reader:** Designed to be mounted to a door mullion.
MT15	**Multi-technology Single Gang Reader:** Medium-sized reader designed to be mounted on a wall over a single gang junction box.
MTK15	**Multi-technology Single Gang Reader with Keypad:** Medium-sized reader designed to be mounted on a wall over a single gang junction box.
MTMS15	**Multi-technology Magnetic Stripe Reader:** Designed to be mounted on a wall over a single gang junction box with magnetic stripe capability.
MTMSK15	**Multi-technology Magnetic Stripe Reader with Keypad:** Designed to be mounted on a wall over a single gang junction box with magnetic stripe capability.

2. RS-485 Capability

Ingersoll Rand readers (multi-technology only) have been designed with an option to interface directly with controllers that utilize RS-485 protocol. RS-485 is a communication protocol that allows a two way communication between the reader and the panel, for example OSDP protocol.

To order readers with RS-485 capability, add **"-485"** after the reader model number. If you are using the standard Wiegand protocol, do not add a suffix (leave blank).

3. Reader Color Options

Ingersoll Rand Readers are available in four color options. Add the appropriate suffix after the reader model number and RS-485 option (if applicable).

Black (standard) – do not add a color suffix, leave blank
Cream – add **"C"**
Warm Tone Brown – add **"BN"**
Cool Tone Gray – add **"G"**

If the RS-485 option is chosen, add the color suffix after "-485." If the RS-485 option is not chosen, add the color suffix after the reader part number (ex: MT11BN).

4. PIV Format

75-bit PIV is the default format for all Ingersoll Rand readers. Other format requirements are determined by the access control system, agency requirements, and customer specifications. The other available formatting options are listed below. Add "PIV" and the format number after the reader model number, RS-485 option (if applicable), and color suffix (if applicable).

Format Number	Bit Information
1	75-bit PIV
2	58-bit TWIC/CAC
3	200-bit FASC-N
4	64-bit (BCD) TWIC/CAC
5	83-bit TWIC/CAC
6	66-bit (58-bit format +TSM) TWIC/CAC
7	64-bit (58-bit format (no parity) + TSM) TWIC/CAC
8	91-bit (83 bit format + TSM) TWIC/CAC
9	40–bit BCD
10	40-bit reversed BCD
11	64-bit BCD
12	64-bit reversed BCD
13	128-bit BCD
14	128-bit reversed BCD
15	58-bit HSE

If you need assistance in determining the PIV format for your facility, please contact your Ingersoll Rand Security Technologies Sales Professional directly.

5. Special Instructions

Please specify any other special instructions directly on your PO.

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

ALLEGION™

SCHLAGE®

CL-ENCODER2

Magnetic stripe credential encoder

Overview

The CL-ENCODER2 is a motorized magnetic stripe encoder-reader that allows credentials to be instantly encoded and issued to users. Its compact footprint, rugged design and low audible noise make it a perfect choice for credential issuance in applications of any kind. A single card-slot design simplifies user interface - ensuring quality encoding every time. A smooth mechanical card-transport ensures fast, reliable, and high-quality encoder operation. A dual-color red/green LED provides clear status indications to the operator. Power-fail card return and manual card-eject features ensure that a customer's card can easily be retrieved under any conditions.

Features and benefits

- Read and write Hi-Co and Lo-Co magnetic stripe cards per ISO 7810 and 7811
- Motorized for increased encoding precision and reliability
- Dual color LED status indicator
- Remote power pack
- Small footprint

Specifications

Interface	▪ RS232 - for use with Schlage software ▪ USB
Dimensions (HxWxD)	3.85" x 4.47" x 8.44" (9.78 mm x 11.18 mm x 21.10 mm)
Weight	2 lbs (0.9 kg)
Magnetic stripe	Tracks 1, 2, 3 Hi-Co/Lo-Co read/write per ISO 7810, 7811
Card speed	7-11 i.p.s.
Input Voltage	+12 VDC ffl 5 %
Current Draw	Idle: 300 mA Maximum: 3.0 A (during Hi-Co encode sequence) 1 A draw from an auxiliary serial port device
Communication Protocol	MagTek® MCP protocol
Command Set	MagTek MCP command set
MTBF	Electronics: 125,000 hours Magnetic read head: 1,000,000 passes (500,000 insertion cycles)
Temperature	Operating: 41°F to 113°F (5°C to 45°C) Storage: -40°F to 158°F (-40°C to 70°C)
Humidity	Operating and Storage: 5% to 95% non-condensing
Certifications	UL/CRU, CE Class B, FCC Class B
Material	PBT Polymer

Ordering information

- **CL-ENCODER2** - Magnetic Stripe Encoder, includes power supply

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises 27 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

ALLEGION™

aptiQ™

Multi-technology credentials

Overview

aptiQ® multi-technology credentials are extremely flexible. Particularly useful during a transition from proximity technology to smart technology, this card can be read by both proximity readers and smart readers. This allows customers to economically migrate to the latest smart technology at their own pace.

aptiQ multi-technology credentials contain both 125 kHz proximity and 13.56 MHz contactless smart card capability in one unit, and are available in the newest technologies of today, including both MIFARE® Classic and MIFARE DESFire™ EV1 technology.

Features and benefits

- Open architecture design is built on ISO 14443A standards, providing for a faster data transfer speed
- Only available in ISO style cards
- Utilize 125 kHz proximity and 13.56 MHz MIFARE® Classic technology or 125 kHz proximity
  and 13.56 MHz MIFARE DESFire™ EV1 technology
- Custom artwork and laser engraving available

125 kHz/13.56 MHz multi-technology credentials

Model number	9951	9958	8920/8940/8980
Credential type	ISO-Glossy White[1]	ISO-Glossy White[1]	ISO-Glossy White[1]
Credential technology; ISO standard	125 kHz Prox/MIFARE® Classic; ISO 14443	125 kHz Prox/MIFARE® Classic; ISO 14443	125 kHz Prox/MIFARE DESFire™ EV1; ISO 14443
Dimensions (H x W x D)	3.37" x 2.125" x 0.033"	3.37" x 2.125" x 0.033"	3.37" x 2.125" x 0.033"
Slot punch (printed guide)	Vertical	Vertical	Vertical
Memory capacity; application sectors	8K bit/1K byte; 16 sectors	32K bit/4K byte; 40 sectors	2K/4K/8K byte
Warranty	Lifetime - Credentials have a lifetime warranty against manufacturers defects. See sales policy for complete warranty details.		

[1] ISO-Glossy White style credentials are made from composite material, are printable, and can include a magnetic stripe as an option. Add M1 to the model number for a magnetic stripe when ordering.

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

ALLEGION™

aptiQ™

Smart credentials

Overview

aptiQ® contactless smart credentials put you in control by delivering smarter solutions. These credentials protect your most sensitive data by utilizing extra layers of security protection, and can be used for many other applications including transit, cashless vending, and cafeteria point of sale.

aptiQ contactless smart credentials operate on a 13.56 MHz frequency, and utilize high security encrypted data, which is mutually authenticated in communication between the card and reader, providing optimum security. aptiQ™ smart credentials offer the choice of 2.5k, 8k, 16k, 32k, and 64k bits of storage, which will meet the most demanding storage requirements.

Features and benefits

- Open architecture design is built on ISO 14443A standards, providing for a faster data transfer speed
- Offered in clamshell, ISO style cards, key fobs, and adhesive patches
- Utilize MIFARE® Classic or MIFARE DESFire™ EV1 technology
- Custom artwork and laser engraving available for clamshell and ISO style cards

13.56 MHz smart credentials

Model number	9420	9451	9520	9551	9558	9651	9651T	9351
Credential type	Clamshell	Clamshell	ISO-Glossy White[1]	ISO-Glossy White[1]	ISO-Glossy White[1]	Keyfob	Thin keyfob	Silicone wristband
Credential technology; ISO standard	MIFARE® Classic; ISO 14443	MIFARE Classic; ISO 14443	MIFARE Classic; ISO 14443	MIFARE Classic; ISO 14443	MIFARE Classic; ISO 14443	MIFARE Classic; ISO 14443	MIFARE Classic; ISO 14443	MIFARE Classic; ISO 14443
Dimensions (H x W x T in inches)	3.37 x 2.125 x 0.075	3.37 x 2.125 x 0.075	3.37 x 2.125 x 0.033	3.37 x 2.125 x 0.033	3.37 x 2.125 x 0.033	2 x 1.24 x 0.038	1.77 x 1.18 x .06	0.63 x 7.68 x 0.295
Slot punch (printed guide)	Vertical (punched)	Vertical (punched)	Vertical or horizontal	Vertical or horizontal	Vertical or horizontal	Key ring	Key ring	N/A
Memory capacity; application sectors	2.5k bit; 5 sectors	8k bit/ 1K byte; 16 sectors	2.5k bit; 5 sectors	8k bit/ 1K byte; 16 sectors	32k bit/ 4K byte; 40 sectors	8k bit/ 1K byte; 16 sectors	8k bit/ 1K byte; 16 sectors	8k bit/ 1k byte;
Warranty	Lifetime - Credentials have a lifetime warranty against manufacturers defects. See sales policy for complete warranty details.							

13.56 MHz smart credentials

Model number	9751	9758	8420 8440 8480	8520 8540 8580	8620 8640 8680	8720 8740 8780
Credential type	PVC patch	PVC patch	Clamshell	ISO-Glossy White[1]	Keyfob	PVC patch
Credential technology; ISO standard	MIFARE Classic; ISO 14443	MIFARE Classic; ISO 14443	MIFARE DESFire™ EV1	MIFARE DESFire™ EV1	MIFARE DESFire™ EV1	MIFARE DESFire™ EV1
Dimensions (H x W x T in inches)	3.37 x 2.125 x 0.033	3.37 x 2.125 x 0.033	3.37 x 2.125 x 0.075	3.37 x 2.125 x 0.033	2 x 1.24 x 0.28	3.37 x 2.125 x 0.033
Slot punch (printed guide)	Vertical	Vertical	Vertical (punched)	Vertical or horizontal	Keyring	Vertical
Memory capacity; application sectors	8k bit/ 1K byte; 16 sectors	32k bit/ 4K byte; 40 sectors	2K/4K/8K byte	2K/4K/8K byte	2K/4K/8K byte	2K/4K/8K byte
Warranty	Lifetime - Credentials have a lifetime warranty against manufacturers defects. See sales policy for complete warranty details.					

[1] ISO Glossy White style credentials are made from composite material, are printable, and can include a magnetic stripe as an option. Add M1 to the model number for a magnetic stripe when ordering.

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

© 2016 Allegion
005424, Rev. 08/16
www.allegion.com/us

ALLEGION™

aptiQ™

aptiQ™ advantages

When you choose aptiQ readers and credentials from Allegion, you're making the right decision. We offer unique advantages that help your business thrive and make doing business easier.

24 HOUR shipments

Standard orders of cards and readers are shipped in 24-48 hours.

WARRANTY limited lifetime[1]

Know you're protected against defects in materials and workmanship under normal use and service.

FAIR pricing

No upcharges for services that should come standard...like CardTrax™ and our standard composite material cards that eliminate warping from high-heat printers.

OPEN architecture

We secure our access control application sector, but the rest of the sectors are open for you to work with any company you choose.

QUALITY assurance

Quality control measures, advanced equipment and technology, and a no-fault replacement policy protect your investment.

MOBILE solutions today

With aptiQmobile™, your customers can use their NFC-enabled smart phone just like an ID card, and in many cases without replacing your existing readers.

CARDTRAX
card number tracking services

Ensure facility code and badge ID combinations are unique and never duplicated on any other cards we make. Compatible with Corporate 1000™.

SECURE
highest encryption available

aptiQ credentials using MIFARE DESFire™ EV1 offer our highest level of security through the use of mutual authentication, key diversification, and encryption.

CUSTOM
programming

Program any smart cards and readers with your custom key format and proprietary bit format.

ENGRAVING
permanent laser

Permanently label ISO and clamshell cards with badge ID information, logos, pictures and text.

Use aptiQ readers along with aptiQ credentials

- Simple lineup with only 7 SKUs but all of the technology options you need
- Available in Wiegand and RS-485
- All readers are FIPS 201-1 by default
- Multi-technology allows for easy transitions from one technology to the next
- Create your own reader label with the custom reader label program
- Color options and custom covers available

[1] Warranty periods different for networked reader keypads, networked magnetic striped read heads, and magnetic stripe credentials.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises 27 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

Ingersoll Rand
Security Technologies

CardTrax™

Account Tracking Program

Enhance your security without adding cost through our CardTrax account tracking program. We keep track of card numbers that have shipped and fulfill future orders so that card numbers are never duplicated. The program is available to clients who order cards on a regular basis.*

Why would you want us to guarantee unique ID numbers for all your cards? CardTrax provides the following advantages:

- **Added Security** – We ensure your facility code and badge ID combination is unique and never duplicated on any other cards we make.
- **Avoid Card Ordering Mistakes** – You'll eliminate potential errors or order duplication from other offices and facilities in your organization. We'll keep track of the next badge ID number you need to assign to your next card order.
- **Flexibility** – You can order your cards through the same provider or a different provider each time—either way we'll still know what facility code to assign your cards and what badge ID number to start with.
- **No Upcharges** – Other card providers often charge additional fees for card tracking services. We don't; we offer the same security without the added cost. Compare & save.
- **Compatible with HID® Corporate 1000™** - Our card tracking program fulfills card orders for both the 35C and 40X bit formats. Any proximity credentials that were previously enrolled in the HID Corporate 1000™ program are compatible with the CardTrax program. And we don't charge for our card tracking services.

* Minimum Annual Order Quantity: 2000 cards/year or 10 orders per year

Interested in enrolling in CardTrax?

Contact your local sales representative or Inside Sales at **855-248-0302** or **electronicinsidesales@irco.com**.

The program is available to an end-user facility, integrator, or other business partners and is available for new and existing customers.

Credential order guide

ALLEGION™

This guide is designed to help you determine the correct credential for your facility, and to aid in the ordering process. This is not meant to substitute a purchase order, and a valid purchase order must be submitted to order credential products. If you have any questions, please contact your Allegion sales representative.

Specify programming information

Please refer to the “Programming Information” section to fill out the chart below.

Part Number	Bit Format	Facility Code	Start Number		Quantity	Special Instructions	CardTrax™ Number
			Internal				
			External				
Please submit orders to readers.credentials.orders@allegion.com with purchase order.							

Programming Information	• Part number - Refer to credential part number from the “Choose A Credential” section • Bit Format – Example 26 bit; See bit format chart below. If you have questions, contact your sales representative. • Facility code - See bit format chart below. If you have questions, contact your sales representative • Start Number – Specify the internal and external start numbers. By default, the internal number matches the external number; please specify if this is not your desired option. • No Programming – If you would like your cards blank, please make sure you include **NP** in special instructions. If you would like your proximity cards blank, please make sure you include either 88i or initialized as they cannot be non programmed. • Slot Punch – Punch mark guides are on all ISO cards. Clamshells are punched on the landscape profile. Please specify slot punch orientation. • Custom Artwork – Please note any custom artwork requests and contact Inside Sales at 855-248-0302 for further instruction. • CardTrax™ - CardTrax format is a unique 40 bit format for smart cards and 35 bit format for prox cards. Cards will automatically be provided as “next in line” unless otherwise specified.

Choose the bit format

Bit formats	Facility Code Range	Number Range	Prox	Smart
26A (125kHz Standard)	0-255	0-65,535	Y	Y
32X	N/A	0-1,073,741,823	Y	Y
34N	0-255	0-65,535	Y	Y
34S	0-4,095	0-1,048,575	Y	Y
35C	0-4,095	0-1,048,575	Y	Y
35X	0-4,095	0-1,048,575	Y	Y
36X	0-4,095	0-2,097,151	Y	Y
37H	N/A	0-34,359,738,367	Y	Y
37X	0-65,535	0-524,288	Y	Y
40X (13.56MHz Standard)	0-1,023	0-268,435,455	N	Y
48X	0-1,048,575	0-1,048,575	N	Y

Choose a credential

Part Number	Comparable HID Part Number	Card Form Factor	Description
Proximity Credentials			
7410	1326	Clamshell	125 kHz proximity technology
7510*	1386/1586	ISO Glossy white	125 kHz proximity technology, Composite
7610	1346	Keyfob	125 kHz proximity technology Keyfob
7010	1391	Adhesive PVC Disk	125 kHz proximity technology 35mm Adhesive Disk
Multi-Technology Credentials			
9951*	1431/1437†	ISO Glossy white	125kHz proximity / 13.56MHz smart with MIFARE; 1K byte
9958*	1441/1447†	ISO Glossy white	125kHz proximity / 13.56MHz smart with MIFARE; 4K byte
8920/8940/8980*	1451/1457†	ISO Glossy white	125kHz proximity / 13.56MHz smart with MIFARE DESFire EV1; 2K/4K/8K byte
aptiQ Smart Credentials with MIFARE® Classic Technology			
9420	N/A	Clamshell	MIFARE – ISO 14443; 2.5k bit; 5 sectors
9451	N/A	Clamshell	MIFARE – ISO 14443; 8k bit / 1K byte; 16 sectors
9520*	N/A	ISO Glossy white	MIFARE – ISO 14443; 2.5k bit; 5 sectors
9551*	1430/1436	ISO Glossy white	MIFARE – ISO 14443; 8k bit / 1K byte; 16 sectors
9558*	1440/1446	ISO Glossy white	MIFARE – ISO 14443; 32k bit / 4K byte; 40 sectors
9651	1434	Keyfob	MIFARE – ISO 14443; 8k bit / 1K byte; 16 sectors
9751	N/A	PVC Patch	MIFARE – ISO 14443; 8k bit / 1K byte; 16 sectors
9758	N/A	PVC Patch	MIFARE – ISO 14443; 32k bit / 4K byte; 40 sectors
aptiQ Smart Credentials with MIFARE DESFire™ EV1 Technology			
8420/8440/8480	N/A	Clamshell	MIFARE DESFire EV1 – ISO 14443; 2K/4K/8K byte
8520/8540/8580*	1450	ISO Glossy White	MIFARE DESFire EV1 – ISO 14443; 2K/4K/8K byte
8620/8640/8680	N/A	Keyfob	MIFARE DESFire EV1 – ISO 14443; 2K/4K/8K byte
8720/8740/8780	1455	PVC Patch	MIFARE DESFire EV1 – ISO 14443; 2K/4K/8K byte
aptiQmobile™ Credentials			
9100**	N/A	Virtual	aptiQmobile Virtual Credential

*ISO Glossy White style credentials are made from composite material, are printable, and can include a magnetic stripe as an option. Add M1 to the model number for a magnetic stripe when ordering.

**Standard discounts do not apply. Contact your sales representative for pricing.

†Multi-technology credentials are comparable to HID Flexsmart®. 125 kHz proximity portion is comparable; however, the MIFARE portion may vary based on chip configuration and security measures employed.

Clamshell	ISO – Glossy White	Keyfob	Adhesive PVC Patch

Cards ordered with a plain white front and back, with no artwork or custom artwork, will have a small logo and reference number printed in the lower left-hand corner and slot punch target printed on the back of the card.

See complete warranty for details. Allegion standard terms and conditions apply. Minimum order is 100 pieces per credential type (50 for Keyfobs and 25 for aptiQmobile).

aptiQ™

Credential Compatibility Guide

125 kHz STANDARD PROXIMITY

XceedID™	LenelProx®
Schlage	HID®
GE/CASI®	AWID®

For added security, customers can choose to disable proximity functionality once the transition from proximity to contactless smart cards is complete.

13.56 MHz CONTACTLESS SMART

		Secure Format	Configurable Format	Card Serial Number Only†
ISO 14443	aptiQ™ MIFARE®	🔒		
	MIFARE® CSN†		🔧	
	aptiQ™ MIFARE DESFire™ EV1 with PACSA	🔒		
	MIFARE DESFire™ EV1		🔧	
	FIPS 201-1/PIV II US Government (ie Oberthur® and Gemalto®) must order PIV compliant readers	🔒	🔧	
	DESFire®		🔧	CSN ONLY
ISO 15693	HID iCLASS®			CSN ONLY
	Infineon my-d®			CSN ONLY
	Inside PicoTag™			CSN ONLY
	Texas Instruments Tag-it™		🔧	
	ST Microelectronics®		🔧	

Functionality for FIPS 201/PIV II is in default configuration.

Ingersoll Rand
Security Technologies

877-671-7011 · securitytechnologies.ingersollrand.com

004245 04/13

ALLEGION™

aptiQ™

Smart technology

Why make the switch?

Smart technology credentials

High frequency (13.56 MHz) smart technology credentials have been used for over 25 years in industries such as banking, U.S. government and metropolitan mass transit. These credentials offer the highest in security with MIFARE® and MIFARE DESFire™ EV1 technology options, in comparison to the outdated technologies in magnetic stripe and proximity credentials. With unique storage capabilities, smart credentials also offer the flexibility to provide more than just access control. Below are specifications for all three types of technologies to highlight the major upgrades realized when investing in smart technology.

Security		Proximity	Magnetic stripe	Smart
Encryption	Data being relayed between the card and reader is protected	—	—	■
Diversified keys	If one card is compromised, only that one card is affected; all other cards remain secure	—	—	■
Mutual authentication	Two way communication between the card and the reader to ensure both have authority to exchange data	—	—	■

Convenience		Proximity	Magnetic stripe	Smart
Contactless	Does not wear down card or reader	■	—	■
Communication rate	13.56 MHz; 100 times faster data transfer than proximity	—	—	■
Data storage	Can store multiple applications for a variety of functions	—	—	■

Storage		Proximity	Magnetic stripe	Smart
Programming	Open-architecture system that allows uses beyond access control such as cashless vending, record storage, biometric template, etc.	—	—	■
Standardization	Gives vendors flexibility to write applications to the card	—	—	■

Making the switch

Are your readers and credentials providing the features that have come to be expected from your access control system? Without the security, convenience and storage features and capabilities of smart technology your credentials are not allowing you to optimize your system and protect your facility.

With aptiQ™ multi-technology readers and multi-technology credentials from Allegion, you can transition systems from an existing population of magnetic stripe or proximity cards to more secure smart card technology at your own pace. The aptiQ reader portfolio is versatile enough to read magnetic stripe, 125 kHz proximity, and 13.56 MHz contactless smart cards in a single unit.[1]

Not only do aptiQ multi-technology readers allow you to easily and economically upgrade your credentials at your own pace, but they are also easy to install or replace with a quick-connect design that uses standard wiring currently used in most existing installations.

[1] PR10 and SM10 read proximity or smart technology only, respectively.

Learn more

To learn more about aptiQ readers and credentials call your local sales representative at 855.248.0302 or visit allegion.com/us and go to Brands > aptiQ.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

© 2014 Allegion
009810, Rev. 12/14
www.allegion.com/us

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

Proximity credentials

Overview

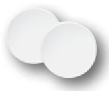
XceedID® proximity technology is an easy, convenient access control solution. Proximity technology, which operates on 125 kHz frequency, is easily integrated into existing legacy proximity systems or ideal for a new installation. Proximity credentials can easily fit into a wallet or may be used as a strapped or clipped badge.

From highly durable clamshell-style cards, to basic ISO style cards, to keyfobs and adhesive patches, XceedID offers several different form factors to meet the needs of many different customers.

Proximity credentials by XceedID are compatible with all industry leading proximity readers and are also completely ISO compliant. These credentials also have a passive design, requiring no batteries or maintenance for the life of the card.

Features and benefits

- Clamshell style offers high durability, and is suitable for harsh environments
- ISO style card is similar in size and thickness to a credit card, and has the ideal surface to print custom artwork, images, and photographs for identification
- Keyfob proximity credentials can easily be attached to any key ring for convenience
- Adhesive patch proximity credentials can be adhered to any frequently used surface
- Custom artwork and laser engraving available for clamshell and ISO style cards



125 kHz proximity credentials

Model number	7410	7510	7610	7010
Credential type	Clamshell	ISO-Glossy White[1]	Keyfob	PVC Disk
Credential technology; ISO standard	125 kHz prox	125 kHz prox	125 kHz prox	125 kHz prox
Dimensions (H x W x T)	3.37" x 2.125" x 0.075"	3.37" x 2.125" x 0.033"	2" x 1.24" x 0.38"	35 mm
Slot punch (printed guide)	Vertical (punched)	Vertical or horizontal	Keyring	N/A
Memory capacity; application sectors	N/A	N/A	N/A	N/A
Warranty	Lifetime - Credentials have a lifetime warranty against manufacturers defects. See sales policy for complete warranty details.			

[1] ISO-Glossy White style credentials are made from composite material, are printable, and can include a magnetic stripe as an option. Add M1 to the model number for a magnetic stripe when ordering.

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

005426, Rev. 08/15
www.allegion.com/us

Schlage

Electronic security

Readers & Credentials

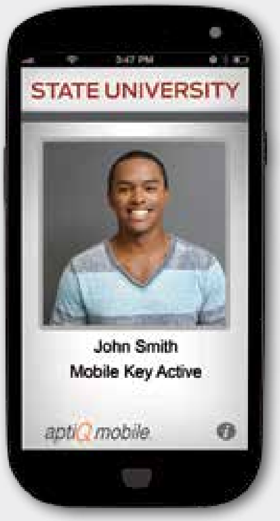
Brochures / Sales Materials

Master Index

ALLEGION™

aptiQ mobile™

Mobile credentials



Overview

aptiQmobile™ is the new way of delivering credentials to your smartphone. Utilizing near field communication (NFC) technology, aptiQmobile turns an app on your phone into your ID card, providing you the convenience of using your phone for access control and a variety of other applications such as vending[1], secure printing, discounts, or anything else your ID card is used for today.

Not only is it convenient, but your aptiQmobile credential offers a higher level of security than the average ID card, including advanced encryption and an optional passcode screen lock to help ensure that sensitive data is not compromised.

aptiQmobile credentials can be used on the same readers as aptiQ smart cards, so you can migrate to mobile credentials easily and at your own pace. Or issue mobile credentials to some employees while giving others cards; the system is designed to meet your dynamic security needs.

aptiQmobile credentials can be assigned using your existing access control software[2] or with the web-based aptiQmobile Admin Portal. Mobile credentials are created and issued by the account administrator via the aptiQmobile cloud service. Then the user downloads the free aptiQmobile app and verifies their identity before downloading the secure credential to their phone.

Features and benefits

- aptiQmobile works with any phone carrier
- Eliminates need to print ID's and keep inventory of cards on hand
- Painless replacement of lost cards anytime or anywhere
- Screen lock feature on phone keeps credential safe if phone is lost or stolen
- Credential information stored in same memory location as other app passwords and sensitive information
- aptiQmobile uses a 128 bit AES encrypted credential
- Patent-pending anti-playback technology prevents cloning

[1] When used in conjunction with a closed loop payment system
[2] aptiQ developer network participants

Mobile credential management

aptiQmobile credentials using NFC technology

Near field communication (NFC) is a short-range wireless connectivity technology designed for intuitive, simple and safe communication between two electronic devices that are both NFC-enabled. NFC-enabled phones can provide contactless solutions in access control, closed loop payments[1], and many other applications.

aptiQmobile has the flexibility to be implemented with a variety of NFC-enabled phones due to its ability to utilize three different communication modes, allowing your credential to adapt to various phone types and operating system versions. The communication mode is paired with its corresponding phone and OS version automatically (see chart below), allowing it to seamlessly communicate with aptiQ readers you already have in place.

Communication modes

Host Card Emulation	Android 4.4 or higher
Peer-to-peer	Android 4.1 up to 4.4
Card Emulation	iPhone + NFC enabled phone case

A higher level of security

All aptiQmobile credentials are secured using 128bit AES encryption (regardless of communication mode), making these mobile credentials more secure than the average ID card. In addition, key diversification, mutual authentication and a patent-pending anti-playback technology are also used as additional layers of security to help ensure the user's information is protected. On top of that, the password protected screen lock feature on mobile phones doesn't exist on a physical ID card. Pairing its increased level of security with all of the other conveniences of a mobile phone, aptiQmobile is a superior solution for your security needs.

How to order aptiQmobile

- Credential part number 9100
  - Minimum order quantity: 25
- NFC-enabled cases (required for iPhones):▪ KIT420B iPhone 4, black
  - KIT420W iPhone 4, white
  - KIT520B iPhone 5, black
  - KIT520W iPhone 5, white
- Visit aptiQmobile.com under the resources page to check if your phone is compatible with aptiQmobile credentials.

For more information or to order aptiQmobile credentials, contact our sales team at 855.248.0302 or visit aptiQmobile.com

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

010430, Rev. 08/15
www.allegion.com/us

Ingersoll Rand
Security Technologies

Basic Overview of Smart Card Technology

What is a Smart Card?

Smart cards are typically credit card sized, plastic credentials containing a microprocessor chip that serves the dual functions of communication and extensive data storage. Although it is packaged in the form of a card, a smart card operates much like a personal computer in that it can store data, manipulate data, and perform functions like mathematical equations. Smart cards normally contain application fields/sectors secured by special, application-specific security keys (much like keys that unlock various rooms in a building). These sectors can contain information for various applications – such as access control, cashless vending, mass transit, and payment systems – securely separated from one other by security keys. Smart cards can come in two forms: contact and contactless. Contact smart cards operate much like magnetic stripe cards (credit cards, etc.), requiring insertion into or direct contact with a reader. Contactless cards are read when presented near or in "proximity" to a reader.

Contact Smart Cards

Most cards originally introduced in the market were contact smart cards. This technology contains hundreds of times the storage capacity of its predecessor, the magnetic stripe card. Although most new applications of smart cards appear to be heading toward contactless technology, contact smart cards are still the standard for logical (computer) access and some other applications, such as payment systems in Europe.

Contactless Smart Cards

Contactless cards should not be confused with their predecessor – the proximity card. Although both technologies transmit data via radio frequency (and the visible operation of each appears the same to a user), a contactless card provides much greater security and contains 100 times the data storage of a traditional proximity card. Most new applications of smart cards, such as payments systems, are currently running pilots in anticipation of transitioning to contactless technology.

ISO Standards Governing Smart Cards

The International Standards Organization (ISO) is a network of 148 countries' institutes of standards that provides consensus for decisions governing standards for various products worldwide. Members include one representative per nation, including both government and private sector individuals. Decisions made by the ISO affect both business and government standards.

- *ISO 7816* is the ISO standard governing contact smart cards. The standard covers physical characteristics, dimensions and contact locations, transmission protocols, commands for interchange, application identifier systems and data elements.
- *ISO 14443* is a four-part contactless standard consisting of physical card characteristics, radio frequency power and signal interference, initialization and anti-collision and transmission protocols. The operating frequency defined in this standard is 13.56 MHz, providing a read range up to 4 inches (10 cm). There are two types of ISO *14443:*

Type A and Type B. Although originally meant to serve different functions, both Type A and Type B are now microprocessor standards similar in function. However, ISO 14443A is the more commonly used technology, while Type B is used primarily in banking applications. Due to faster data speeds, 14443 technology is recommended for applications in which extensive amounts of data, such as large biometric templates, need to be transmitted. Anticipating an increase in data-intensive applications requiring high data rates, the U.S. government recently selected ISO 14443 as its official standard.

- *ISO 15693* is a 13.56 MHz technology referred to as vicinity because it provides greater operational read ranges, making it the preferred choice for many high-traffic locations like access control.
- *Proximit*y can refer to ISO14443 or to the older 125 kHz technology traditionally used in access control. 125 kHz proximity is not "smart" technology and is not governed by ISO standards. 125 kHz proximity is typically proprietary, requiring that cards and readers be purchased from the same vendor.
- *Unique Identifier (UID):* All ISO-compliant smart cards are provided with a UID number (akin to a VIN number on a vehicle). For interoperability purposes, a card's UID is open and available to be read by all compliant readers. Since this unique number is not secured by keys, reading the UID of a smart card is comparable to reading a proximity card, mag stripe card or other technology that utilizes open, unsecured numbers.

Advantages of Contactless Smart Cards

There are a number of advantages to consider when comparing contactless technology to contact smart cards and 125 kHz proximity cards:

1. *Convenience:* Given the choice, users will virtually always choose contactless over contact technology. Contactless smart card users do not have to worry about where to insert the card, how to insert the card, or how fast to slide the card.
2. *Less Maintenance/Warranty:* Contactless smart cards require very little wear and tear maintenance because they contain no moving parts and require no points of contact. As a result, most contactless smart cards come with lifetime warranties covering defects and workmanship.
3. *Higher Security:* Contactless smart cards are uniquely capable of providing optimal transmission security with optional encryption and mutual authentication features. Mutual authentication is a three-way communication process between a card and reader using hashed, encrypted messages to authenticate each other without broadcasting a shared secret key.
4. *Large Memory:* Contactless cards have a data storage capacity hundreds of times greater than that of a proximity card. Contactless smart cards can also process information, calculate mathematical formulas and perform other computing functions.
5. *Enhanced Privacy:* Even large biometric templates can be stored and verified using a single contactless smart card, allowing private information to stay in the possession of the card holder instead of being stored in a data base.
6. *Versatile Form Factors:* Unlike its contact counterparts, contactless smart communication can utilize a variety of credential technologies. Keychain fobs, watches and even stickers can be used as contactless credentials.
7. *Multiple Applications:* Carrying a contactless smart card is like carrying many cards in one. A single contactless smart card can manage multiple applications such as access control, payment systems, cashless vending, paring, mass transit, etc. Additional features and applications can be added to a contactless smart card as user needs evolve.
8. *Future Protection:* Contactless smart card technology will no doubt soon replace mag stripe and proximity technologies. Choosing contactless products now will avoid the use of obsolete and outdated systems while providing the best avenue for system expandability.

continued (pg. 3 of 3)

Card Technology Overview

aptiQ™ using MIFARE® is a 13.56 MHz contactless technology family of microprocessors developed by Philips. MIFARE® is the most common contactless chipset on the market and is used in many applications around the globe. It is an ISO 14443 product that ensures compatibility with future products. Cards can be purchased that contain memory up to 32k bits, a capacity robust enough to process the largest biometric templates while still incorporating other applications.

DESFire® is a high-end chipset in the MIFARE® family that is the first chip compliant with the Government Smart Card Interoperability Specification (GSC-IS). The GSC-IS standard was created to ensure the interoperability of contactless and contact smart cards throughout the federal government.

aptiQ™ using MIFARE DESFire™ EV1 is based on open global standards for both air interface and cryptographic methods. It is compliant to all 4 levels of ISO / IEC 14443A and uses optional ISO / IEC 7816-4 commands. MIFARE DESFire™ EV1 card can hold up to 28 different applications and 32 files per application. The size of each file is defined at the moment of its creation, making MIFARE DESFire™ EV1 a truly flexible and convenient product.

DES Encryption is a strong cryptographic algorithm protecting classified information. It is a public algorithm determined by the National Institute of Standards and Technology (NIST) to be open, inexpensive, widely available and – most of all – very secure.

Triple DES is slower than regular DES but its longer key length and triple encryption process is billions of times more secure. Its advantage over other security algorithms is that it is based on the DES algorithm, making it easy to modify existing software to incorporate triple DES. Triple DES is also public with proven reliability.

AES (Advanced Encryption Standard) is a symmetric-key encryption standard adopted by the U.S. government. AES is slower than DES, but faster than Triple DES. AES-128 (128 bit key) and was the first publicly accessible and open cipher approved by NSA for top secret info.

my-d® is a 13.56 MHz contactless technology family of microprocessors developed by Infineon Technologies, one of the world's leading semiconductor companies. Its advanced security algorithms also make it a worldwide leader in ISO 15693 contactless technology.

iCLASS® is a proprietary, ISO 15693 compliant, 13.56 MHz contactless product line developed by HID® Corporation (an industry-leading card and reader manufacturer).

Security

The aptiQ™ smart card system offers a high level of security and data integrity through the use of high-level cryptographic techniques. The memory of the MIFARE DESFire™ EV1 with PACSA credential is divided into several sectors (also called application areas). Each sector is secured by an *Authentication Key*. A reader can only access a secure sector after a successful mutual authentication is performed. A successful mutual authentication requires that the reader and the card share a common secret - the mutual authentication key. The size of the mutual authentication key employed by the MIFARE DESFire™ EV1 with PACSA smart card system is 128 bits – the largest in the industry. After a successful authentication has taken place between the reader and the credential, communication is authorized and the reader gains access to the authenticated sector or application using *Message Authentication Codes (MACs)*. Each message going back and forth between the reader and the credential is digitally signed, ensuring that the communication remains authentic at all times and that an unauthorized device cannot interfere with the communication between the credential and the reader. The ISO smart card system is the only ISO14443 access control system offering Message Authentication Coding (MAC). The ISO smart card system also offers encryption of the data stored on the credential. The encryption algorithms employed by the PACSA is AES, which is a strong, proven algorithms.*

Ingersoll Rand®

Harnessing the Power of Multi-Technology Readers

In this world of acquisitions, mergers, and multiple/remote office locations, large organizations often find themselves burdened by a hodge-podge mix of card and reader access control technologies. And to make matters worse, a monumental change in the security industry is hovering on the horizon: the inevitable transition from existing but outdated proximity card technology to new, dynamic smart card technology.

The global reach of this transition is undeniable: already much of Asia and Europe has adopted contactless smart technologies as the new standard for security, transportation and identity management systems. The question is no longer if or when smart technologies will reach North American shores – they already have. The real question is how to harness the power of those technologies.

Although both proximity and smart card reader systems utilize radio frequency technology, the latest smart card technology operates on a much higher frequency, allowing data to be communicated at much higher speeds and with increased security. It is important to note that traditional proximity readers offer no data security and relatively slow data transmission speeds. In contrast, contactless smart card technology provides data encryption and mutual authentication security with data transmission speeds 100 times faster than proximity technology. Upgrading to smart technology is a no-brainer. But how do we get there?

Enter: the multi-technology reader. Housing both proximity and smart card technology in a single reader, multi-technology readers create an ideal transition pathway from proximity technology to smart card technology. Imagine all the nightmares that could have been spared during the DOS® to Windows® computing transition had there only been a machine that could function on both platforms at once!

Amazingly, multi-technology readers are very affordable (nearly the same price as single technology readers) and just as reliable and easy to install as the familiar proximity reader. They are compatible with virtually all existing access control system panels and can read multiple access card types simultaneously. The most common proximity cards in use today (HID Proximity® and GE/CASI ProxLite®) can all be read by an aptiQ™ multi-technology reader, as well as other industry-leading smart cards including MIFARE®, MIFARE DESFire™ EV1, and HID iCLASS® can be read by aptiQ™ multi-technology readers as well.

Finally, the big choices – which card technologies to use and how quickly to upgrade your systems while staying within your budget – are back in your hands. Because multi-technology readers are so flexible, you can choose the card technology, or even multiple card technologies, you want to use. You can upgrade your systems one facility at a time or even one door at a time.

You can make the transition to smart cards with all of your employees, a single department, or even just your executive staff. Multi-technology readers allow you to have blended reader populations and blended card populations for an indefinite period of time without compromising the functionality or reliability of your access control system. Suddenly, the daunting idea of upgrading your system doesn't seem so overwhelming. It doesn't have to break your budget or cripple your business because you don't have to rip out and totally replace your access infrastructure all at once.

Why would anyone installing a new security system or performing a system upgrade choose anything other than a multi-technology proximty/smart card reader? Whether you plan to continue using existing proximity cards or to migrate to smart cards in the future, multi-technology readers protect you from waking up one day to an obsolete system and the monumental budgetary, logistical and security crisis that presents.

Offering performance, security and unprecedented versatility, these products are truly today's value leader and have become the new standard in reader technology.

Ingersoll Rand
Security Technologies

Key Management: A Vital Element To A Contactless Smart Card System

The use of cryptography is now widespread in the technological world of smart cards and contactless or wireless security products. Large digital numbers called keys, along with cryptographic algorithms, are employed to provide secrecy and to protect the information stored on smart cards. Most contactless smart card communications are secured by a symmetric key system, in which both communicators must share a common secret (a key) as well as a common cryptographic algorithm in order to make the communication successful.

Digital Communication

A contactless smart card system can be viewed as a digital communication channel between a contactless smart card and a terminal. A contactless reader provides the translation between the RF link and the card and between the hardwired link and the terminal. These two digital links must be bidirectional to enable mutual authentication between the communicators (who must prove to each other that they all know the common secret – the key). In some cases, the contactless reader can also act as the terminal and make all the decisions locally. No one-way communication link can provide cryptographic security. For example, Wiegand is a one-way communication protocol widely used between card readers and terminals, but cannot be used to provide true security for smart card communication systems. With the exception of legacy installations/upgrades, new projects should be designed with serial or other two-way communication protocols to maximize security and system integrity.

Benefits of Cryptography

Mutual authentication between the smart card and the terminal allows communicators to positively identify each other. Pseudo random sequence generators, unique identification numbers and one-way hash functions are used in this process, along with an authentication key to prevent repeat attacks and illicit duplications of a communicator. After a successful mutual authentication, the communication between the card and the terminal is allowed. The privacy of that communication can be ensured through encryption/decryption of the data. A cipher like DES (Data Encryption Standard) or AES (Advanced Encryption Standard) and an encryption key are paired to protect the secrecy of the communication. Cryptography helps to ensure integrity and non-repudiation within a smart card system through the computation of MACs (Message Authentication Codes) accompanying the data exchanged between the communicators. Authentication keys, encryption keys, integrity keys and nonrepudiation keys are secret numbers used to protect the smart card communication system. Each type of key protects the system against various potential attacks and frauds and should therefore be managed with great care.

Using “Keys”

Keys protect a smart card system – algorithms do not. It should never be assumed that an algorithm will remain secret for a significant period of time. In fact, an algorithm that has been widely scrutinized and approved by the private and governmental scientific communities provides more strength than a secret algorithm. Most smart card systems can be used in a plug-and-play fashion. Cards, readers and terminals are often factory programmed with default keys. In the real world, most systems are never updated after initial installation and operate using the same default keys. Upgrading system security by replacing default keys with truly secure keys can be inconvenient, but it should be assumed that factory default keys will eventually become known and hence compromise the security of the systems they are meant to protect. It is important to utilize the full capability of a smart card system by protecting it with secret keys.

Smart card systems can be in use for years at a time. Partial information can slowly leak out of the system as cards are lost or stolen or as communications are illicitly monitored. Therefore, regularly updating keys may be beneficial to a smart card system. Keys should be difficult to remember, securely stored and frequently backed-up. Keys should look random and should not be considered weak. For example, a 56-bit key made of all zeros is very weak when used with DES. Other weak keys include those chosen from a narrow or reduced key set (such as lowercase letters in place of random 8-bit ASCII characters). Other reduced key spaces include English language phrases, dates, names and any other non-random selections. To demonstrate the weakness of a reduced key space, consider the following example: In the case of DES (or any 7-byte key algorithm), a key made of lowercase letters is 9 million ((256/26)7) times weaker than a key composed of 7 random bytes. Therefore, a brute force attack (also called an "exhaustive search"), that averages 100 years in duration, could take place in less than 6 minutes on a reduced key space made of lowercase letters. The best possible algorithms should be chosen to ensure system security. For instance, if a system offers a choice between DES and AES, the latter should be chosen without hesitation. If a smart card system is advertised to be secure, that claim should be supported with a solid study of its cryptographic algorithms (unless those algorithms are public and already well studied). Customers will feel comfortable using a system with algorithms that are known to be strong because the overall security of the system can be controlled by simply protecting system keys.

Design of the smart card system

A well-designed smart card system includes robust, upgradeable and flexible architecture and non-proprietary design features that are based on existing standards easily understood by the public. The robustness of a system is achieved through the responsible use of well-studied cryptographic techniques and algorithms. Optimal results occur when all parties involved in the design and integration of a system work openly together in the common interest of providing security. Disgruntled parties can easily introduce splits or vulnerabilities in the security of a system. For example, an angry firmware contractor could introduce a 'Trojan Horse' in the design to illicitly compromise the security of a system. The system should offer flexibility and upgradeability. A reader should be designed to communicate with various types of standardized terminals. Smart cards and readers should strictly adhere to communication standards in order to facilitate compatibility with future products and promote openness. Once again, the parties involved in the design of the system should be carefully selected and share the common goal of optimal security.

Readers and credentials

Simplifying the security industry like never before.

Allegion's aptiQ™ and XceedID® readers and credentials not only feature cutting-edge security technology, but are transforming basic access control products into all-in-one solutions, providing convenience and options to meet the needs of any facility or business.

The aptiQ line of multi-technology readers provides flexibility with an open architecture design. These versatile readers are capable of interfacing with many systems and security products currently on the market to provide you with the security you need now, and support for future technologies.

The wide variety of credential offerings from aptiQ and XceedID allows you to choose the best option to fit any budget or security need. Whether a facility requires a highly secure smart card option with the ability to be used for other applications, or a traditional proximity technology for less demanding installations, Allegion has a credential suitable for nearly any situation.

Introducing aptiQ smart technology

At the center of aptiQ is an open architecture multi-technology reader designed to be ultra easy, complete, and versatile. Built to work with what you have now and into tomorrow— accommodating most manufacturers' magnetic stripe cards, proximity cards, aptiQ smart cards, and the latest in mobile technology (NFC).

The aptiQ line of multi-technology readers are designed to simplify your access control solutions. Transition from proximity to smart card technology at your own pace without having to change out readers as new technologies are available. Also, aptiQ readers are NFC compatible and able to communicate with NFC-enabled phones whenever you're ready to take that step.

aptiQ contactless smart credentials offer a variety of data storage options and impressive data transfer rates in an open architecture design. These credentials can be read by both proximity readers and smart readers. This allows you to economically migrate to the latest smart technology at your own pace.

All this paired with aptiQ's comprehensive support program that's so encompassing, it's like someone opened a door to a new day in customer service. All so you can perform like never before.

aptiQ technology is also integrated into Allegion's full line of electronic access control products

HandPunch® GT-400 with multi-technology reader featuring aptiQ

The HandPunch GT-400 brings the flexibility of a full-function time and attendance terminal together with a versatile multi-technology credential reader. Featuring aptiQ smart card technology, the GT-400 allows employees to clock-in using the same credential they use to enter your building.

AD Series electronic locks with multi-technology readers featuring aptiQ.

AD Series electronic locks feature multi-technology readers that read a variety of proximity and smart cards. Built on the latest smart technology, AD Series locks feature the aptiQ technology as an open solution that allows you to keep up with future advancements.

When you need both smart and proximity technology, we read you.

With our versatile proximity, smart, and multi-technology reader options, we have a solution for any physical access control need. This comprehensive, yet simple reader line-up is suitable for any new smart or proximity installation.

Plus, the multi-technology readers can be used to economically and gradually change over from magnetic stripe or proximity to smart technology in an existing system. Easy to install and stylish in design, these readers can perfectly complement any facility's décor.

aptiQ multi-technology readers

aptiQ multi-technology readers are ideal for any new smart, proximity, or magnetic stripe installation—or as a cost effective way to migrate from existing magnetic stripe or proximity to smart technology.

- 13.56MHz and 125kHz technology in one reader
- Magnetic stripe option
- RS-485 optional
- Anti-microbial keypad
- Compatible with:
  - aptiQ smart credentials
    - using MIFARE DESFire™ EV1
    - using MIFARE® classic
  - Most popular proximity credentials
  - CSN of most existing 13.56MHz credentials
  - Magnetic stripe

aptiQ smart mini-mullion reader

The aptiQ smart mini-mullion reader is an excellent option for a smart-only installation.

- 13.56MHz smart technology
- Compact, unobtrusive design is easily installed in small spaces
- Compatible with:
  - aptiQ smart credentials
    - using MIFARE DESFire™ EV1
    - using MIFARE® classic
  - CSN of most existing 13.56MHz credentials

XceedID proximity mini-mullion reader

This reader is a great solution for proximity-only facilities.

- 125kHz proximity technology
- Compact, unobtrusive design is easily installed in small spaces
- Reads most proximity formats on the market today

Standard features:

- Open architecture design provides compatibility with nearly any access control system on the market
- Easy to install with standard wiring, quick-connect wiring harness and simplified mounting bracket

- LEDs plus audio feedback provides status for visually or audibly impaired
- Standard Wiegand output provides flexibility and optional RS-485 output provides more robust security
- Stylish contemporary designs in multiple finishes to complement any facility's architecture and décor

Multi-technology readers

Model MT11

aptiQ multi-technology mullion reader

Frequency
13.56 MHz and 125 kHz

Model MT15

aptiQ multi-technology single gang reader

Frequency
13.56 MHz and 125 kHz

Model MTK15

aptiQ multi-technology single gang reader with keypad

Frequency
13.56 MHz and 125 kHz

Model MTMS15

aptiQ multi-technology single gang magnetic stripe reader

Frequency
13.56 MHz and 125 kHz
Magnetic stripe

Model MTMSK15

aptiQ multi-technology single gang magnetic stripe reader with keypad

Frequency
13.56 MHz and 125 kHz
Magnetic stripe

AVAILABLE FINISHES:

- Black (standard)
- Cool tone gray
- Cream
- Warm tone brown

Smart and proximity readers

Model SM10

aptiQ smart mini-mullion reader

Frequency
13.56 MHz

Model PR10

XceedID proximity mini-mullion reader

Frequency
125 kHz

We pack a lot into every card.

With the latest in smart card technology and traditional proximity technology, we have an option for every budget and business need.

aptiQ smart cards using MIFARE DESFire™ EV1 technology are Allegion's highest security credentials. Or ditch the card altogether by downloading aptiQmobile™ credentials to your compatible NFC-enabled smartphone.

aptiQ smart and multi-technology credentials

aptiQ using MIFARE DESFire™ EV1 technology

These credentials offer the highest in security from Allegion. With multiple memory options, aptiQ credentials using MIFARE DESFire™ EV1 can be used for a variety of applications in addition to access control, such as cashless vending, cafeteria services, transportation, secure printing, and more.

aptiQ using MIFARE® Classic technology

aptiQ credentials using MIFARE® Classic technology are ideal for facilities with moderate security needs, and for businesses that want to use credentials to support multiple business functions.

aptiQmobile technology

aptiQmobile using NFC technology turns an app on your phone into your ID card providing the convenience of using your phone for access control and other closed-loop payment activities all with existing smart readers.

XceedID proximity credentials

XceedID proximity credentials are an excellent solution for facilities with less demanding security needs. XceedID proximity credentials are a cost effective solution, and are able to interface with many industry leading proximity readers including HID's 26-A bit Indala readers

Why transition to smart technology?

- Extra layers of security protection
- Open platform for other applications
- Same cost as proximity credentials
- Keep pace with future technologies

aptiQ mobile™

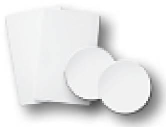
- Works with any phone carrier
- Eliminates need to print IDs and keep an inventory of cards on hand
- Screen lock feature on phone keeps credential safe if phone is lost or stolen
- Credential information stored in same memory location as other app passwords and sensitive information
- Stores a 128 bit AES encrypted credential that has to be decrypted by the access control reader
- Uses patent pending anti-playback technology that prevents cloning

Allegion's credentials are offered in a variety of form factors:

ISO-STYLE CARD
Similar in size and thickness to a credit card; available with magnetic stripe upon request

CLAMSHELL
Credit card-sized credential, highly durable

KEY FOB
Highly durable; able to be attached to a key ring



ADHESIVE PVC PATCH
35mm round or credit card-sized patch that can be attached to existing surfaces (only available as proximity credentials)

MOBILE CREDENTIAL
Credential downloaded directly to your smartphone

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit www.**allegion.com**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

005538, Rev. 09/14
www.allegion.com/us

ALLEGION™

Ingersoll Rand
Security Technologies

Sorting Through Credential Technology Choices

Significant evolution of card/credential and RFID technology in recent years has generated many questions from end-users and suppliers. What are the technologies and what is the best choice for your organization? Answering these questions is the purpose of this white paper.

Most people have used Magnetic Stripe, Bar Code, and Proximity technology cards or credentials. However, there tends to be some confusion surrounding the capabilities and advantages of bar code, proximity and – most recently – smart card technology.

Card Types

First, it is important to note that although we refer mainly to cards, most card technologies related to proximity and contactless may appear in several forms including cards, keyfobs, and tickets.

- *Magnetic Stripe* cards have been the most common technology used in many applications in recent decades. Also referred to as mag-stripe or swipe cards, these cards contain a strip of coated magnetic recording tape affixed to the outside of a card that is read when swiped through a reader. Mag-stripe cards have been the standard in the payment systems industry for years as well as the technology used in swipe access control systems. There are three tracks on a magnetic stripe that differentiate simple information (similar to the transfer of "license plate" information). Although typically lower in cost, mag stripe cards have very low security in regard to the protection of the information stored on the card.
- *Bar Code* credentials contain a series of lines that vary in width and distance from one another. Bar code readers use a laser beam (sensitive to the reflected light of the lines) to translate reflections into digital data that is transferred to a host computer for decision or storage. To date, bar code technology is the standard for retail check-out, inventory control and postal service. Next to magnetic stripe credentials, bar code credentials are the easiest and least expensive to produce. However, since bar codes are visible and easy to duplicate, the bar code card is the least secure of the access control credentials. (Recently, more secure bar code credentials have become available but represent an extremely limited percentage of access control credentials.)
- *Proximity cards* have become the standard for access control credentials. These credentials utilize radio-frequency identification (RFID) technology to communicate between a card and reader. The reader translates the information from a card into a digital format read by a host panel/computer that makes the decision to authorize a person's entry or acceptance. Proximity has become the standard in access control due to convenience (reading a credential presented within several inches of a door or reader) as well as greater transaction security when compared to magnetic stripe and bar code technologies.

- *Smart Card* credentials are typically credit card sized credentials containing an embedded processor chip with a memory capacity approximately 800 times that of a magnetic stripe card. Most smart card systems have the capacity to both read and write information to the card from the reader or panel, providing better data security while creating much greater flexibility for use in various applications. Smart Card credentials can be Contact or Contactless. Contact cards are similar in operation to mag-stripe cards in that they must be swiped or inserted into a reader to be read. They are recognizable by the gold chip visible on the outside of the card (which must make contact with the reader). Contactless cards utilize RFID technology, which may appear identical in operation to a proximity card to the average user. However, contactless smart cards have 100 times the information storage capacity, work on a different RF frequency and have far greater data security than a traditional proximity card.

A Smart Card Revolution in the U.S.?

A common question may be: We have heard of wide acceptance of smart card technology in Europe and of the impending smart card revolution in the United States for years, yet it has not appeared to happen. What would indicate that a revolution is more likely today than several years ago? In the 1990s, acceptance of smart technology in the U.S. lagged behind Europe and Asia because the U.S. already possessed a highly advanced telecommunications and banking network. Lack of strong telecommunications infrastructures, increasing rates of identity fraud and the high cost of processing information drove Europe and Asia to quickly adopt technology that could address these acute challenges.

The absence of government and industry standards for smart cards in the 1990s also contributed to the slow acceptance of the technology in the U.S. Without standards to facilitate interoperability, the full potential of smart card technology could not be realized. In July, 2003, the U.S. government adopted industry standards (ISO 14443 and other requirements) that have since propelled acceptance of smart card technologies at an exponential rate.

Finally, most smart cards originally introduced in the U.S. were contact smart cards, whose limitations generated increased access control system maintenance (chip and reader damage, etc.). Since proximity standard in the security industry in the U.S., there was also the perception of going backwards in technology – from proximity back to contact technology.

Brief Overview of RFID Technology (Proximity vs. Contactless)

Most experts project that RFID technology will gain acceptance explosively in the coming decades. However, there are many misconceptions regarding the capabilities of and privacy issues related to the technology. Pilot tests are being run in many industries but RFID technology has already been well proven and accepted in the security and public transportation industries.

The function of an RFID reader is very similar to that of a radio. Readers contain a receiver and transmitter used to send and receive radio waves (measured in hertz as a representation of frequency). Like a wave in the ocean, a radio wave goes up and down over time. The unit of measure representing one wave cycle per second is the hertz (Hz). The *frequency* of a wave is the number of wave cycles completed over a period of time, typically one second. Proximity technology operates in the low frequency band of 125 kHz (125,000 hertz/second). Contactless technology works in the higher frequency band of 13.56 MHz (13.56 million/second), roughly 100 times the speed of proximity technology. Higher frequency improves data transmission speed and security.

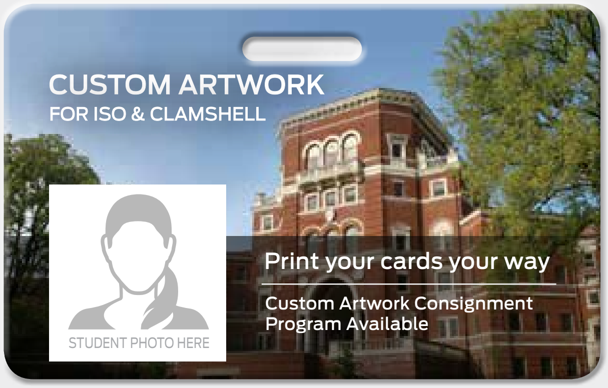
Simple 125 kHz proximity RFID technology has been the standard in access control for many years. Proximity is very similar to the technology used in applications such as animal identification and supply-chain inventory tracking. A basic RFID credential includes a simple chip of static memory and an antenna capable of transmitting the chip's ID to the reader. When a credential comes within range of the reader, it is powered by the electromagnetic field produced by the reader and proceeds to transmit its ID in much the same way a license plate identifies a vehicle. The communication is a simple, non-secure, one-way, read-only communication.

Contactless technology is typically a read/write, secure communication. Contactless smart cards are programmed with a unique identifier (UID) or badge identifier (BID) – similar to a vehicle VIN number – that enables interoperability and identification worldwide. Security information, such as the badge number used for access control, is contained within the application fields of the card (like pages of a book or rooms in a building) and is secured by special keys. Security of the information is further guarded by a process called mutual authentication, in which the reader and card verify that they belong to and are authorized to communicate with one another. The card and reader share a secret key that can only be verified through a process of hashing (mixing) random numbers with the secret key through an encryption method of algorithm processing. The secret key ensures secure communication because it is never communicated through the "air", and therefore cannot be intercepted (see application note #4 for more detail XceedID's website for more detail). In addition to superior security, contactless smart card technology also allows greater information storage and speed. One card can handle many applications like cashless vending, cafeteria or payment systems, and biometrics. Contactless smart cards are particularly effective for biometric applications (the unique identification of a person's identity through physical characteristics such as fingerprint, iris recognition, hand geometry, etc.). Biometric templates containing large blocks of information can be stored securely on a smart card, ensuring the privacy of physical data (the card stays in the individual's possession) without the need for large data base storage.

What does the future hold? With standards in place, the market appears to be moving quickly towards contactless smart card technology. A far more powerful card, protected by superior data transmission security, clearly presents numerous advantages and potential applications to explore. VISA, Mastercard, and American Express have all begun pilot tests of contactless payment system programs with great success and an eye toward implementing the technology in the years ahead. Consumers prefer the simplicity of waving a card near a reader to the archaic swipe method of presentation. Vendors enjoy the benefits of that simplicity, as well as the lower maintenance inherently associated with contactless systems. The contactless revolution is clearly in full swing – be sure to incorporate this technology in your next credential decision-making process.

ALLEGION™

Custom card printing services


CUSTOM ARTWORK
FOR ISO & CLAMSHELL
STUDENT PHOTO HERE
Print your cards your way
Custom Artwork Consignment Program Available

Did you know Allegion offers custom card printing services?

Custom cards offer a way to stand out from the crowd and provide a way to creatively express features of your business. Display your company logo, showcase unique artwork, or convey a simple sales message with a custom credential.

Ordering is easy

Contact Inside Sales at 855-248-0302 or ElectronicInsideSales@allegion.com to get started

1. Art requirements will be provided for your design submission
2. Once you finalize your design, Inside Sales will generate a quote and proof for your approval
3. Once your proof is approved a custom artwork number, to be included on your PO, will be assigned
4. You then submit your PO to order entry at readers.credentials.orders@allegion.com

Details

- Available for all ISO and clamshell cards
- Design must fit within space allotted
- $350 set up fee (one time per artwork file)
- 19¢ per card for single sided custom artwork; 29¢ per card for double sided custom artwork
- 4-5 week lead time is typical after PO is submitted
- Initial order must be for 1000 cards or more; recurring minimum quantity of 500 cards per order

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

Readers and credentials

Simplifying the security industry like never before.

Allegion's aptiQ™ and XceedID® readers and credentials not only feature cutting-edge security technology, but are transforming basic access control products into all-in-one solutions, providing convenience and options to meet the needs of any facility or business.

The aptiQ line of multi-technology readers provides flexibility with an open architecture design. These versatile readers are capable of interfacing with many systems and security products currently on the market to provide you with the security you need now, and support for future technologies.

The wide variety of credential offerings from aptiQ and XceedID allows you to choose the best option to fit any budget or security need. Whether a facility requires a highly secure smart card option with the ability to be used for other applications, or a traditional proximity technology for less demanding installations, Allegion has a credential suitable for nearly any situation.

Introducing aptiQ smart technology

At the center of aptiQ is an open architecture multi-technology reader designed to be ultra easy, complete, and versatile. Built to work with what you have now and into tomorrow— accommodating most manufacturers' magnetic stripe cards, proximity cards, aptiQ smart cards, and the latest in mobile technology (NFC).

The aptiQ line of multi-technology readers are designed to simplify your access control solutions. Transition from proximity to smart card technology at your own pace without having to change out readers as new technologies are available. Also, aptiQ readers are NFC compatible and able to communicate with NFC-enabled phones whenever you're ready to take that step.

aptiQ contactless smart credentials offer a variety of data storage options and impressive data transfer rates in an open architecture design. These credentials can be read by both proximity readers and smart readers. This allows you to economically migrate to the latest smart technology at your own pace.

All this paired with aptiQ's comprehensive support program that's so encompassing, it's like someone opened a door to a new day in customer service. All so you can perform like never before.

aptiQ technology is also integrated into Allegion's full line of electronic access control products

HandPunch® GT-400 with multi-technology reader featuring aptiQ

The HandPunch GT-400 brings the flexibility of a full-function time and attendance terminal together with a versatile multi-technology credential reader. Featuring aptiQ smart card technology, the GT-400 allows employees to clock-in using the same credential they use to enter your building.

AD Series electronic locks with multi-technology readers featuring aptiQ.

AD Series electronic locks feature multi-technology readers that read a variety of proximity and smart cards. Built on the latest smart technology, AD Series locks feature the aptiQ technology as an open solution that allows you to keep up with future advancements.

When you need both smart and proximity technology, we read you.

With our versatile proximity, smart, and multi-technology reader options, we have a solution for any physical access control need. This comprehensive, yet simple reader line-up is suitable for any new smart or proximity installation.

Plus, the multi-technology readers can be used to economically and gradually change over from magnetic stripe or proximity to smart technology in an existing system. Easy to install and stylish in design, these readers can perfectly complement any facility's décor.

aptiQ multi-technology readers

aptiQ multi-technology readers are ideal for any new smart, proximity, or magnetic stripe installation—or as a cost effective way to migrate from existing magnetic stripe or proximity to smart technology.

- 13.56MHz and 125kHz technology in one reader
- Magnetic stripe option
- RS-485 optional
- Anti-microbial keypad

- Compatible with:
  - aptiQ smart credentials
    - using MIFARE DESFire™ EV1
    - using MIFARE® classic
  - Most popular proximity credentials
  - CSN of most existing 13.56MHz credentials
  - Magnetic stripe

aptiQ smart mini-mullion reader

The aptiQ smart mini-mullion reader is an excellent option for a smart-only installation.

- 13.56MHz smart technology
- Compact, unobtrusive design is easily installed in small spaces

- Compatible with:
  - aptiQ smart credentials
    - using MIFARE DESFire™ EV1
    - using MIFARE® classic
  - CSN of most existing 13.56MHz credentials

XceedID proximity mini-mullion reader

This reader is a great solution for proximity-only facilities.

- 125kHz proximity technology
- Compact, unobtrusive design is easily installed in small spaces
- Reads most proximity formats on the market today

Standard features:

- Open architecture design provides compatibility with nearly any access control system on the market
- Easy to install with standard wiring, quick-connect wiring harness and simplified mounting bracket

- LEDs plus audio feedback provides status for visually or audibly impaired
- Standard Wiegand output provides flexibility and optional RS-485 output provides more robust security
- Stylish contemporary designs in multiple finishes to complement any facility's architecture and décor

Multi-technology readers

Model MT11

aptiQ multi-technology mullion reader

Frequency
13.56 MHz and 125 kHz

Model MT15

aptiQ multi-technology single gang reader

Frequency
13.56 MHz and 125 kHz

Model MTK15

aptiQ multi-technology single gang reader with keypad

Frequency
13.56 MHz and 125 kHz

Model MTMS15

aptiQ multi-technology single gang magnetic stripe reader

Frequency
13.56 MHz and 125 kHz
Magnetic stripe

Model MTMSK15

aptiQ multi-technology single gang magnetic stripe reader with keypad

Frequency
13.56 MHz and 125 kHz
Magnetic stripe

AVAILABLE FINISHES:

- Black (standard)
- Cool tone gray
- Cream
- Warm tone brown

Smart and proximity readers

Model SM10

aptiQ smart mini-mullion reader

Frequency
13.56 MHz

Model PR10

XceedID proximity mini-mullion reader

Frequency
125 kHz

We pack a lot into every card.

With the latest in smart card technology and traditional proximity technology, we have an option for every budget and business need.

aptiQ smart cards using MIFARE DESFire™ EV1 technology are Allegion's highest security credentials. Or ditch the card altogether by downloading aptiQmobile™ credentials to your compatible NFC-enabled smartphone.

aptiQ smart and multi-technology credentials

aptiQ using MIFARE DESFire™ EV1 technology

These credentials offer the highest in security from Allegion. With multiple memory options, aptiQ credentials using MIFARE DESFire™ EV1 can be used for a variety of applications in addition to access control, such as cashless vending, cafeteria services, transportation, secure printing, and more.

aptiQ using MIFARE® Classic technology

aptiQ credentials using MIFARE® Classic technology are ideal for facilities with moderate security needs, and for businesses that want to use credentials to support multiple business functions.

aptiQmobile technology

aptiQmobile using NFC technology turns an app on your phone into your ID card providing the convenience of using your phone for access control and other closed-loop payment activities all with existing smart readers.

XceedID proximity credentials

XceedID proximity credentials are an excellent solution for facilities with less demanding security needs. XceedID proximity credentials are a cost effective solution, and are able to interface with many industry leading proximity readers including HID's 26-A bit Indala readers

Why transition to smart technology?

- Extra layers of security protection
- Open platform for other applications
- Same cost as proximity credentials
- Keep pace with future technologies

aptiQ mobile™

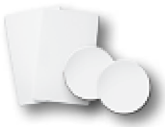
- Works with any phone carrier
- Eliminates need to print IDs and keep an inventory of cards on hand
- Screen lock feature on phone keeps credential safe if phone is lost or stolen
- Credential information stored in same memory location as other app passwords and sensitive information
- Stores a 128 bit AES encrypted credential that has to be decrypted by the access control reader
- Uses patent pending anti-playback technology that prevents cloning

Allegion's credentials are offered in a variety of form factors:

ISO-STYLE CARD
Similar in size and thickness to a credit card; available with magnetic stripe upon request

CLAMSHELL
Credit card-sized credential, highly durable

KEY FOB
Highly durable; able to be attached to a key ring



ADHESIVE PVC PATCH
35mm round or credit card-sized patch that can be attached to existing surfaces (only available as proximity credentials)

MOBILE CREDENTIAL
Credential downloaded directly to your smartphone

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit www.**allegion.com**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

005538, Rev. 09/14
www.allegion.com/us

ALLEGION™

Schlage

Electronic security

Readers & Credentials

Installation Manuals

Master Index

24195349

Support and Warranty
www.schlage.com/support
U.S.A./Mexico (877) 671-7011
International (512) 712-1316

Suporte e garantia
www.schlage.com/support
EUA/México (877) 671-7011
Internacional (512) 712-1316

ALLEGION™

KEYPAD CONFIGURATION

USER GUIDE

1 **Power cycle the reader.**

2 **Within 1 minute from powering on the unit, enter:**

* 8 8 8 8 9 9 9 9

The LED will turn green and the keypad will beep three times.

3 **Within 5 seconds, enter the necessary keypad format using the keypad.**

1. 4 bit burst - Enter 0 1
2. 8 bit burst - Enter * 0 *This is enabled by default.*
3. 26 bit Wiegand - Enter # followed by a 3 digit facility code between 000 and 255.

Examples:

- Enter # 0 9 6 for fixed facility code 96.
- Enter # 1 2 8 for fixed facility code 128.

The LED will turn green and the keypad will beep three times.

a **26-bit Wiegand Output**

In this mode, enter your PIN and press #

The reader sends the PIN (packaged as a 26-bit Wiegand output with the fixed facility code). The PIN must be a number between 1 and 65535.

Example: 1 10000000 0000101010100000 1
8 bit facility code is 128
16 bit PIN or card number is 2720

b **26-bit Keypad Format**

E XXXXXXXXXXXX XXXXXXXXXXXX O

X - data bit
E - Even parity bit computation
O - Odd parity bit computation

CONFIGURAÇÃO DO TECLADO

GUIA DO USUÁRIO

1 **Reinicie o leitor.**

2 **Dentro de 1 minuto após ligar a unidade, insira:**

* 8 8 8 8 9 9 9 9

O LED ficará verde e o teclado apitará três vezes.

3 **Dentro de 5 segundos, insira o modelo necessário do teclado através do mesmo.**

1. Burst de 4 bits - digite 0 1
2. Burst de 8 bits - digite * 0 *Isto está habilitado por padrão.*
3. Wiegand de 26 bits - digite # seguido de um código de acesso (facility code) de 3 dígitos entre 000 e 255.

Exemplos:

- Digite # 0 9 6 para código de acesso fixo 96.
- Digite # 1 2 8 para código de acesso fixo 128.

O LED ficará verde e o teclado apitará três vezes.

a **Saída Wiegand de 26 bits**

Nesse modo de trabalho, insira o seu PIN e pressione #

O leitor envia o PIN (compactado como uma saída Wiegand de 26 bits com o código de acesso fixo). O PIN deve ser um número entre 1 e 65535.

Exemplo: 1 10000000 0000101010100000 1
O código de acesso (facility code) de 8 bits é 128
O PIN de 16 bits ou número do cartão é 2720

b **Modelo de teclado de 26 bits**

E XXXXXXXXXXXX XXXXXXXXXXXX O

X - bit de dados
E - Computação de bit de paridade par
O - Computação de bit de paridade ímpar

Printed in U.S.A.
24195349 Rev. 01/14-b

Soporte y garantía
www.schlage.com/support

EE. UU./México	(877) 671-7011
Internacional	(512) 712-1316

CONFIGURACIÓN DEL TECLADO
GUÍA DEL USUARIO

1 Encienda el lector.

2 Después de 1 minuto de haber encendido la unidad, ingrese:

* 8 8 8 8 9 9 9 9

El LED se colocará en verde y el teclado emitirá tres pitidos.

3 Después de 5 segundos, ingrese el formato de teclado necesario utilizando el teclado.

1. Impulso de 4 bits: ingrese 0 1
2. Impulso de 8 bits: ingrese * 0 *Está habilitado de manera predeterminada.*
3. Wiegand de 26 bits: ingrese # seguido de un código de instalación de 3 dígitos entre 000 y 255.

Exemplos:

- Digite # 0 9 6 para el código de instalación fija 96.
- Digite # 1 2 8 para el código de instalación fija128.

O LED ficará verde e o teclado apitará três vezes.

a Salida de Wiegand de 26 bits

En este modo, ingrese su PIN y presione #

El lector envía el PIN (empaquetado como una salida Wiegand de 26 bits con el código de instalación fija). El PIN debe ser un número entre 1 y 65535.

Ejemplo: 1 10000000 0000101010100000 1

El código de instalación de 8 bits es 128

El PIN o número de tarjeta de 16 bits es 2720

b Formato de teclado de 26 bits

E XXXXXXXXXXXX XXXXXXXXXXXX O

X - bit de datos

E - Informática de bits de paridad par

O - Informática de bits de paridad impar

Soutien et garantie
www.schlage.com/support

É.-U./Mexique	(877) 671-7011
International	(512) 712-1316

CONFIGURATION DU CLAVIER
MANUEL DE L'UTILISATEUR

1 Mettez le lecteur sous tension.

2 Moins d'une minute après la mise sous tension, saisissez :

* 8 8 8 8 9 9 9 9

Le voyant à DEL sera vert et le clavier émettra trois bips.

3 Dans les cinq secondes suivantes, entrez au clavier le format de clavier requis.

1. Paquet de 4 bits – Entrez 0 1
2. Paquet de 4 bits – Entrez * 0 *Ceci est désactivé par défaut.*
3. Wiegand de 26 bits: ingrese # suivi du code d'installation à 3 chiffres compris entre 000 et 255.

Exemples:

- Entrez # 0 9 6 pour le code d'installation fixe 96.
- Entrez # 1 2 8 pour le code d'installation fixe 128.

Le voyant à DEL sera vert et le clavier émettra trois bips.

a Sortie Wiegand 26 bits

Dans ce mode, entrez votre NIP et appuyez sur #

Le lecteur transmet le NIP (incorporé dans une sortie Wiegand 26 bits avec le code d'installation fixe). Le NIP doit être un nombre entre 1 et 65535.

Exemples: 1 10000000 0000101010100000 1

Le code d'installation à 8 bits est 128

Le NIP ou le numéro de carte à 16 bits est 2720

b Format de clavier 26 bits

E XXXXXXXXXXXX XXXXXXXXXXXX O

X - bit d'information

E - Traitement du bit de parité

O - Traitement du bit d'imparité

23923337

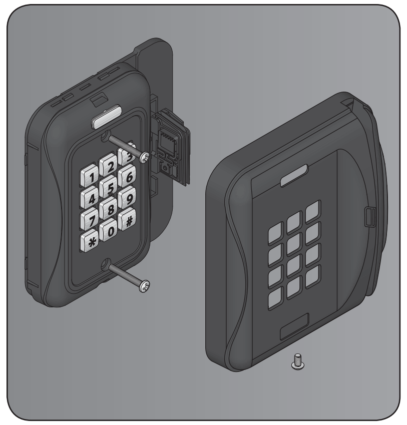
Support and Warranty
www.schlage.com/support
(877) 671-7011
+1 512-712-1316

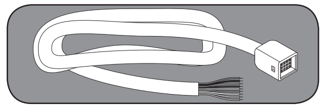
Soporte y garantía
www.schlage.com/support
+1 512-712-1316

ALLEGION

MTMS SINGLE GANG READER
INSTALLATION INSTRUCTIONS
MODELS MTMS15, MTMS15-485, MTMSK15, MTMSK15-485

LECTOR MTMS SINGLE GANG
INSTRUCCIONES DE INSTALACIÓN
MODELOS MTMS15, MTMS15-485, MTMSK15, MTMSK15-485





For Indoor/Outdoor Use		Para uso en interiores/exteriores
MTMS15	Multi-Technology Reader with Card Swipe— Single-Gang	Lector multitecnológico con lector de tarjeta magnética— Banda única
MTMSK15	Multi-Technology Reader with Card Swipe and Keypad— Single-Gang	Lector multitecnológico con lector de tarjeta magnética y teclado— Banda única

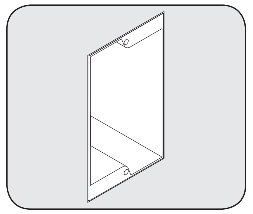
Tools
- Phillips Screwdriver
- 6-32 Tap
- 1" (25 mm), ⅛" (3 mm) Drill Bits
- T10 Security Torx™ Bit (Optional)

Herramientas
- Desatornillador Phillips
- Macho de roscar de 6-32
- Brocas de 1" (25 mm), ⅛" (3 mm)
- Mecha T10 Security Torx™ (Opcional)

By default, the MTMS(*) readers will read track 2 of the magnetic strip. If you require the ability to read track 1 or track 3, please contact Technical Support at 1-877-671-7011 for configuration options.
Los lectores MTMS(*) leerán, de manera predeterminada, la pista 2 de la banda magnética. Si desea poder leer la pista 1 o la pista 3, comuníquese con Soporte técnico al +1 512-712-1316 para cambiar las opciones de configuración.

1 Locate and/or install single gang box.

Ubique o instale la caja de banda única.



Consult manufacturer's instructions for installation.

Consulte las instrucciones del fabricante para la instalación.

2 Wire the cable to the control module.

A power limited, class 2 UL 294 approved power supply must be used.

Voltage rating: 5V to 16V

Conecte el cable al módulo de control.

Una potencia limitada, Clase 2 UL 294 suministro de energía debe ser aprobado utilizado..

Rango de tensión: 5 V a 16 V

Max. Length to Panel	
Length	**AWG**
200' (60 m)	22
300'	20
500'	18

Long. máx. al panel	
Longitud	**AWG**
60 m	22
90 m	20
150 m	18

Current @ 12V and 25C	
Avg. mA	**Max. mA**
165	195

Corriente a 12 V y 25 C	
Promedio de mA	**Máximo de mA**
165	195

Cable Connections	
Black	Ground
Blue	Unused
Brown	Red LED Control
Gray	Tamper Out
Green	Wiegand Data 0 / Data
Orange	Green LED Control
Pink*	RS485-A/Y
Red	Power In
Shield	Shield Ground
Tan*	RS485-B/Z
White	Wiegand Data 1 / Clock
Yellow	Beeper Control

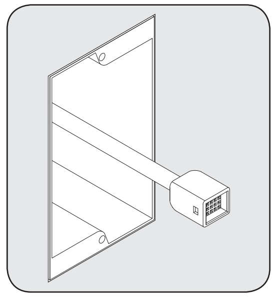
Conexiones de cables	
Negro	Tierra
Azul	Sin uso
Marrón	Control de LED rojo
Gris	Manipulación
Verde	Datos Wiegand 0 / Datos
Anaranjado	Control de LED verde
Rosa*	RS485-A/Y
Rojo	Encendido
Blindado	Descarga del blindaje
Habano*	RS485-B/Z
Blanco	Datos Wiegand 1 / Reloj
Amarillo	Control de alerta sonora

*These wires are unused for readers that do not support RS485 communication.

*Estos cables no se utilizan para lectores que no admiten la comunicación RS485.

3 Route cable through box.

Pase el cable a través de la caja.

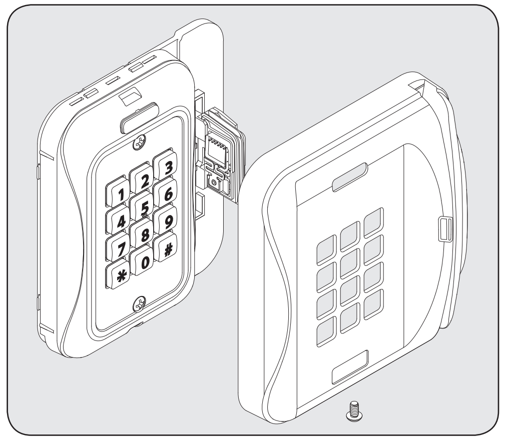


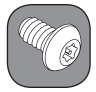
4 See BASEPLATE OPTION section before continuing.

Antes de continuar, consulte la sección OPCIÓN DE PLACA BASE.

5 Snap cover into place and install cover screw.

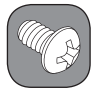
Coloque la cubierta en su lugar e instale el tornillo de la cubierta.





Tamper Resistant
6-32 x ¼" Pin-in-Torx button head, Use if desired.

Resistente a la manipulación
Perno de cabeza semiesférica Pin-in-Torx de 6-32 x ¼", Utilícelo si lo desea.



Regular
6-32 x ¼"

Regular
6-32 x ¼"

⚠ **Do not over-tighten!** **¡No apriete demasiado!**

TEST

PRUEBA

a Power the reader.

The LED will light followed by a beeper tone. This indicates that the reader is ready.

If LED and beeper do not respond, check cable connections.

Encienda el lector.

Se encenderá el LED seguido de un tono de alerta sonora. Eso indica que el lector está preparado.

Si el LED y la alerta sonora no responden, verifique las conexiones de los cables.

Test reader alignment by swiping card through slot.

Pruebe la alineación del lector pasando la tarjeta a través de la ranura.

b Present a proper card or token programmed to operate the reader.

Presente una tarjeta apropiada o una clave programada para operar el lector.

LED Indicators	
Green	Card was read and accepted
Red	Card was read but not accepted (does not indicate faulty installation)

Indicadores de LED	
Verde	Se leyó y aceptó la tarjeta
Rojo	Se leyó la tarjeta, pero no se aceptó (no indica que haya una instalación defectuosa)

BASEPLATE OPTIONS

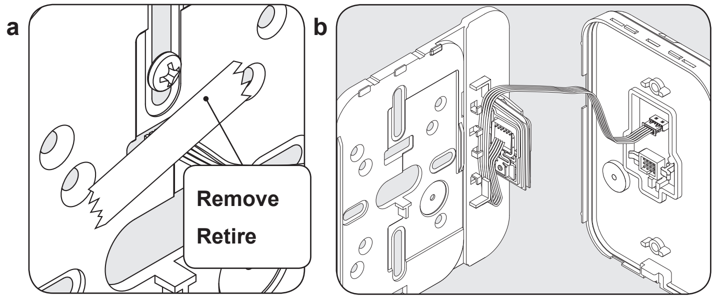
OPCIONES DE LA PLACA DE BASE

OPTION 1

OPCIÓN 1

i Plug Reader Cable into case.

Enchufe el cable del lector en la caja.

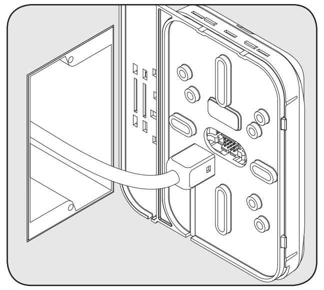


Wire must align with cutout in reader.

El cable debe alinearse sin recortes en el lector.

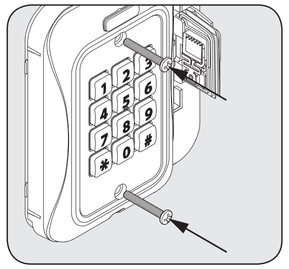
ii Plug cable into case.

Enchufe el cable en la carcasa.



iii Install case.

Instale la carcasa.



In case of alternative mounting screws, only a #6 diameter Pan Head Screw should be used. NOTE: Do not pinch reader cable.

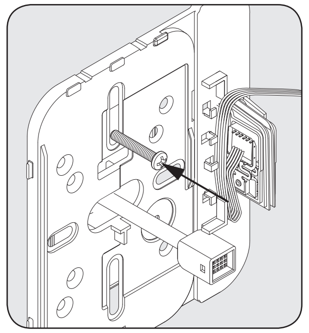
En caso de que se necesiten tornillos de montaje alternativos, solo deben utilizarse tornillos de cabeza troncocónica de diámetro N° 6. NOTA: No aplaste el cable del lector.

OPTION 2

OPCIÓN 2

i Install baseplate.

Instale la placa base.



Use this option for more robust tamper resistance.

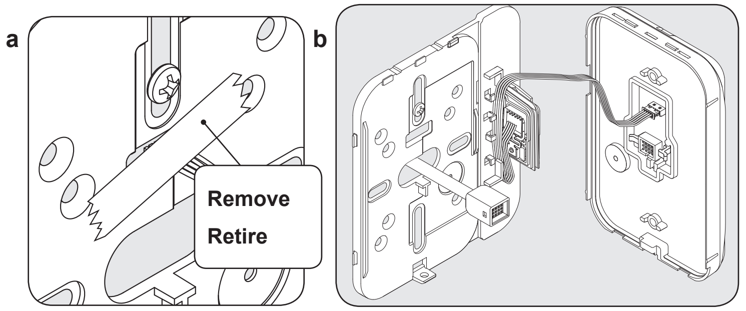
Continue to step 5 after completing this step.

Utilice esta opción para obtener una resistencia a la manipulación más intensa.

Luego de completar este paso, continúe en el paso 5.

ii Plug Reader Cable into case.

Enchufe el cable del lector en la caja.

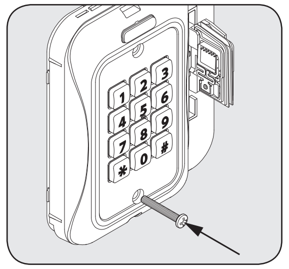


Wire must align with cutout in reader.

El cable debe alinearse sin recortes en el lector.

iii Install case.

Instale la carcasa.



In case of alternative mounting screws, only a #6 diameter Pan Head Screw should be used. NOTE: Do not pinch reader cable.

En caso de que se necesiten tornillos de montaje alternativos, solo deben utilizarse tornillos de cabeza troncocónica de diámetro N° 6. NOTA: No aplaste el cable del lector.

CE

RS485 connection shall not be used in S319 applications until a compatible S319 panel is identified with RS485 communications.

La conexión RS485 no debe utilizarse en aplicaciones S319 hasta que se identifique un panel S319 compatible con comunicaciones RS485.

ULC-S319 compliance is no longer valid when any add-on, expansion, memory, or other module manufactured or supplied by the manufacturer or manufacturer's representative is used. ULC-S319 Listed PSU must be used for Canadian installations.

FCC Statement
This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications to this equipment not expressly approved by Ingersoll Rand could void the user’s authority to operate the equipment.

Industry Canada Statement:
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. This Class A digital apparatus complies with Canadian ICES-003.

El certificación LUC-S319 deja de ser válida cuando se usa cualquier agregado, expansión, memoria u otro módulo fabricado o provisto por el fabricante o el representante del fabricante.

Declaraciones de la FCC
Este dispositivo cumple con la Sección 15 de las normas de la CCF. La utilización está sujeta a las siguientes dos condiciones: (1) Este dispositivo no puede causar interferencia dañina y (2) este dispositivo debe aceptar cualquier interferencia recibida, incluyendo interferencia que pueda causar un funcionamiento indeseado.

Los cambios o modificaciones a este equipo sin autorización expresa de Ingersoll Rand podrían anular la autoridad del usuario para utilizar el equipo.

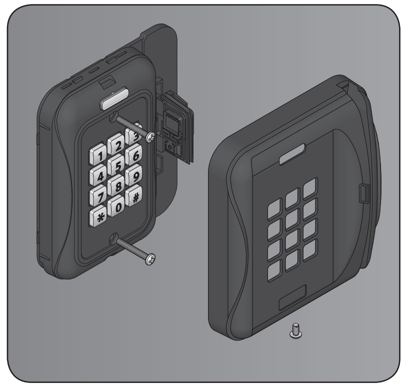
Declaraciones de Industry Canada
Este dispositivo cumple con los estándares RSS de licencia exenta de Industry Canada. Su utilización está sujeta a las siguientes dos condiciones: (1) este dispositivo no puede causar interferencia y (2) este dispositivo debe aceptar cualquier interferencia, incluyendo interferencia que pueda causar un funcionamiento no deseado. Este aparato digital Clase A cumple con la ICES-003 canadiense.

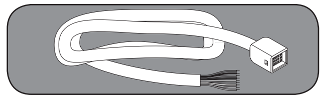
Soutien et garantie
www.schlage.com/support
+1 512-712-1316

Suporte e garantia
www.schlage.com/support
0800 774 8080

LECTEUR À COMMANDE UNIQUE MTMS
INSTRUCTIONS D'INSTALLATION
MODÈLES MTMS15, MTMS15-485, MTMSK15, MTMSK15-485

LEITOR ÚNICO DE GRUPO MTMS
INSTALLATION INSTRUCTIONS
MODELS MTMS15, MTMS15-485, MTMSK15, MTMSK15-485





Pour une utilisation en intérieur/extérieur — **Para utilização interna/externa**

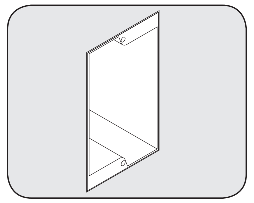
MTMS15	**Lecteur multitechnologique avec saisie par glissement de cartes— Lecteur à commande unique**	**Leitor de multitecnologias com leitora magnética— Caixa de distribuição única**
MTMSK15	**Lecteur multitechnologique avec saisie par glissement de cartes et clavier— Lecteur à commande unique**	**Leitor de multitecnologias com leitora magnética e teclado— Caixa de distribuição única**

Outils
- Tournevis cruciforme
- Taraud 6 - 32
- Mèches 1" (25 mm), ⅛" (3 mm)
- Mèche T10 Security Torx^MD (en option)

Ferramentas
- Chave de fenda Phillips
- Parafuso 6-32
- Brocas de 1" (25 mm), ⅛" (3 mm)
- Broca de segurança T10 Torx™ (Opcional)

Par défaut, les lecteurs MTMS (*) liront la piste 2 de la bande magnétique. Si vous devez lire la piste 1 ou la piste 3, veuillez communiquer avec le soutien technique au +1 512 712 1316 pour obtenir les options de configuration.
Por padrão, os leitores MTMS(*) conseguem ler a faixa 2 da faixa magnética. Se você precisar da opção de leitura da faixa 1 ou 3, entre em contato com o Suporte Técnico em 0800-774-8080 para opções de configuração.

1 Situez ou installez la boîte à commande unique. / Localize e/ou instale a única caixa de distribuição.



Consultez les directives du fabricant pour l'installation.

Consulte as instruções do fabricante para instalação.

2 Branchez le câble dans le module de contrôle. / Ligue o cabo ao módulo de controle.

Un bloc d'alimentation A UL 294 approuvé doit être utilisé.

Deve ser usada uma fonte de alimentação aprovada pela UL 294.

Plage de tension : De 5 V à 16 V

Classificação de voltagem: 5V a 16V

Longueur max. jusqu'au panneau	
Longueur	**Calibre américain du fil**
60 m	22
90 m	20
150 m	18

Comprimento máximo para o painel	
Comprimento	**AWG**
60 m	22
90 m	20
150 m	18

Courant @ 12 V et 25 C	
mA moyen	**mA max.**
165	195

Corrente @ 12V e 25C	
Média mA	**Máx. mA**
165	195

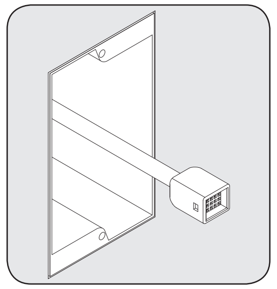
Connexions au câble	
Noir	Mise à la terre
Bleu	Inutilisé
Brun	Voyant de contrôle DEL rouge
Gris	Inviolable
Vert	Donnée Wiegand 0 / Donnée
Orange	Voyant de contrôle DEL vert
Rose*	RS485-A/Y
Rouge	Mise en marche
Blindage	Mise à la terre
Sable*	RS485-B/Z
Blanc	Donnée Wiegand 1 / Horloge
Jaune	Contrôle de l'avertisseur

*Ces fils sont inutilisés pour les lecteurs qui ne supportent pas de communication RS485.

Conexões de cabos	
Preto	Terra
Azul	Não utilizado
Marrom	Controle de LED vermelho
Cinza	Sem calçadeira
Verde	Dados Wiegand 0 / Dados
Laranja	Controle de LED verde
Rosa*	RS485-A/Y
Vermelho	Ligue
Blindado	Aterramento da proteção
Bege*	RS485-B/Z
Branco	Dados Wiegand 1 / Relógio
Amarelo	Controle de beeper

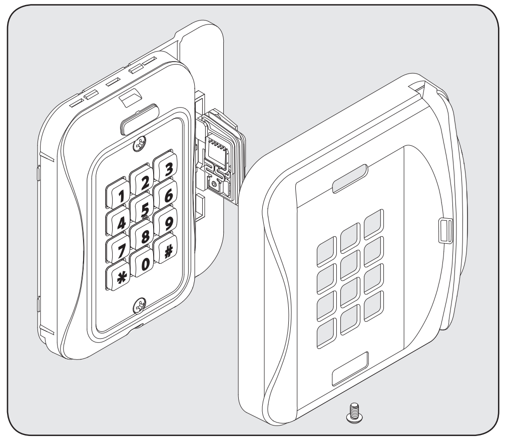
*Esses fios não são usados para leitores que não suportam comunicação RS485.

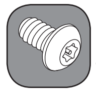
3 Connectez le câble du lecteur au boîtier. / Conecte o cabo do leitor na caixa.



4 Consultez la section OPTION DE LA PLAQUE DE BASE avant de continuer. / Veja a seção OPÇÃO DE PLACA BASE antes de continuar.

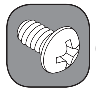
5 Alignez le couvercle et installez la vis. / Prenda a tampa no lugar e instale o parafuso da tampa.





Inviolable
Rivet à tête ronde Pinin- Torx 6 - 32 x ¼", Utilisez si souhaité.

Resistente à calçadeira
Cabeça arredondada presa com pino Torx 6-32 x ¼", Use, se desejado.



Regular
6-32 x ¼"

Regular
6-32 x ¼"

⚠ **Ne resserrez pas exagérément!** **Não aperte demais!**

TEST / TESTE

a Mettez le lecteur en marche. / Ligue o leitor.

Le voyant DEL s'allumera d'abord et le signal sonore retentira ensuite. Cela signifie que le lecteur est prêt.

O LED se acenderá seguido por um sinal de bip. Isso indica que o leitor está pronto.

Si le voyant DEL et l'avertisseur ne répondent pas, vérifiez les connexions au câble.

Se o led e o bip não responderem, verifique as conexões de cabos.

Vérifiez l'alignement du lecteur en passant une carte dans la fente.

Teste o alinhamento do leitor passando o cartão no slot.

b Présentez une carte adéquate ou un jeton programmé pour faire fonctionner le lecteur. / Apresente um cartão adequado ou um sinal programado para operar a máquina.

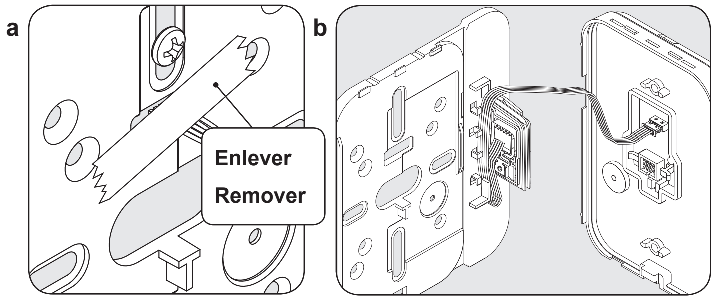
Voyants DEL	
Vert	La carte a été lue et acceptée
Rouge	La carte a été lue, mais n'a pas été acceptée (ne signifie pas une mauvaise installation)

Indicadores de LED	
Verde	O cartão foi lido e aceito
Vermelho	O cartão foi lido, mas não aceito (não indica instalação falha)

OPTIONS DE LA PLAQUE DE BASE / OPÇÕES DE PLACA DE BASE

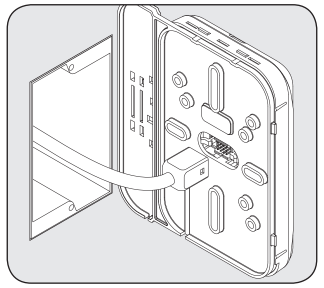
OPTION 1 / OPÇÃO 1

i Branchez le câble du clavier dans le caisson. / Conecte o cabo do teclado na caixa.

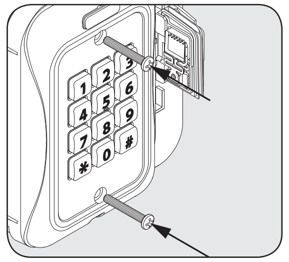


Le câble doit être aligné avec l'échancrure du lecteur. **O cabo deve estar alinhado com o corte na leitora.**

ii Branchez le câble dans le caisson. / Conecte o cabo na caixa.



iii Install case. / Instale la carcasa.

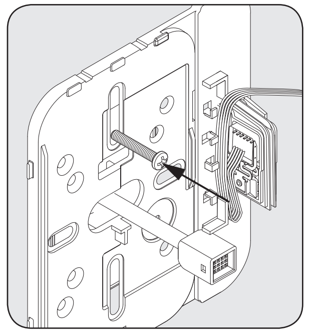


Si les vis de montage doivent être substituées, utiliser seulement une vis à tête cylindrique n ° 6. REMARQUE : ne pas pincer le câble du lecteur.

Se utilizar parafusos alternativos, utilize parafuso tamanho 6. NOTA: Não aperte o cabo do leitor.

OPTION 2 / OPÇÃO 2

i Installez la plaque de base. / Instale a placa base.



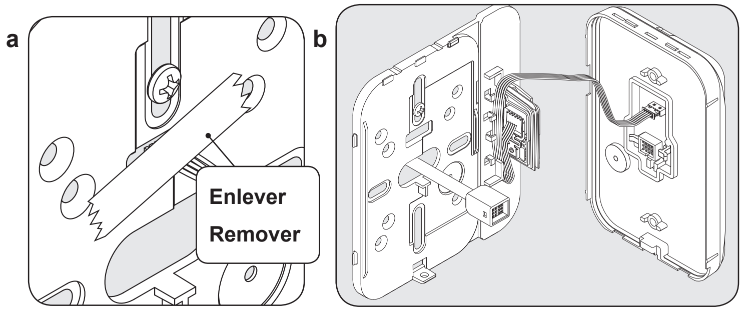
Utilisez cette option pour amplifier le caractère inviolable.

Passez à l'étape 5 après avoir effectué cette étape.

Use essa opção para uma resistência mais robusta da calçadeira.

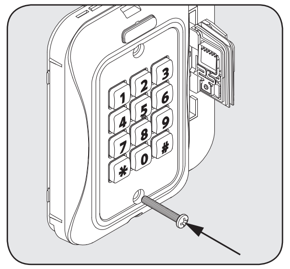
Continue até a etapa 5 após concluir esta etapa.

ii Branchez le câble du clavier dans le caisson. / Conecte o cabo do teclado na caixa.



Le câble doit être aligné avec l'échancrure du lecteur. **O cabo deve estar alinhado com o corte na leitora.**

iii Installez le caisson. / Instale a caixa.



Si les vis de montage doivent être substituées, utiliser seulement une vis à tête cylindrique n ° 6. REMARQUE : ne pas pincer le câble du lecteur.

Se utilizar parafusos alternativos, utilize parafuso tamanho 6. NOTA: Não aperte o cabo do leitor.

La connexion en RS485 ne doit pas être utilisée dans les applications S319 jusqu'à ce qu'un panneau S319 compatible soit identifié avec les communications RS485.

A conexão RS485 não deve ser utilizada em aplicativos S319 até que um painel compatível com S319 seja identificado pela comunicação RS485.

La conformité à la norme ULC-S319 n'est plus respectée si un ajout, une extension, une mémoire ou un autre module fabriqué ou fourni par le fabricant ou un représentant du fabricant est utilisé. L'installation d'un boitier d'alimentation homologue ULC-S319 est obligatoire au Canada.

Énoncés FCC
Cet appareil est conforme à la partie 15 des normes FCC. L'utilisation est soumise aux deux conditions suivantes : (1) Le dispositif ne doit pas émettre d'interférences nuisibles, et (2) ce dispositif doit accepter toutes les interférences reçues incluant celles pouvant nuire au fonctionnement.
Tous changements et toutes modifications à cet équipement sans l'approbation expresse de Ingersoll Rand peut annuler l'autorisation de fonctionnement de cet équipement par son utilisateur.

Déclarations D'industrie Canada
Ce dispositif est conforme à la norme RSS d'Industrie Canada relative aux dispositifs exempts de licence. Le fonctionnement est assujetti aux deux conditions suivantes : (1) ce dispositif ne doit pas occasionner de brouillage, et (2) ce dispositif doit accueillir tout brouillage y compris le brouillage qui risque d'entraîner un mauvais fonctionnement du dispositif. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
A conformidade ULC-S319 perde a validade quando qualquer acessório, expansão, memória ou outro módulo fabricado ou fornecido pelo fabricante ou representante do fabricante é utilizado.

Declaração de Anatel
Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

CE

Printed in U.S.A.
23923337 Rev. 01/14-b

23923329

Support and Warranty
www.schlage.com/support
(877) 671-7011
+1 512-712-1316

Soporte y garantía
www.schlage.com/support
+1 512-712-1316

ALLEGION

MULLION READERS

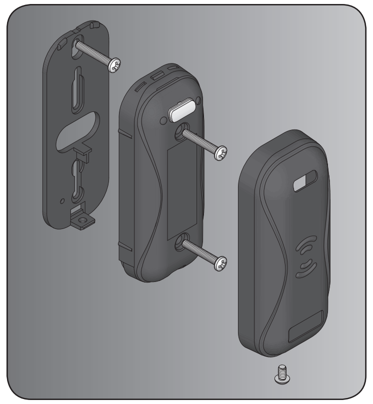
INSTALLATION INSTRUCTIONS

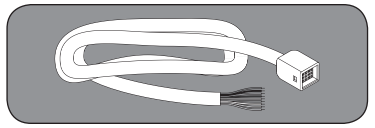
MODELS PR10, SM10, MT11, MT11-485

LECTORES MULLION

INSTRUCCIONES DE INSTALACIÓN

MODELOS PR10, SM10, MT11, MT11-485





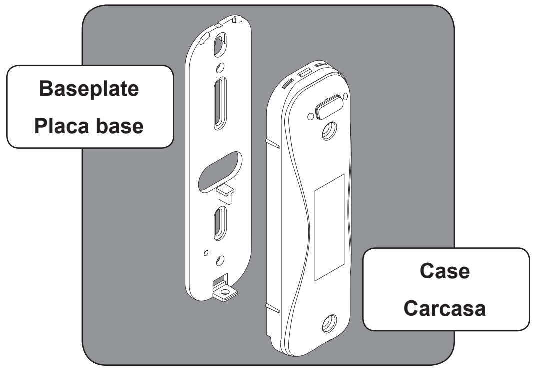
For Indoor/Outdoor Use		Para uso en interiores/exteriores
PR10	**Proximity Reader—Mini-Mullion**	**Lector de proximidad—Minimontante**
SM10	**Smart Reader—Mini-Mullion**	**Lector inteligente—Minimontante**
MT11	**Multi-Technology Reader—Mullion**	**Lector multitecnología—Montante**

Tools
- Phillips Screwdriver
- 6-32 Tap
- 1" (25 mm), ⅛" (3 mm) Drill Bits
- T10 Security Torx™ Bit (Optional)

Herramientas
- Desatornillador Phillips
- Macho de roscar de 6-32
- Brocas de 1" (25 mm), ⅛" (3 mm)
- Mecha T10 Security Torx™ (Opcional)

1 Separate case from baseplate.

Separe la carcasa de la placa base.

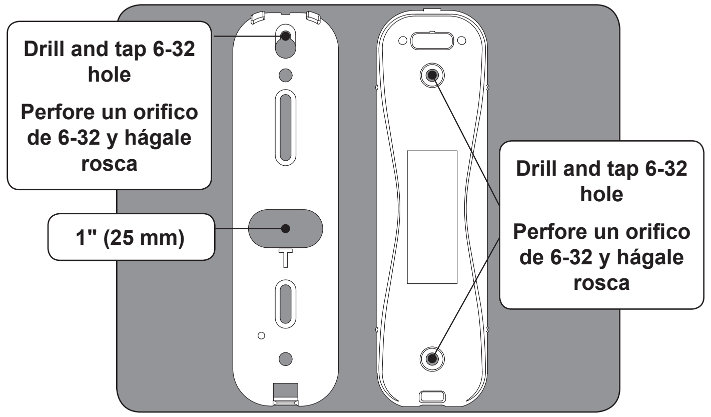


2 Mark and drill holes.

NOTE: Drill and tap for mounting on metal surface. Use ⅛" (3 mm) holes for mounting on wood, or appropriate anchors for other surfaces.

Marque y perfore orificios.

NOTA: Para el montaje, perfore orificios sobre una superficie metálica y hágales rosca. Utilice orificios de ⅛" (3 mm) para montar sobre madera, o bien anclajes adecuados para otras superficies.


Drill and tap 6-32 hole
Perfore un orifico de 6-32 y hágale rosca
1" (25 mm)
Drill and tap 6-32 hole
Perfore un orifico de 6-32 y hágale rosca

3 Wire the cable to the control module.

A power limited, class 2 UL 294 approved power supply must be used.

Voltage rating: 5V to 16V

Conecte el cable al módulo de control.

Una fuente de poder limitada, clase 2 UL 294 debe ser utilizada.

Rango de tensión: 5 V a 16 V

Max. Length to Panel	
Length	**AWG**
200' (60 m)	22
300' (90 m)	20
500' (150 m)	18

Long. máx. al panel	
Longitud	**AWG**
60 m	22
90 m	20
150 m	18

Current @ 12V and 25C		
Model	**Avg. mA**	**Max. mA**
PR10	65	110
SM10	95	195
MT11	100	165

Corriente a 12 V y 25 C		
Modelo	**Promedio de mA**	**Máximo de mA**
PR10	65	110
SM10	95	195
MT11	100	165

Cable Connections	
Black	Ground
Blue	Unused
Brown	Red LED Control
Gray**	Tamper Out
Green	Wiegand Data 0 / Data
Orange	Green LED Control
Pink*	RS485-A/Y
Red	Power In
Shield	Shield Ground
Tan*	RS485-B/Z
White	Wiegand Data 1 / Clock
Yellow	Beeper Control

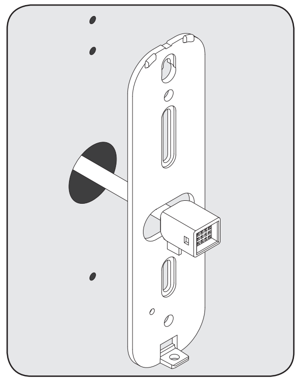
Conexiones de cables	
Negro	Tierra
Azul	Sin uso
Marrón	Control de LED rojo
Gris**	Manipulación
Verde	Datos Wiegand 0 / Datos
Anaranjado	Control de LED verde
Rosa*	RS485-A/Y
Rojo	Encendido
Blindado	Descarga del blindaje
Habano*	RS485-B/Z
Blanco	Datos Wiegand 1 / Reloj
Amarillo	Control de alerta sonora

* These wires are unused for readers that do not support RS485 communication.
** Tamper Outputs are to be connected to a UL Burglary System.

* Estos cables no se utilizan para lectores que no admiten la comunicación RS485.
** Las salidas de sabotaje se deben conectar a un sistema antirrobo con certificación UL.

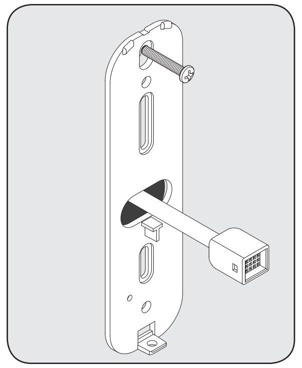
4 Route cable through holes.

Pase el cable a través de los orificios.



5 Install baseplate.

Instale la placa base.

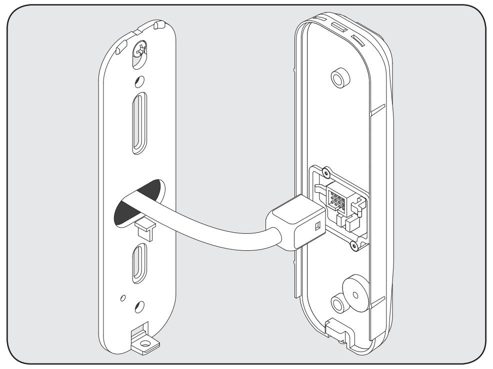


In case of alternative mounting screws, only a #6 diameter Pan Head Screw should be used.

En caso de que se necesiten tornillos de montaje alternativos, solo deben utilizarse tornillos de cabeza troncocónica de diámetro N° 6.

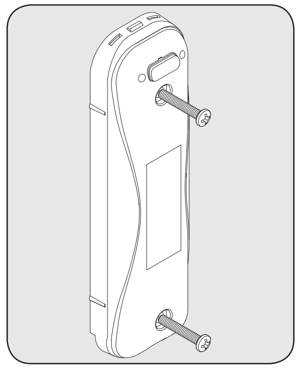
6 Plug cable into case.

Enchufe el cable en la carcasa.



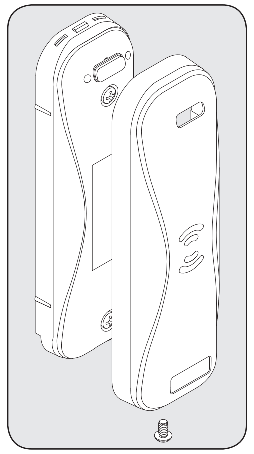
7 Install case.

Instale la carcasa.



8 Snap cover into place and install cover screw.

Coloque la cubierta en su lugar e instale el tornillo de la cubierta.



	Tamper Resistant 6-32 x ¼" Pin-in-Torx button head, Use if desired.	**Resistente a la manipulación** Perno de cabeza semiesférica Pin-in-Torx de 6-32 x ¼", Utilícelo si lo desea.
	Regular 6-32 x ¼"	**Regular** 6-32 x ¼"

⚠ **Do not over-tighten!** **¡No apriete demasiado!**

TEST

PRUEBA

a Power the reader.

The LED will light followed by a beeper tone. This indicates that the reader is ready.

If LED and beeper do not respond, check cable connections.

Encienda el lector.

Se encenderá el LED seguido de un tono de alerta sonora. Eso indica que el lector está preparado.

Si el LED y la alerta sonora no responden, verifique las conexiones de los cables.

b Present a proper card or token programmed to operate the reader.

Presente una tarjeta apropiada o una clave programada para operar el lector.

LED Indicators	
Green	Card was read and accepted
Red	Card was read but not accepted (does not indicate faulty installation)

Indicadores de LED	
Verde	Se leyó y aceptó la tarjeta
Rojo	Se leyó la tarjeta, pero no se aceptó (no indica que haya una instalación defectuosa)

CE

RS485 connection shall not be used in S319 applications until a compatible S319 panel is identified with RS485 communications.

La conexión RS485 no debe utilizarse en aplicaciones S319 hasta que se identifique un panel S319 compatible con comunicaciones RS485.

ULC-S319 compliance is no longer valid when any add-on, expansion, memory, or other module manufactured or supplied by the manufacturer or manufacturer's representative is used. ULC-S319 Listed PSU must be used for Canadian installations.

FCC Statement
This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications to this equipment not expressly approved by Ingersoll Rand could void the user’s authority to operate the equipment.

Industry Canada Statement:
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. This Class A digital apparatus complies with Canadian ICES-003.

El certificación LUC-S319 deja de ser válida cuando se usa cualquier agregado, expansión, memoria u otro módulo fabricado o provisto por el fabricante o el representante del fabricante.

Declaraciones de la FCC
Este dispositivo cumple con la Sección 15 de las normas de la CCF. La utilización está sujeta a las siguientes dos condiciones: (1) Este dispositivo no puede causar interferencia dañina y (2) este dispositivo debe aceptar cualquier interferencia recibida, incluyendo interferencia que pueda causar un funcionamiento indeseado.

Los cambios o modificaciones a este equipo sin autorización expresa de Schlage podrían anular la autoridad del usuario para utilizar el equipo.

Declaraciones de Industry Canada
Este dispositivo cumple con los estándares RSS de licencia exenta de Industry Canada. Su utilización está sujeta a las siguientes dos condiciones: (1) este dispositivo no puede causar interferencia y (2) este dispositivo debe aceptar cualquier interferencia, incluyendo interferencia que pueda causar un funcionamiento no deseado. Este aparato digital Clase A cumple con la ICES-003 canadiense.

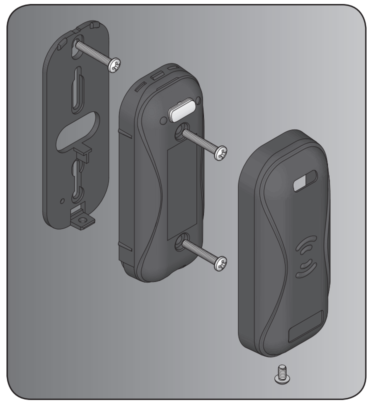
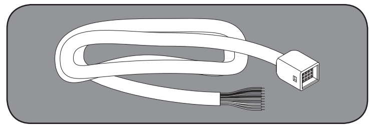
Soutien et garantie
www.schlage.com/support
+1 512-712-1316

Suporte e garantia
www.schlage.com/support
0800 774 8080

ALLEGION

DÉTECTEURS DE MENEAUX
INSTRUCTIONS D'INSTALLATION
MODÈLES PR10, SM10, MT11, MT11-485

LEITORAS MINI MULLION
INSTRUÇÕES DE INSTALAÇÃO
MODELOS PR10, SM10, MT11, MT11-485

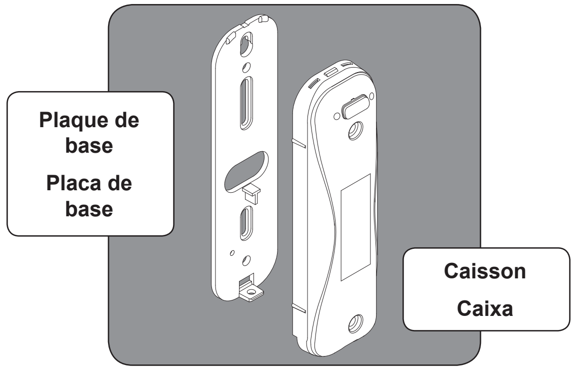
Pour une utilisation en intérieur/extérieur		Para utilização interna/externa
PR10	Lecteur de proximité—Minimeneau	Leitor de proximidade— Mini-coluna
SM10	Lecteur intelligent—Minimeneau	Leitor esperto— Mini coluna
MT11	Lecteur multitechnologique—Meneau	Leitor de múltiplas tecnologias— Coluna

Outils
- Tournevis cruciforme
- Taraud 6 - 32
- Mèches 1" (25 mm), ⅛" (3 mm)
- Mèche T10 Security Torx^{MD} (en option)

Ferramentas
- Chave de fenda Phillips
- Parafuso 6-32
- Brocas de 1" (25 mm), ⅛" (3 mm)
- Broca de segurança T10 Torx™ (Opcional)

1 Séparez le caisson de la plaque de base.

Separe a caixa da placa base.

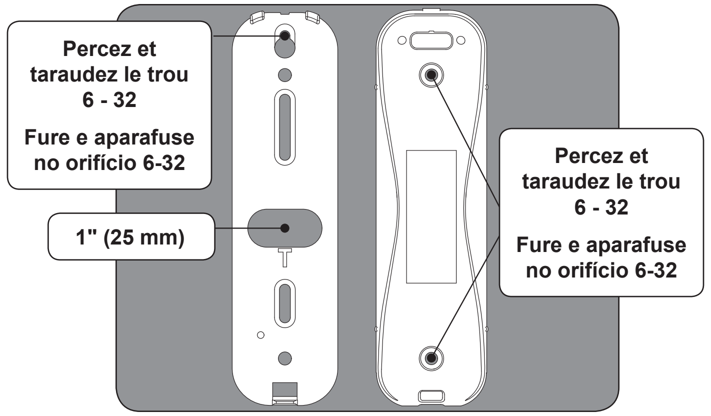


2 Marquez et percez les trous.

REMARQUE : Percez et taraudez pour montage sur une surface métallique. Utilisez des trous de ⅛" (3 mm) pour le montage sur bois, ou des ancrages appropriés pour d'autres surfaces.

Marque e faça os furos.

OBSERVAÇÃO: Perfure e aparafuse para montagem em superfície de metal. Use orifícios de ⅛" (3 mm) para montagem em madeira, ou os apoios adequados para outras superfícies.


Percez et taraudez le trou 6 - 32
Fure e aparafuse no orifício 6-32
1" (25 mm)
Percez et taraudez le trou 6 - 32
Fure e aparafuse no orifício 6-32

3 Branchez le câble dans le module de contrôle.

Un boitier d'alimentation homologué Classe 2 UL 294 doit être utilisé.

Plage de tension : De 5 V à 16 V

Ligue o cabo ao módulo de controle.

Classificação de voltagem: 5V a 16V

Longueur max. jusqu'au panneau	
Longueur	**Calibre américain du fil**
60 m	22
90 m	20
150 m	18

Comprimento máximo para o painel	
Comprimento	**AWG**
60 m	22
90 m	20
150 m	18

Courant @ 12 V et 25 C		
Modèle	**mA moyen**	**mA max.**
PR10	65	110
SM10	95	195
MT11	100	165

Corrente @ 12V e 25C		
Modelo	**Média mA**	**Máx. mA**
PR10	65	110
SM10	95	195
MT11	100	165

Connexions au câble	
Noir	Mise à la terre
Bleu	Inutilisé
Brun	Voyant de contrôle DEL rouge
Gris**	Inviolable
Vert	Donnée Wiegand 0 / Donnée
Orange	Voyant de contrôle DEL vert
Rose*	RS485-A/Y
Rouge	Mise en marche
Blindage	Mise à la terre
Sable*	RS485-B/Z
Blanc	Donnée Wiegand 1 / Horloge
Jaune	Contrôle de l'avertisseur

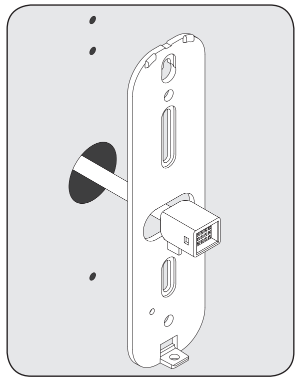
Conexões de cabos	
Preto	Terra
Azul	Não utilizado
Marrom	Controle de LED vermelho
Cinza**	Sem calçadeira
Verde	Dados Wiegand 0 / Dados
Laranja	Controle de LED verde
Rosa*	RS485-A/Y
Vermelho	Ligue
Blindado	Aterramento da proteção
Bege*	RS485-B/Z
Branco	Dados Wiegand 1 / Relógio
Amarelo	Controle de beeper

* Ces fils sont inutilisés pour les lecteurs qui ne supportent pas de communication RS485.
** Les sorties antisabotage doivent être branchées à un système antivol UL.

* Esses fios não são usados para leitores que não suportam comunicação RS485.
** As saídas do tamper devem ser conectadas a um sistema anti-vandalismo certificado UL.

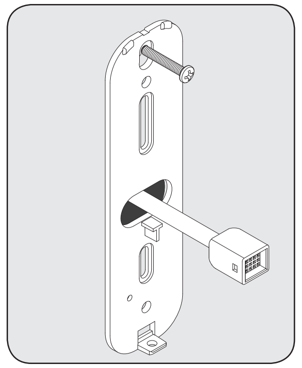
4 Acheminez le câble dans les trous.

Guie o cabo pelos furos.



5 Installez la plaque de base.

Instale a placa base.

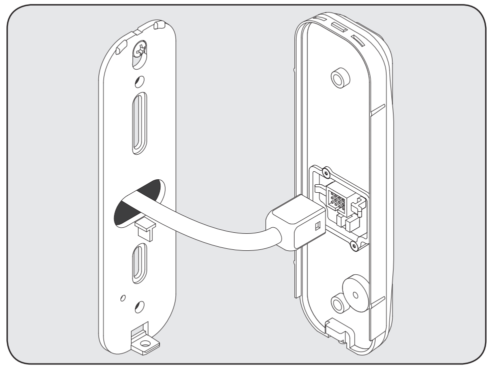


Si les vis de montage doivent être substituées, utiliser seulement une vis à tête cylindrique n ° 6.

Se utilizar parafusos alternativos, utilize parafuso tamanho 6.

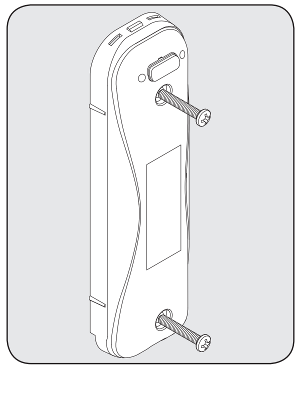
6 Branchez le câble dans le caisson.

Conecte o cabo na caixa.



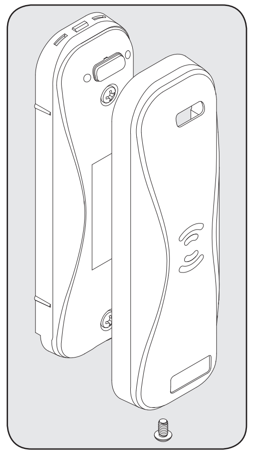
7 Installez le caisson.

Instale a caixa.



8 Alignez le couvercle et installez la vis.

Prenda a tampa no lugar e instale o parafuso da tampa.



Inviolable
Rivet à tête ronde Pin-in-Torx 6 - 32 x ¼", Utilisez si souhaité.

Resistente à calçadeira
Cabeça arredondada presa com pino Torx 6-32 x ¼", Use, se desejado.

Regular
6-32 x ¼"

Regular
6-32 x ¼"

⚠ **Ne resserrez pas exagérément!**

Não aperte demais!

TEST

TESTE

a Mettez le lecteur en marche.

Le voyant DEL s'allumera d'abord et le signal sonore retentira ensuite. Cela signifie que le lecteur est prêt.

Si le voyant DEL et l'avertisseur ne répondent pas, vérifiez les connexions au câble.

Ligue o leitor.

O LED se acenderá seguido por um sinal de bip. Isso indica que o leitor está pronto.

Se o led e o bip não responderem, verifique as conexões de cabos.

b Présentez une carte adéquate ou un jeton programmé pour faire fonctionner le lecteur.

Apresente um cartão adequado ou sinal programado para operar a máquina.

Voyants DEL	
Vert	La carte a été lue et acceptée
Rouge	La carte a été lue, mais n'a pas été acceptée (ne signifie pas une mauvaise installation)

Indicadores de LED	
Verde	O cartão foi lido e aceito
Vermelho	O cartão foi lido, mas não aceito (não indica instalação falha)

La connexion en RS485 ne doit pas être utilisée dans les applications S319 jusqu'à ce qu'un panneau S319 compatible soit identifié avec les communications RS485.

A conexão RS485 não deve ser utilizada em aplicativos S319 até que um painel compatível com S319 seja identificado pela comunicação RS485.

La conformité à la norme ULC-S319 n'est plus respectée si un ajout, une extension, une mémoire ou un autre module fabriqué ou fourni par le fabricant ou un représentant du fabricant est utilisé. L'installation d'un boitier d'alimentation homologue ULC-S319 est obligatoire au Canada.

Énoncés FCC
Cet appareil est conforme à la partie 15 des normes FCC. L'utilisation est soumise aux deux conditions suivantes : (1) Le dispositif ne doit pas émettre d'interférences nuisibles, et (2) ce dispositif doit accepter toutes les interférences reçues incluant celles pouvant nuire au fonctionnement.

Tous changements et toutes modifications à cet équipement sans l'approbation expresse de Schlage peut annuler l'autorisation de fonctionnement de cet équipement par son utilisateur.

Déclarations D'industrie Canada
Ce dispositif est conforme à la norme RSS d'Industrie Canada relative aux dispositifs exempts de licence. Le fonctionnement est assujetti aux deux conditions suivantes : (1) ce dispositif ne doit pas occasionner de brouillage, et (2) ce dispositif doit accueillir tout brouillage y compris le brouillage qui risque d'entraîner un mauvais fonctionnement du dispositif. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

A conformidade ULC-S319 perde a validade quando qualquer acessório, expansão, memória ou outro módulo fabricado ou fornecido pelo fabricante ou representante do fabricante é utilizado.

Declaração de Anatel
Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

CE

Printed in U.S.A.
23923329 Rev. 10/14-d

23940620

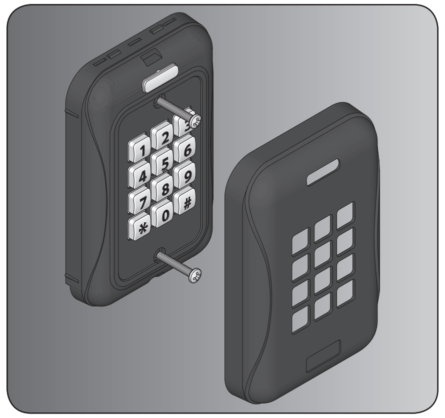
Support and Warranty
www.schlage.com/support
(877) 671-7011
+1 512-712-1316

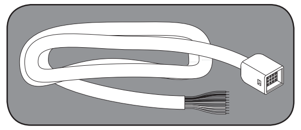
Soporte y garantía
www.schlage.com/support
+1 512-712-1316

ALLEGION

SINGLE GANG READER
INSTALLATION INSTRUCTIONS
MODELS MT15, MT15-485, MTK15, MTK15-485

LECTOR DE BANDA ÚNICA
INSTRUCCIONES DE INSTALACIÓN
MODELOS MT15, MT15-485, MTK15, MTK15-485





For Indoor/Outdoor Use	Para uso en interiores/exteriores

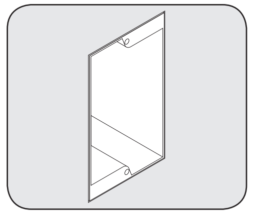
MT15	**Multi-Technology Reader—Single-Gang**	**Lector multitecnológico—Banda única**
MTK15	**Multi-Techology Reader with Keypad— Single-Gang**	**Lector multitecnológico con teclado— Banda única**

Tools
- Phillips Screwdriver
- 6-32 Tap
- 1" (25 mm), ⅛" (3 mm) Drill Bits
- T10 Security Torx™ Bit (Optional)

Herramientas
- Desatornillador Phillips
- Macho de roscar de 6-32
- Brocas de 1" (25 mm), ⅛" (3 mm)
- Mecha T10 Security Torx™ (Opcional)

1 Locate and/or install single gang box.

Ubique o instale la caja de banda única.



Consult manufacturer's instructions for installation.

Consulte las instrucciones del fabricante para la instalación.

2 Wire the cable to the control module.

Conecte el cable al módulo de control.

A power limited, class 2 UL 294 approved power supply must be used.

Voltage rating: 5V to 16V

Una fuente de poder limitada, clase 2 UL 294 debe ser utilizada.

Rango de tensión: 5 V a 16 V

Max. Length to Panel	
Length	**AWG**
200' (60 m)	22
300' (90 m)	20
500' (150 m)	18

Long. máx. al panel	
Longitud	**AWG**
60 m	22
90 m	20
150 m	18

Current @ 12V and 25C		
Model	**Avg. mA**	**Max. mA**
MT15, MT15-485	165	195
MTK15, MTK15-485	165	225

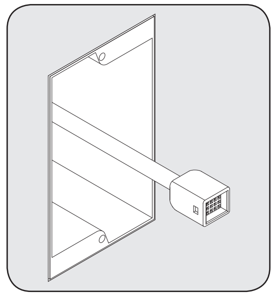
Corriente a 12 V y 25 C		
Modelo	**Promedio de mA**	**Máximo de mA**
MT15, MT15-485	165	195
MTK15, MTK15-485	165	225

Cable Connections	
Black	Ground
Blue	Unused
Brown	Red LED Control
Gray**	Tamper Out
Green	Wiegand Data 0 / Data
Orange	Green LED Control
Pink*	RS485-A/Y
Red	Power In
Shield	Shield Ground
Tan*	RS485-B/Z
White	Wiegand Data 1 / Clock
Yellow	Beeper Control

Conexiones de cables	
Negro	Tierra
Azul	Sin uso
Marrón	Control de LED rojo
Gris**	Manipulación
Verde	Datos Wiegand 0 / Datos
Anaranjado	Control de LED verde
Rosa*	RS485-A/Y
Rojo	Encendido
Blindado	Descarga del blindaje
Habano*	RS485-B/Z
Blanco	Datos Wiegand 1 / Reloj
Amarillo	Control de alerta sonora

3 Route cable through box.

Pase el cable a través de la caja.

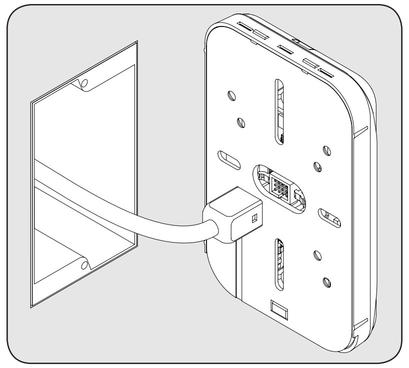


4 See BASEPLATE OPTION section before continuing.

Antes de continuar, consulte la sección OPCIÓN DE PLACA BASE.

5 Plug cable into case.

Enchufe el cable en la carcasa.

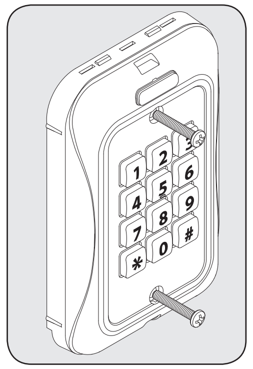


* These wires are unused for readers that do not support RS485 communication.
** Tamper Outputs are to be connected to a UL Burglary System.

* Estos cables no se utilizan para lectores que no admiten la comunicación RS485.
** Las salidas de sabotaje se deben conectar a un sistema antirrobo con certificación UL.

6 Install case.

Instale la carcasa.

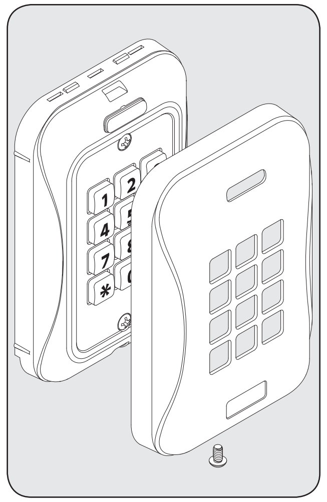


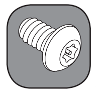
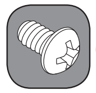
In case of alternative mounting screws, only a #6 diameter Pan Head Screw should be used.

En caso de que se necesiten tornillos de montaje alternativos, solo deben utilizarse tornillos de cabeza troncocónica de diámetro N° 6.

7 Snap cover into place and install cover screw.

Coloque la cubierta en su lugar e instale el tornillo de la cubierta.



	**Tamper Resistant** 6-32 x ¼" Pin-in-Torx button head, Use if desired.	**Resistente a la manipulación** Perno de cabeza semiesférica Pin-in-Torx de 6-32 x ¼", Utilícelo si lo desea.
	**Regular** 6-32 x ¼"	**Regular** 6-32 x ¼"

⚠ **Do not over-tighten!** **¡No apriete demasiado!**

TEST

PRUEBA

a Power the reader.

The LED will light followed by a beeper tone. This indicates that the reader is ready.

If LED and beeper do not respond, check cable connections.

Encienda el lector.

Se encenderá el LED seguido de un tono de alerta sonora. Eso indica que el lector está preparado.

Si el LED y la alerta sonora no responden, verifique las conexiones de los cables.

b Present a proper card or token programmed to operate the reader.

Presente una tarjeta apropiada o una clave programada para operar el lector.

LED Indicators	
Green	Card was read and accepted
Red	Card was read but not accepted (does not indicate faulty installation)

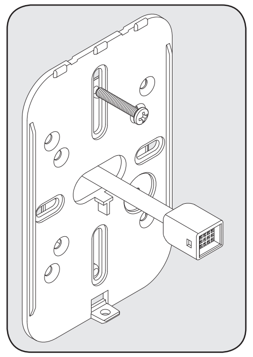
Indicadores de LED	
Verde	Se leyó y aceptó la tarjeta
Rojo	Se leyó la tarjeta, pero no se aceptó (no indica que haya una instalación defectuosa)

BASEPLATE OPTION

OPCIÓN DE PLACA BASE

i Install baseplate.

Instale la placa base.



Use this option for more robust tamper resistance.

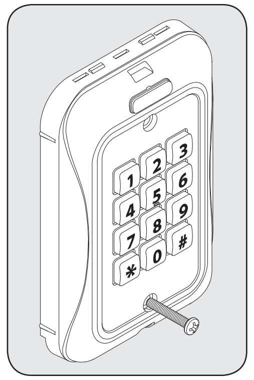
Continue to step 5 after completing this step.

Utilice esta opción para obtener una resistencia a la manipulación más intensa.

Luego de completar este paso, continúe en el paso 5.

ii Install case.

Instale la carcasa.



This step replaces step 6.

Este paso reemplaza al paso 6.

CE

RS485 connection shall not be used in S319 applications until a compatible S319 panel is identified with RS485 communications.

La conexión RS485 no debe utilizarse en aplicaciones S319 hasta que se identifique un panel S319 compatible con comunicaciones RS485.

ULC-S319 compliance is no longer valid when any add-on, expansion, memory, or other module manufactured or supplied by the manufacturer or manufacturer's representative is used. ULC-S319 Listed PSU must be used for Canadian installations.

FCC Statement
This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications to this equipment not expressly approved by Ingersoll Rand could void the user's authority to operate the equipment.

Industry Canada Statement:
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. This Class A digital apparatus complies with Canadian ICES-003.

El certificación LUC-S319 deja de ser válida cuando se usa cualquier agregado, expansión, memoria u otro módulo fabricado o provisto por el fabricante o el representante del fabricante.

Declaraciones de la FCC
Este dispositivo cumple con la Sección 15 de las normas de la CCF. La utilización está sujeta a las siguientes dos condiciones: (1) Este dispositivo no puede causar interferencia dañina y (2) este dispositivo debe aceptar cualquier interferencia recibida, incluyendo interferencia que pueda causar un funcionamiento indeseado.

Los cambios o modificaciones a este equipo sin autorización expresa de Schlage podrían anular la autoridad del usuario para utilizar el equipo.

Declaraciones de Industry Canada
Este dispositivo cumple con los estándares RSS de licencia exenta de Industry Canada. Su utilización está sujeta a las siguientes dos condiciones: (1) este dispositivo no puede causar interferencia y (2) este dispositivo debe aceptar cualquier interferencia, incluyendo interferencia que pueda causar un funcionamiento no deseado. Este aparato digital Clase A cumple con la ICES-003 canadiense.

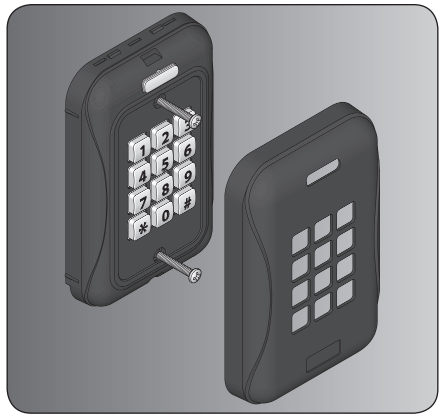
Soutien et garantie
www.schlage.com/support
+1 512-712-1316

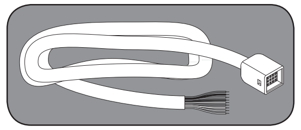
Suporte e garantia
www.schlage.com/support
0800 774 8080

ALLEGION

LECTEUR À COMMANDE UNIQUE
INSTRUCTIONS D'INSTALLATION
MODÈLES MT15, MT15-485, MTK15, MTK15-485

LEITOR DE BANDA ÚNICA
INSTRUÇÕES DE INSTALAÇÃO
MODELOS MT15, MT15-485, MTK15, MTK15-485





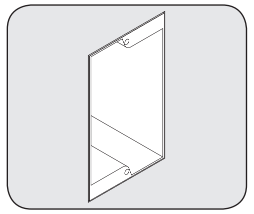
Pour une utilisation en intérieur/extérieur | **Para utilização interna/externa**

MT15	**Lecteur multitechnologique— Lecteur à commande unique**	**Leitor de multitecnologias— Caixa de distribuição única**
MTK15	**Lecteur multitechnologique à clavier— Lecteur à commande unique**	**Leitor de multitecnologias com teclado— Caixa de distribuição única**

Outils
- Tournevis cruciforme
- Taraud 6 - 32
- Mèches 1" (25 mm), ⅛" (3 mm)
- Mèche T10 Security Torx^{MD} (en option)

Ferramentas
- Chave de fenda Phillips
- Parafuso 6-32
- Brocas de 1" (25 mm), ⅛" (3 mm)
- Broca de segurança T10 Torx™ (Opcional)

1 Situez ou installez la boîte à commande unique. / Localize e/ou instale a única caixa de distribuição.



Consultez les directives du fabricant pour l'installation.

Consulte as instruções do fabricante para instalação.

2 Branchez le câble dans le module de contrôle. / Ligue o cabo ao módulo de controle.

Un boitier d'alimentation homologué Classe 2 UL 294 doit être utilisé.

Plage de tension : De 5 V à 16 V

Classificação de voltagem: 5V a 16V

Longueur max. jusqu'au panneau	
Longueur	**Calibre américain du fil**
60 m	22
90 m	20
150 m	18

Comprimento máximo para o painel	
Comprimento	**AWG**
60 m	22
90 m	20
150 m	18

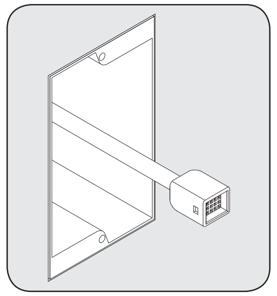
Courant @ 12 V et 25 C		
Modèle	**mA moyen**	**mA max.**
MT15, MT15-485	165	195
MTK15, MTK15-485	165	225

Corrente @ 12V e 25C		
Modelo	**Média mA**	**Máx. mA**
MT15, MT15-485	165	195
MTK15, MTK15-485	165	225

Connexions au câble	
Noir	Mise à la terre
Bleu	Inutilisé
Brun	Voyant de contrôle DEL rouge
Gris**	Inviolable
Vert	Donnée Wiegand 0 / Donnée
Orange	Voyant de contrôle DEL vert
Rose*	RS485-A/Y
Rouge	Mise en marche
Blindage	Mise à la terre
Sable*	RS485-B/Z
Blanc	Donnée Wiegand 1 / Horloge
Jaune	Contrôle de l'avertisseur

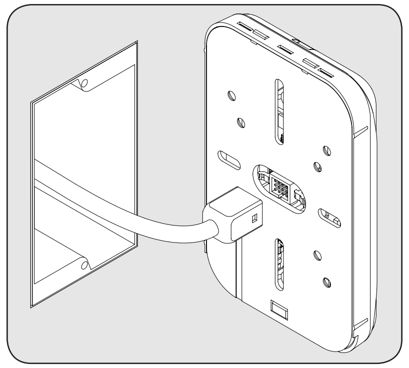
Conexões de cabos	
Preto	Terra
Azul	Não utilizado
Marrom	Controle de LED vermelho
Cinza**	Sem calçadeira
Verde	Dados Wiegand 0 / Dados
Laranja	Controle de LED verde
Rosa*	RS485-A/Y
Vermelho	Ligue
Blindado	Aterramento da proteção
Bege*	RS485-B/Z
Branco	Dados Wiegand 1 / Relógio
Amarelo	Controle de beeper

3 Passez le câble à travers la boîte. / Gire o cabo pela caixa.



4 Consultez la section OPTION DE LA PLAQUE DE BASE avant de continuer. / Veja a seção OPÇÃO DE PLACA BASE antes de continuar.

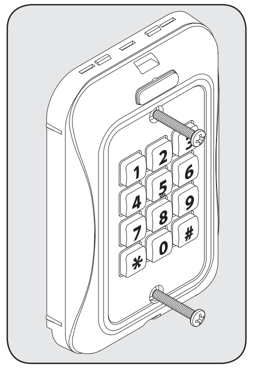
5 Branchez le câble dans le caisson. / Conecte o cabo na caixa.



* Ces fils sont inutilisés pour les lecteurs qui ne supportent pas de communication RS485.
** Les sorties antisabotage doivent être branchées à un système antivol UL.

* Esses fios não são usados para leitores que não suportam comunicação RS485.
** As saídas do tamper devem ser conectadas a um sistema anti-vandalismo certificado UL.

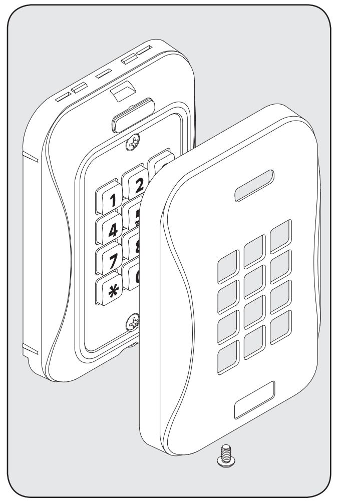
6 Installez le caisson. / Instale a caixa.



Si les vis de montage doivent être substituées, utiliser seulement une vis à tête cylindrique n ° 6.

Se utilizar parafusos alternativos, utilize parafuso tamanho 6.

7 Alignez le couvercle et installez la vis. / Prenda a tampa no lugar e instale o parafuso da tampa.



Inviolable Rivet à tête ronde Pin-in-Torx 6 - 32 x ¼", Utilisez si souhaité.	**Resistente à calçadeira** Cabeça arredondada presa com pino Torx 6-32 x ¼", Use, se desejado.
Regular 6-32 x ¼"	**Regular** 6-32 x ¼"

⚠ **Ne resserrez pas exagérément!** **Não aperte demais!**

TEST / TESTE

a Mettez le lecteur en marche. / Ligue o leitor.

Le voyant DEL s'allumera d'abord et le signal sonore retentira ensuite. Cela signifie que le lecteur est prêt.

Si le voyant DEL et l'avertisseur ne répondent pas, vérifiez les connexions au câble.

O LED se acenderá seguido por um sinal de bip. Isso indica que o leitor está pronto.

Se o led e o bip não responderem, verifique as conexões de cabos.

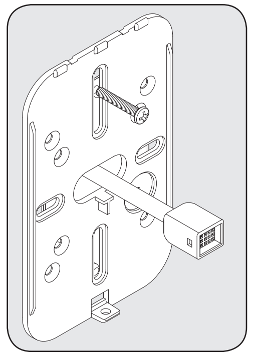
b Présentez une carte adéquate ou un jeton programmé pour faire fonctionner le lecteur. / Apresente um cartão adequado ou sinal programado para operar a máquina.

Voyants DEL	
Vert	La carte a été lue et acceptée
Rouge	La carte a été lue, mais n'a pas été acceptée (ne signifie pas une mauvaise installation)

Indicadores de LED	
Verde	O cartão foi lido e aceito
Vermelho	O cartão foi lido, mas não aceito (não indica instalação falha)

OPTION DE LA PLAQUE DE BASE / OPÇÃO DE PLACA DE BASE

i Installez la plaque de base. / Instale a placa base.



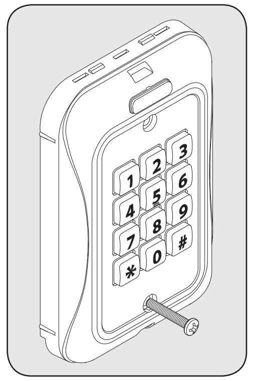
Utilisez cette option pour amplifier le caractère inviolable.

Passez à l'étape 5 après avoir effectué cette étape.

Use essa opção para uma resistência mais robusta da calçadeira.

Continue até a etapa 5 após concluir esta etapa.

ii Installez le caisson. / Instale a caixa.



Cette étape remplace l'étape 6.

Esta etapa substitui a etapa 6.

La connexion en RS485 ne doit pas être utilisée dans les applications S319 jusqu'à ce qu'un panneau S319 compatible soit identifié avec les communications RS485.

A conexão RS485 não deve ser utilizada em aplicativos S319 até que um painel compatível com S319 seja identificado pela comunicação RS485.

La conformité à la norme ULC-S319 n'est plus respectée si un ajout, une extension, une mémoire ou un autre module fabriqué ou fourni par le fabricant ou un représentant du fabricant est utilisé. L'installation d'un boitier d'alimentation homologue ULC-S319 est obligatoire au Canada.

Énoncés FCC
Cet appareil est conforme à la partie 15 des normes FCC. L'utilisation est soumise aux deux conditions suivantes : (1) Le dispositif ne doit pas émettre d'interférences nuisibles, et (2) ce dispositif doit accepter toutes les interférences reçues incluant celles pouvant nuire au fonctionnement.

Tous changements et toutes modifications à cet équipement sans l'approbation expresse de Schlage peut annuler l'autorisation de fonctionnement de cet équipement par son utilisateur.

Déclarations D'industrie Canada
Ce dispositif est conforme à la norme RSS d'Industrie Canada relative aux dispositifs exempts de licence. Le fonctionnement est assujetti aux deux conditions suivantes : (1) ce dispositif ne doit pas occasionner de brouillage, et (2) ce dispositif doit accueillir tout brouillage y compris le brouillage qui risque d'entraîner un mauvais fonctionnement du dispositif. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

A conformidade ULC-S319 perde a validade quando qualquer acessório, expansão, memória ou outro módulo fabricado ou fornecido pelo fabricante ou representante do fabricante é utilizado.

Declaração de Anatel
Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

CE

© Allegion 2014
Printed in U.S.A.
23940620 Rev. 10/14-d

23852973

KP2000E/EM Series Style Keypad

Installation and Programming Instructions
Models KP2000EXX and KP2000EMXX

Specifications

Parameter	**Specifications**	
Voltage Requirements	10-30 VDC; 12-24VAC	
Keypad Current Requirements (Max)	VDC	VAC
	10V: 85mA	12V: 150mA
	30V: 115mA	24V: 200mA
Relay Contact Rating	2A @ 30VDC (Main & Aux)	
REX Input	Normally Open Dry Contact	
Door Position Switch Input	Normally Closed Dry Contact	
Mechanical Dimensions	4.50” H x 2.75” W x 0.60” D	
Environment	Indoor or Outdoor	
Temperature Tolerance	-31°F to 151°F (-35ºC to 66°C)	
Front End Cable Type	Stranded and Shielded	
Front End Distance and Wire Gauge	1000 Ft. – 18AWG; 500 Ft – 20 AWG; 250 Ft. – 22 AWG	
Firmware Version	1.0x (“1” is the major version; “0” is the minor version; “x” is a minor version, reserved for bug fixes, which is indicated with a letter, such as “a”.)	

Keypad Operating Modes

The KP2000E/EM Series keypad has two operating modes: Standalone Mode and Wiegand Front End Mode. Below is a brief explanation of each mode. Refer to the programming section for details about selecting each mode.

Standalone Mode:

By default, the keypad is programmed for Standalone Mode. In this mode, all the users and other programming options are maintained within the keypad and no additional controller is required. The lock and all other inputs and outputs are connected directly to the keypad.

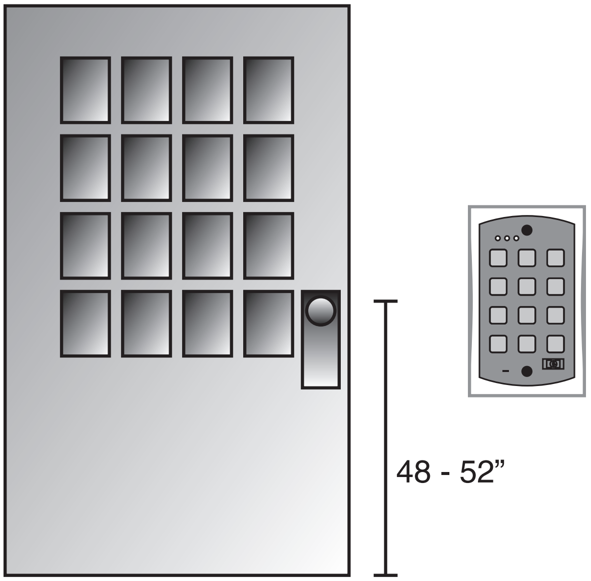
Wiegand Front End Mode:

In Wiegand Front End mode, a separate UL Listed compatible Wiegand Access Control panel is required. When you enter a code on the keypad it is then sent to the control panel as Wiegand card data, depending on which format you’ve programmed it for. The control panel maintains the users and programming options and makes all the access control decisions. The locking device and all inputs and outputs are connected to the control panel.

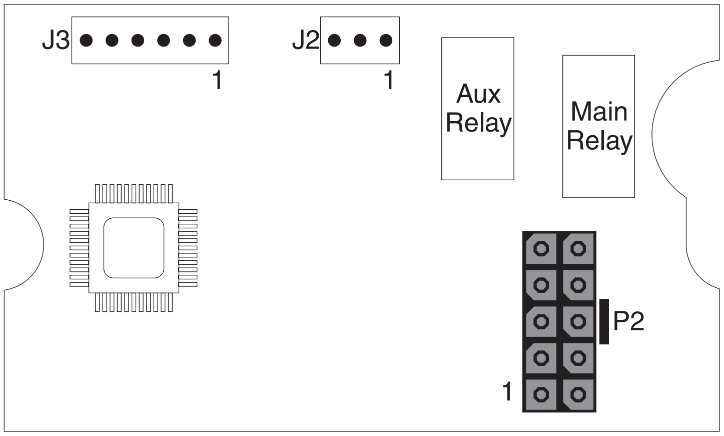
Mounting the Keypad

The keypad is designed to be flush mounted using a standard UL Listed single-gang electrical box. Mounting height can vary depending on requirements. An appropriate range is typically between 48 and 52 inches on center off the floor.

For outdoor installations, use a UL Listed weatherproof back box and seal the wire entry locations with silicone and provide a drain hole. For additional protection, install the provided foam gasket between the keypad and the back box. In addition, use the anti-oxidant grease pack for the wire harness connectors.

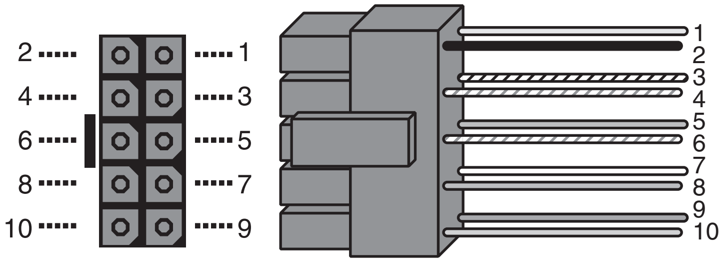


Circuit Board Diagram



Note: J3 is NOT USED

Main Wire Harness (P2)



Pin	Wire Color	Description
1	Red	V+ (Keypad Power)
2	Black	V- (Keypad Power)
3	White/Black	Wiegand Data 0/Secured Series Data
4	White/Yellow	Wiegand Data 1/Secured Series Data
5	Brown	Request to Exit (REX)/LED1
6	White/Orange	Loop Common
7	White	Door Position Switch Input
8	Green	Main Relay Normally Open
9	Blue	Main Relay Common
10	Gray	Main Relay Normally Closed

Auxiliary Relay Wire Harness (J2)

Pin	Wire Color	Description
1	Green	Aux Relay Normally Open
2	Blue	Aux Relay Common
3	Gray	Aux Relay Normally Closed

UL Requirements

The KP2000E/EM Series keypad is a UL Listed access control unit. This section contains information regarding the requirements necessary to meet UL compliance.

Wiring methods shall be in accordance with the National Electrical Code (ANSI/NFPA70), local codes, and the authorities having jurisdiction.

All wires and cables used must be a minimum of 22 AWG, stranded and shielded UL Listed and/or recognized wire suitable for the application. In addition, input and output cables that extend from the unit must be shielded, twisted pair. Ground the shield only at one end, usually the circuit end.

All interconnecting devices (ie. door contacts, REX, locking devices, alarm devices, doorbell, etc.) must be UL Listed.

A UL Listed access control power limited power supply, capable of 4 hours standby, must be used to power the keypad.

A minimum of three user codes must be programmed for controlling access.

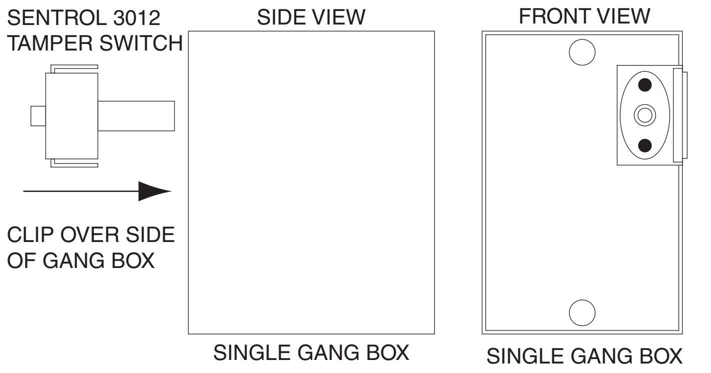
The following Wiegand card formats were not evaluated by UL: 28-bit, 29-bit, 30-bit, 31-bit, 32-bit or 36-bit (formats 2-8 from Wiegand format chart. UL did evaluate the 26-bit card format (format 1).

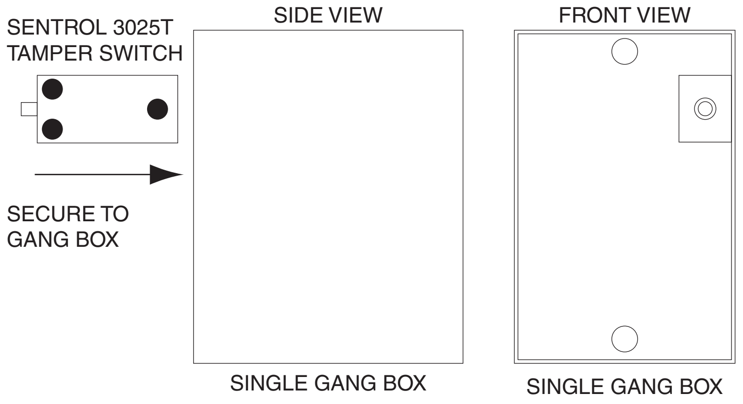
8-Bit Burst Mode was not evaluated by UL.

Installing a Tamper Switch

To meet UL requirements, a UL Listed tamper switch must be installed in a UL Listed single-gang box used for mounting the keypad. The tamper switch must activate if the keypad is removed from the box and must disconnect power from the lock. The lock must be a fail-secure device, meaning the lock remains locked when power is removed.

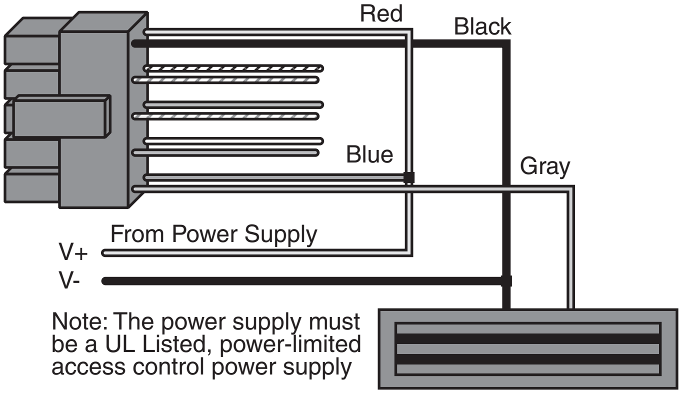
In addition, once the tamper device is activated, it must be configured so that it can only be reset from within the protected area. Only a Sentrol 3012 or Sentrol 3025T tamper switch can be used. The diagrams below show the suggested mounting location for each device.





Wiring a Maglock (Fail-Safe)

1. Connect the red wire (V+) to the blue wire (common), and then connect them to the positive on the power supply.
2. Connect the gray wire (normally closed) to the positive on the Maglock.
3. Connect the black wire (V-) to the negative on the Maglock, and then connect them both to the negative on the power supply.

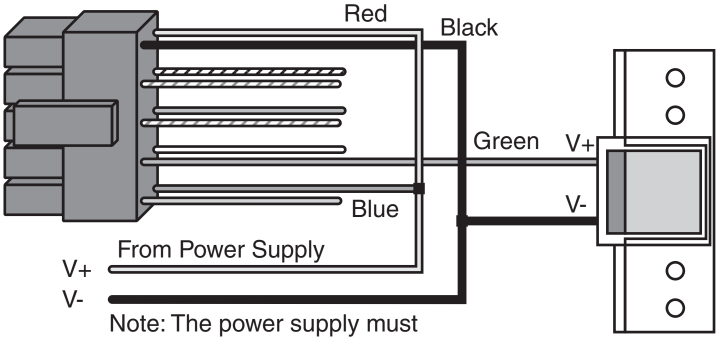


Note: The power supply must be a UL Listed, power-limited access control power supply

Maglock (Fail-Safe)

Wiring an Electric Door Strike (Fail-Secure)

1. Connect the red wire (V+) to the blue wire (common), and then connect them to the positive on the power supply.
2. Connect the green wire (normally open) to the positive on the strike.
3. Connect the black wire (V-) to the negative on the strike, and then connect them both to the negative on the power supply.

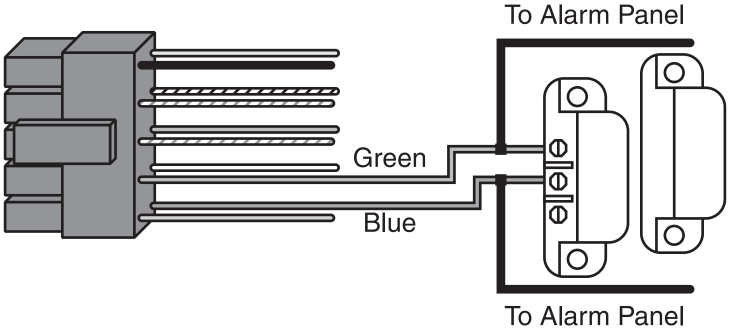


Note: The power supply must be a UL Listed, power-limited access control power supply

Electric Strike (Fail-Secure)

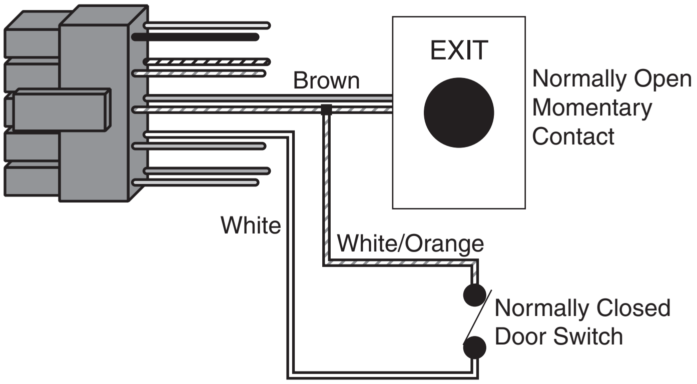
Shunting a Normally Closed Zone

1. Connect the blue wire (common) to the common connection on the door position switch.
2. Connect the green wire (normally open) to the normally closed connection on the door position switch.



Wiring the REX and Door Position Switch

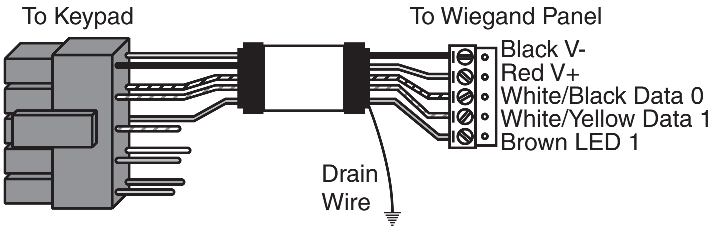
1. Connect the brown wire (REX Input) to the normally open connection on the REX device.
2. Connect the white/orange wire (loop common) to the common on the REX device and the common on the door switch.
3. Connect the white wire (door loop) to the normally closed connection on the door switch.



Note: By default, the forced door and propped door outputs are assigned to the audio alerts. When you power up the keypad for the first time and door contacts are not connected, you may hear audio alert #1 immediately followed by audio alert # 2 thirty seconds later. If you are not using door contacts you must either short the white and white/orange wires together or disable the audio alerts.

Wiegand Front End Wiring Diagram

To use the keypad as a Wiegand Front End, connect the red, black white/black, white/yellow and brown wires on the main keypad wire harness to the corresponding terminals on the UL Listed compatible Wiegand control panel. The drain wire must be connected at the panel side only. Refer to the wiring distance and gauge in the specifications chart.



Changing the Master Code

The first step in setting up your keypad is to enter program mode and change the master code. The default master code is 1234.

1. Enter Program Mode
   Press: 99 # master code * (Yellow LED Flashes Slowly)
2. Change Master Code
   Press: 1 # new master code * repeat code * (Yellow LED Flashes Slowly)
3. Exit Program Mode
   Press: * (Yellow LED Stops Flashing)

Programming a Supervisor Code

Use the following command sequence to program a supervisor code, which is stored user location 2. The supervisor is only allowed to add, delete and disable users .

1. Enter Program Mode
   Press: 99 # master code * (Yellow LED Flashes Slowly)
2. Change Supervisor Code
   Press: 2 # supervisor code * repeat code * (Yellow LED Flashes Slowly)
3. Exit Program Mode
   Press: * (Yellow LED Stops Flashing)

Selecting Wiegand Front End Mode

To select Wiegand Front End Mode, use the following steps:

1. Enter Program Mode
   Press: 99 # master code * (Yellow LED Flashes Slowly)
2. Select Wiegand Front End Mode, press:
   1032 # 0 # 1 # ** (Yellow LED Flashes Slowly)
3. Exit Program Mode
   Press * (Yellow LED Stops Flashing)
4. Any other LED blinking sequence indicates a programming error. Repeat the steps listed above to correct the problem.

Selecting Standalone Mode

Standalone Mode is the default operating mode. If you've changed the operating mode and want to revert back to Standalone Mode, use the following steps:

1. Enter Program Mode
   Press: 99 # master code * (Yellow LED Flashes Slowly)
2. Select Standalone Mode
   Press: 1032 # 0 # 0 # ** (Yellow LED Flashes Slowly)
3. Exit Program Mode
   Press * (Yellow LED Stops Flashing)
4. Any other LED blinking sequence indicates a programming error. Repeat the steps listed above to correct the problem.

Note: If the unit is not connected, the Yellow LED turns on solid after the yellow flash. Press the * key to clear.

Programming Users

(Standalone Mode Only)

The unit can hold up to 500 users. Codes are 1 to 10 digits in length.

Command/Action	Keys to Enter/Details
Add Standard User (short)	user location # code * code *
Add Standard User with Specific Unlock Time	unlock time # user location # code * code *
Add Enhanced User	60 # user type # user location # code * code *
Add User to Trigger Specific Outputs (Lock, OUT2-10)	59 # outputs # user location # code * code * (1 = Lock, 2 = OUT2, 3 = OUT 3, Etc)
Disable User	56 # 0/1 # user location # ** (0 = enabled; 1 = disabled)
Delete User	user location # **

User Types
(Standalone Mode Only)

User Types	Description
Toggle User (0)	A toggle user latches the Lock Output like an on/off switch. When you enter the code the first time, the Lock Output is activated and remains activated until you enter any toggle code.
Standard User (1)	This user type is a standard timed user that activates the lock output for the time duration programmed with command 11 or with the master code.
Lockout User (3)	A Locks Out User is used to lock out users from the keypad. After entering a lock out code, users in a higher user location are denied access. To clear a lock out, enter the same lock out code you used to enter lock out mode.
Single Use Code (5)	This user code can only be used once. After entering the code, the user is deleted from memory. To verify a single use code is still programed, enter 5 # code *. If the code wasn't used, the green LED flashes for ½ a second.
Emergency User (7)	An emergency user operates as a standard timed user, with one exception, it can't be Locked Out by a lock out user.
Duress User (8)	The duress user is another type of emergency user. This user activates both the Lock and Duress Outputs. You would use this code if you wanted to activate an alarm, as well as gain entrance through the door.
Two-Part User Type A (9)	This user type is one half of a two-part user combination. When you enter a type A user code, you must enter a Type B user code to gain access through the door. After entering the code the bi-color LED alternates red and green. You have 15 seconds to enter the second code.
Two-Part User Type B (10)	This user type is the second half of a two-part user combination. After entering a Type B code you must enter a Type A code to gain access through the door.

Assigning Virtual Outputs to Physical Outputs
(Standalone Mode Only)

The keypad is equipped with nineteen Virtual Outputs and twelve Physical Outputs. Virtual Outputs are functions that you can assign to operate any Physical Output. Physical Outputs include the main relay and the two audio alerts on the keypad..

- Using command 10, you can assign any Virtual Output to any Physical Output or disable a Physical Output.
- Each Physical Output can have multiple Virtual Output assigned to it.

Assigning Outputs
(Standalone Mode Only)

Command/Action	Keys to Enter/Details
Assign Outputs	10 # virtual output # physical output # **
Virtual Outputs	Physical Outputs
1 – Lock Output	1 – Main Relay
2 – Alarm Shunt	2 – Aux Relay
3 – Propped Door	
4 – Forced Door	
5 – OUT2	
6 – OUT3	
7 – OUT4	
8 – OUT5	
9 – OUT6	
10 – OUT7	
11 – OUT8	11 – Audio Alert 1
12 – OUT9	12 – Audio Alert 2
13 – OUT10	Note: The keypad is equipped with only two relays.
14 – Duress Output	
15 – Panic Output (see page 5)	
16 – Keypad Active Output	
17 – Doorbell Output*	
18 – REX Input Active	
19 – Door Loop Input Active	
*Note: The Doorbell Output also works in both Front End Modes.	
Disable Virtual Output	10 # virtual output # 0 # **
Disable Physical Output	10 # 0 # physical output # **
Programming the REX/Door Loop Outputs (Lock, OUT2-10)	49 # outputs # input # ** Outputs: Lock =1, OUT2 = 2, OUT3 = 3, OUT4 = 4, etc Input: REX = 0; Door Loop = 1)

Note: The default output settings are: Lock Output = Main Relay; Alarm Shunt = Aux Relay; Forced Door = Audio Alert 1; Propped Door = Audio Alert 2.

Programming Output Times

(Standalone Mode Only)

Command/Action	Keys to Enter/Details
Change Lock Output Time	11 # time # 0 # ** (1-255 sec)
Set OUT2 Time Duration	12 # ttt # mmm # **
Set OUT3 Time Duration	13 # ttt # mmm # **
Set OUT4 Time Duration	14 # ttt # mmm # **
Set OUT5 Time Duration	15 # ttt # mmm # **
Set OUT6 Time Duration	16 # ttt # mmm # **
Set OUT7 Time Duration	17 # ttt # mmm # **
Set OUT8 Time Duration	18 # ttt # mmm # **
Set OUT9 Time Duration	19 # ttt # mmm # **
Set OUT10 Time Duration	110 # ttt # mmm # **
Set Propped Door Time	44 # time # 0 # ** (10-990 sec)
Set Forced Door Time	45 # time # 0 # ** (10-990 sec)

Note: OUT2-10: ttt = time units; mmm = multiplier. Ex: "12 # 2 # 5 # **" = 10 seconds (2 time units multiplied by 5 seconds = 10 seconds). The maximum value of ttt and mmm is 255 (255 x 255). The default output times (Lock Output, OUT2-10) are 5 seconds. To toggle the output enter 0 for both ttt and mmm; Ex: 12 # 0 # 0 # **.

Programming Keypad Options

(Default settings are in bold)

Command/Action	Keys to Enter/Details	
Change Keypad Options	30 # option # setting # **	
Option	Setting	
0 – Audio Keypress Feedback	0 = Disabled	1 = Enabled
1 – Visual Keypress Feedback	0 = Disabled	1 = Enabled
2 – Auto Entry	0 = Disabled	1 = Enabled
3 – Error Lockout	0 = Disabled	1 = Enabled
4 – User Lockout	0 = Disabled	1 = Enabled
5 – Two-Part Users	0 = Disabled	1 = Enabled
6 – Keypad Backlighting	0 = Disabled	1 = Enabled
7 – Keypad Backlight Dimming	0 = Disabled	1 = Enabled
8 – REX Processing Select	0 = Only when door closed	1 = Always
9 – Red LED Dimming	0 = Off when backlighting dim	1 = Always On
10 – Door Loop Output Processing	0 = Not when lock latched	1 = Always
16 – Secured Series In/Out	0 = Records IN	1 = Records Out
18 – 8-Bit Burst Output	0 = Disabled	1 = Enabled
19 – WFE Red LED Select	0 = Disabled	1 = Enabled
20 – WFE Red LED Active State	0 = Low	1 = High
21 – WFE Green LED Select	0 = Disabled	1 = Enabled
22 – WFE Green LED Active State	0 = Low	1 = High
Note: WFE means Wiegand Front End		

Programming Keypad Parameters

(Default settings are in bold)

Command/Action	Keys to Enter/Details
Change Keypad Parameters	32 # parameter # value # **
Parameter	Value
0 – Duress Output Duration	1 – 255 Seconds (default = 5)
1 – Panic Output Duration*	1 – 255 Seconds (default = 5)
2 – Error Lockout Threshold	1 – 50 Attempts (default = 3)
3 – Error Lockout Duration	1 – 255 Seconds (default = 10)
4 – Auto-Entry Count	2 – 10 Digits (default = 4)
7 – Auto-Entry Keypress Timeout	2 – 15 Seconds (default = 2)
10 – Wiegand Format	1 – 8 (default = 1, 26-Bit)
11 – Wiegand Pulse Width	1 – 255 (default = 8, 160µS)
12 – Wiegand Interpulse Spacing	1 – 255 (default = 32, 640µS)
Note: Refer to the Wiegand Format Chart below for parameter 8.	
Change Wiegand Parameters	34 # parameter # value # **
Parameter	Value
0 – Wiegand Site ID	Refer to Wiegand Format Chart
1 – Wiegand Group ID	Refer to Wiegand Format Chart
Note: The default setting for both settings is 0.	

*Note: The Panic Output is activated by pressing the * and # keys at the same time. This is used in case of emergency to activate an auxiliary alarm device, such as a siren, that is used to indicate an emergency condition only. This output should not be used to gain access. All access control functionality should be programmed and remain separate from the Panic Output functionality.

Resetting the Keypad

Note: This does not reset the keypad operating mode.

Command/Action	Keys to Enter/Details
Reset Defaults Only	40 # 00000 # 00000 # **
Reset Entire Keypad	46 # 00000 # 00000 # **

Wiegand Format Chart

The keypad supports the following Wiegand formats (parameter 10).

Format Value	Wiegand Format	Largest PIN Value	Largest Site Value	Largest Group Value
1	26 bit	65535	255	N/A
2	28 bit	32767	255	N/A
3	29 bit	524287	255	N/A
4	30 bit	65535	255	15
5	31 bit	65535	255	31
6	32 bit	8191	2047	63
7	36 bit	999999	1023	N/A
8	29 bit	524287	255	N/A

Wiegand Data

When the keypad is configured in Wiegand mode, the keypad data is sent as a complete Wiegand data packet, as though you presented a card.

LED/Sounder Indications

Indicator	Description
Steady Red*	Door Locked
Steady Green*	Door Unlocked (timed or latched)
Yellow Flashing Slowly	Program Mode
Solid Yellow	Program Error or Error Lockout
Alternating Red/Green	Awaiting 2nd PIN of Two-Part User
LED's Cycling Left to Right	Over Voltage Warning
LED's Cycling Right to Left	Under Voltage Warning
3 Rapid Beeps	Invalid Code
Pair of Double Beeps	User Lockout Activated
Single Double Beep	User Lockout Canceled
1 Long Beep, 1 Short Beep	Access Denied, User Disabled
1 Long Beep, 3 Short Beeps	Access Denied, User Lockout
1 Long Beep, 5 Short Beeps	Access Denied, Code Mismatch
6 Quick Beeps	Toggle Mode Activated
Sounder ¼ sec on, ¼ sec off	Audio Alert 1
Beep Every 2 seconds	Audio Alert 2

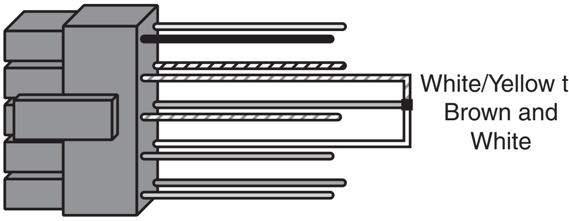
*Note: The Red/Green LED descriptions above are for Standalone Mode only. The operation of these LED's in Wiegand Mode is determined by the LED control wire (brown) and how it is configured. The LED control is configured using keypad options 19, 20, 21 and 22, which are programmed with command 30.

Performing the Programming Mode Loopback

The keypad has a special loopback connection you can make to enter program mode if you do not know the master code. Use the following steps below and refer to the diagram.

Note: This procedure should only be performed by a qualified security or lock industry professional.

1. Power down the keypad.
2. Connect the white/yellow, brown and white wires together and disconnect any other connections to these wires.
3. Power up the keypad
4. Change the master code or default the keypad
5. Power down the keypad and remove the loopback connections and reconnect any other wiring to these wires.
6. Power up the keypad.



Performing the Keypad Self-Test

After installing the keypad, Schlage recommends that you perform the keypad self-test once a year to ensure that the keypad is working properly.

1. To perform the self-test, with the unit powered up, press the following keys on the keypad: 7890#123456*
2. If all 12 key presses are accepted, the keypad enters self-test mode.
3. The LEDs then turn on one at time with a beep in the following order Red, Yellow then Green.
4. After the Green LED, the unit then flashes an LED to indicate which operating mode the keypad is programmed mode. Below shows which LED flashes for each mode:
   - Standalone Mode: Red Flash
   - Wiegand Front End Mode: Green Flash

Programming Wiegand Front End Mode Options

This section contains programming commands that apply only to Wiegand Front End Mode.

Enabling/Disabling 8-Bit Burst Output

8-Bit Burst Mode is an alternate keypad output format.This mode functions only when the keypad is programmed as a Wiegand Front End. When enabled, normal Wiegand operation is disabled and each key press is sent as a separate 8-bit number. The chart below shows these numbers.

1. Enter Program Mode.
   - Press: 99 # Master Code *
   - The yellow LED flashes slowly.
2. To enable 8-Bit Burst Output, press: 30 # 18 # 1 # **
   - The yellow LED continues to blink slowly.
   - To disable 8-Bit Burst Output, press: 30 # 18 # 0 # **
   - The yellow LED continues to blink slowly.
3. Exit Program Mode.
   - Press: *
   - The yellow LED stops flashing.

Key	Binary Data
1	11100001
2	11010010
3	11000011
4	10110100
5	10100101
6	10010110
7	10000111
8	01111000
9	01101001
0	11110000
*	01011010
#	01001011

ALLEGION™

Customer Service

1-877-671-7011 www.allegion.com/us

Printed in U.S.A.
23852973 Rev. 12/14-b

23852890

KP212 Keypad

Installation and Programming Instructions

Specifications

Case Dimensions:
6½"L x 1¾"W x 1⅛"D

Electrical:
Voltage: 12-24VAC/DC

Current: 53mA@12VDC;
72mA@24VDC; 95mA@12VAC
108mA@24VAC

Relay Contacts:
Main Relay (controller): 2A

Bell Relay:
Form A; 1 Amp @ 30VAC/DC

Environmental:
-20° F to 130° F
For Indoor and Outdoor Use

Features

- 120 User Capacity
- Programmable Relay Time (0 to 99 seconds)
- Request to Exit (REX) Input
- Vandal Resistant Case
- Sealed for Indoor or Outdoor Applications
- LED's for Relay Status Indication
- Bell Output
- Surface Mount
- Illuminated Hardened Keys
- Rated for Greater than One Million Key Cycles

Applications

- Low to Medium/Heavy Traffic Areas
- Rough Service Environments
- Mullion Frame Mounting
- Dimly Lit Areas

Description:
Schlage's KP212 keypad combines elegant looks with a mullion mount design in a rugged, vandal resistant case, which you can use for almost any application. The KP212 has hardened backlit keys designed to perform in medium to high traffic areas and in rough duty environments. The electronics are also conformal coated, which makes the keypad suitable for indoor or outdoor applications.

Basic Operation:
To gain access through the door enter your code (1-6 digits) followed by the * key on the keypad.

Packing List:
1) KP212 Keypad

(1) Eight-Conductor Wire Harness

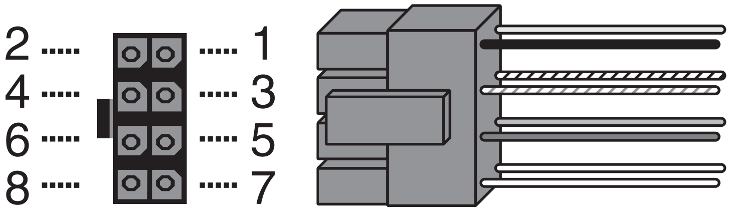
(1) Mullion Hardware Pack

(1) 5⁄64" Allen Wrench

(1) Anti-Oxidant Grease Pack

(1) Installation/Programming Manual

Wire Harness Configuration:



Pin	Wire Color	Signal Name
1	Red	Power (+)
2	Black	Power (-)
3	White/Black	REX
4	White/Yellow	Main Relay NC
5	Blue	Main Relay Common
6	Brown	Main Relay NO
7	White	Bell Relay Contact (A)
8	White	Bell Relay Contact (B)

Customer Service

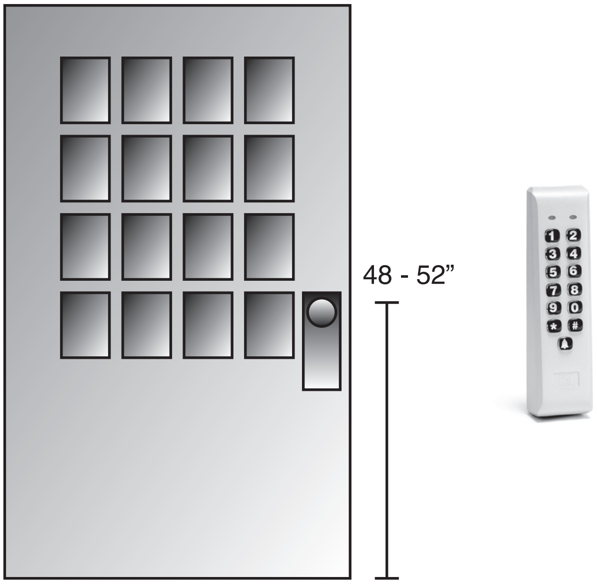
1-877-671-7011 www.allegion.com/us

Keypad Installation Procedure:

1. Drill through the back plate using a 11⁄64" bit. Use the template on the back page to accurately mark the mounting holes before drilling. Then drill the mounting holes with a 9⁄64" drill bit. Also drill the hole for the wires. This may vary depending on the number of conductors required. Refer to mounting height below.
2. Wire the keypad using the diagrams in the following sections.
3. Mount the KP212 keypad onto the mounting surface using the provided screws. Do no over-tighten the screws, which may result in damage.

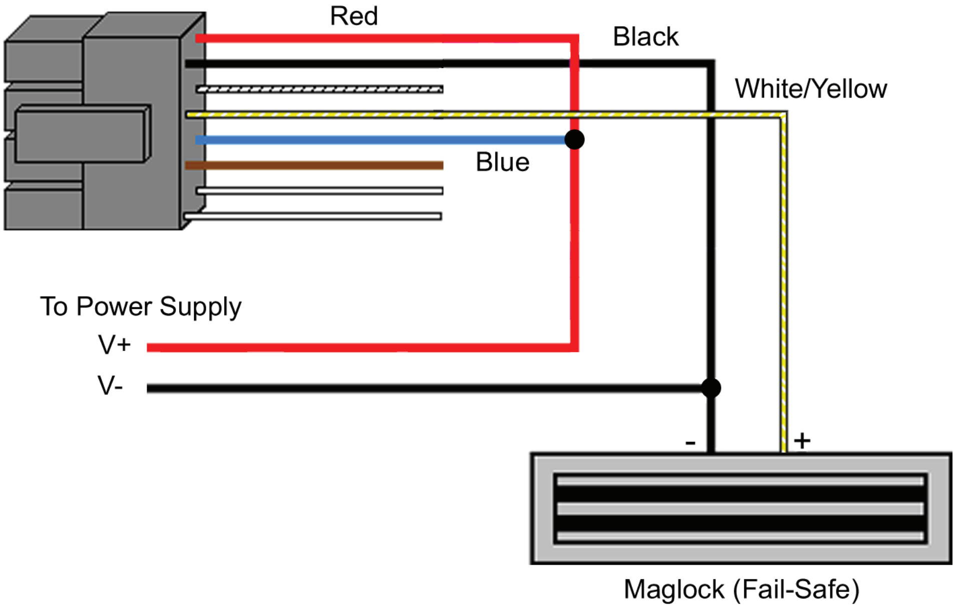
Keypad Mounting Height

Mounting height can vary depending on requirements. An appropriate range is typically between 48 and 52 inches on center off the floor.



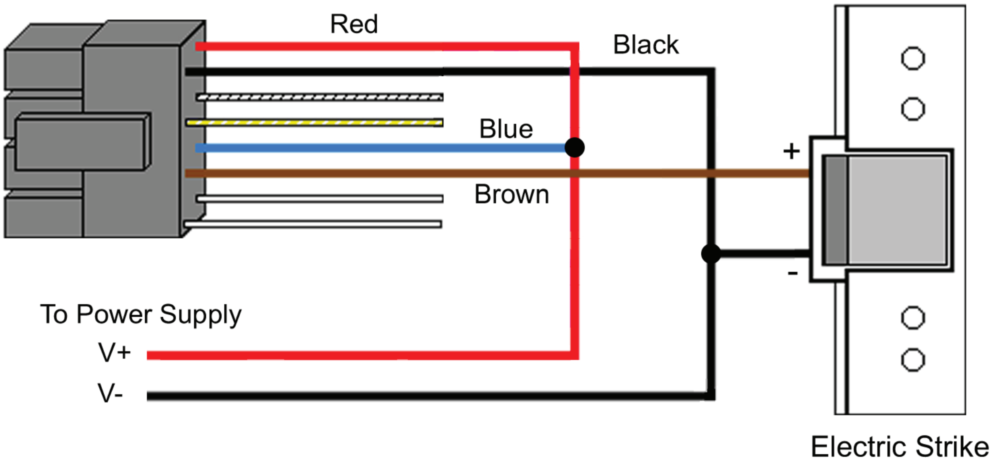
Wiring an Electromagnetic Lock (Maglock)

1. Connect the red (V+) and black (V-) wires to your power supply.
2. Connect the blue wire (relay common) to positive on your power supply.
3. Connect the white/yellow wire (relay normally closed) to the positive connection on your maglock.
4. Connect negative connection on your maglock to the negative on the power supply.



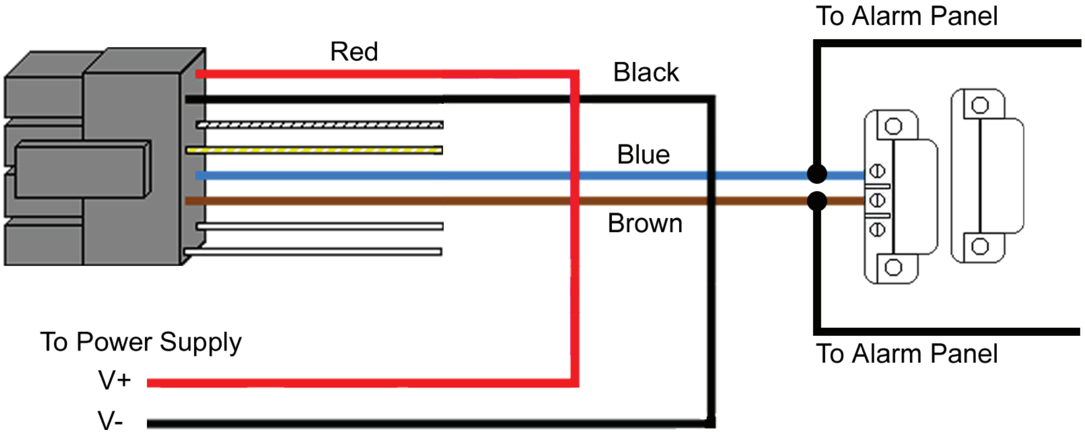
Basic Access Control Using an Electric Door Strike

1. Connect the red (V+) and black (V-) wires to your power supply.
2. Connect the blue wire (relay common) to positive on your power supply.
3. Connect the brown wire (relay normally open) to the positive connection on your door strike.
4. Connect negative connection on your door strike to the negative on the power supply.



Shunting a Normally Closed Zone

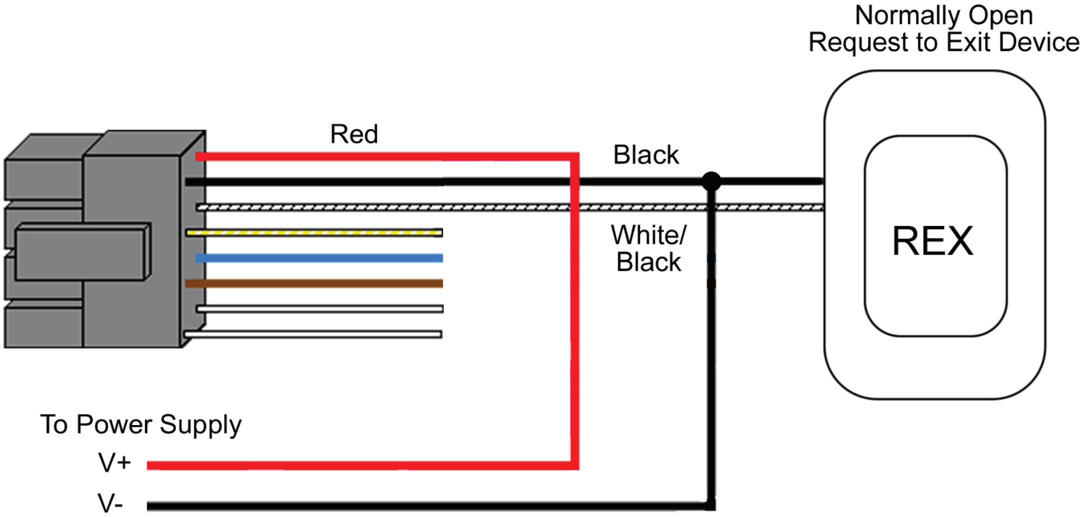
1. Connect the red (V+) and black (V-) wires to your power supply.
2. Connect the blue wire (relay common) to the common connection on the alarm contacts.
3. Connect the brown wire (relay normally open) to the normally open connection on the alarm contacts.



Wiring a Request to Exit Device (REX)

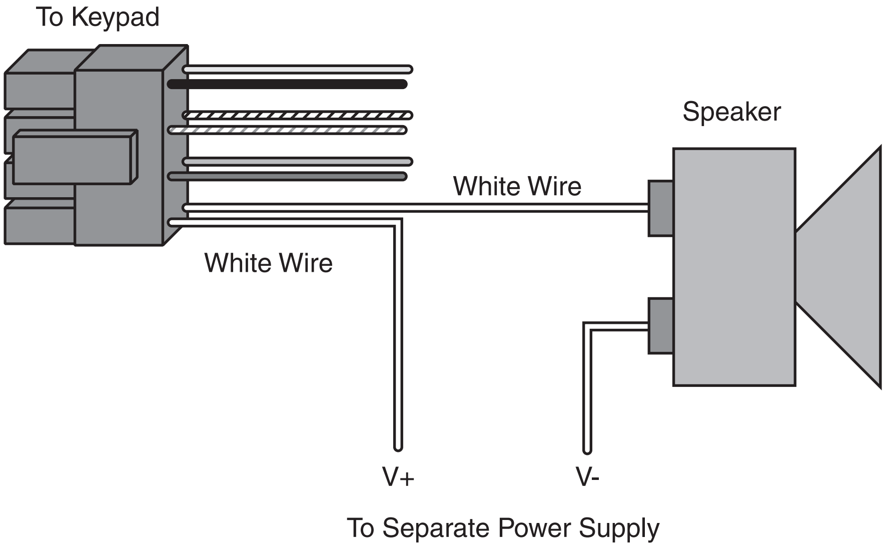
The KP212 is equipped with a REX input. The normally open REX input triggers the main relay for the amount of time you programmed for the master code. If the master code is set to toggle, the REX only triggers the relay for 5 seconds. There is no programming required for the REX to operate.

1. Connect the red (V+) and black (V-) wires to your power supply.
2. Connect the common connection on the REX device to the negative on your power supply.
3. Connect the white/black wire to the normally open connection on the REX device.



Wiring the Bell Output to a Speaker:

The KP212 keypad has a built in bell button, which triggers a relay output when pressed. This relay is normally open and the contact closes when triggered. You can use this relay output to trigger devices that require a momentary closure, such as a doorbell. The relay output provides a dry contact, but you can run up to 30VAC/DC through it for devices that require power to operate. The diagram below shows these connections.



Programming the KP212 Keypad

To program the KP212 you first must enter program mode. To enter program mode enter the following on the keypad: **99 # program code *** (default program code is 1234).

Keypad Default Settings

Option	Default Setting	Option	Default Setting
Master Code	1234	Main Relay Time	5 Seconds
Audio Keypress Feedback	Enabled	Visual Keypress Feedback	Enabled
Auto-Entry	Disabled	Door Bell Select	Continuous
Keypad Illumination	Enabled	Keypad Dimming	Enabled

Programming Options Chart

Command/Action	Keys to Enter/Details	
Change Master Code	**1 # new code * new code ***	
Change Main Relay Time	**relay time # 1 # master code * master code ***	
Add/Change User	**user location # new code * new code *** Note: Users programmed with this command use master code relay time.	
Add Toggle User	**00 # user location # new code * new code ***	
Add User with Specific Relay Time	**relay time # user location # new code * new code ***	
Command 30 Set/Clear Keypad Options (options below, **defaults in bold)**	**30 # option # set/clear # ****	
Option	**Clear**	**Set**
0 – Audio Keypress Feedback	0 = Disabled	**1 = Enabled**
1 – Visual Keypress Feedback	0 = Disabled	**1 = Enabled**
2 – Auto-Entry	**0 = Disabled**	1 = Enabled
3 – Keypad Illumination	0 = Disabled	**1 = Enabled**
4 – Keypad Dimming	0 = Disabled (always bright)	**1 = Enabled**
5 – Door Bell Select	0 = Disabled	**1 = Enabled**
Command 32 Set Bell Output Time	**32 # 0 # time # * ***	Set timed output (1 – 99 seconds)
	32 # 0 # 0 # * *	Set to continuous
Command 46 Reset Keypad to Default Settings	**46 # 00000 # 00000 # * ***	
Exit Program Mode	Press the * Key	

Notes:

1. The KP212 can store 120 user codes, including the master code. Codes can be from 1 to 6 digits long.
2. When auto-entry is enabled, users with codes the same length as the master code do not have to press the * key after entering their code to enter the door.
3. When keypad dimming is disabled the backlighting remains at full intensity (does not dim).
4. When the door bell output is set to continuous the relay is energized as long the door button is pressed. When you release the button the relay de-energizes.

Programming Examples

Changing the Master Code:

The following example show how to change the master code to 4875 from the default of 1234.

1. Enter Program Mode	99 # 1234 *
2. Program New Master Code	1 # 4875 * 4875 *
3. Exit Program Mode	*

Change the Main Relay Time

The following example shows how to change the main relay time. The master code is 4875.

1. Enter Program Mode	99 # 4875 *
2. Change the Main Relay Time	10 # 1 # 4875 * 4875 *
3. Exit Program Mode	*

Adding User Codes:

The following example shows how to program user 2 with a code of 1749 and user 3 with 9328. The master code is 4875.

1. Enter Program Mode	99 # 4875
2. Program User	# 2 2 # 1749 * code *
3. Program User	# 3 3 # 9328 * code *
4. Exit Program Mode	*

Programming a Toggle User

The following example shows how to program user 4 as a toggle user with a code of 98773. The master code is 4875.

1. Enter Program Mode	99 # 4875 *
2. Change the Main Relay Time	00 # 4 # 98773 * 98773 *
3. Exit Program Mode	*

LED Indications

LED State	Description
Red Solid	Door Locked
Green Solid	Door Unlocked
Yellow Solid	Programming Error
Yellow Flashing Slowly	Program Mode
Yellow Momentary Flash	Visual Keypress Feedback

Troubleshooting

Issue	Explanation	Solution
LED's cycling slowly from right to left.	The KP212 Mullion is designed to monitor for low voltage. Once low voltage is detected, the keypad turns off the backlighting to ensure operation of the keypad until the problem can be attended to.	Verify the power supply output voltage. If it is below the voltage threshold of 7.5 Volts AC or 9 Volts DC, you must increase the voltage to between 12-24 Volts.
LED's cycling rapidly from left to right and the keypad has lost all operation.	The KP212 Mullion is designed to monitor for over voltage. This is a very "severe" condition and significantly affects the keypad's operation. Once the over voltage is detected, the keypad shuts down all operation and does not operate until the voltage is lowered.	Verify the power supply output voltage. If it is over the voltage threshold of 35 Volts, you must lower the voltage below 29 Volts.
Can't access programming mode using the master code.	The code you are entering is likely not the master code.	Perform the program mode loopback in the following section to enter program mode and reprogram the master code.
No LED's are lit on the keypad.	Power is not reaching the keypad.	First verify there is voltage at the keypad. If not, verify there is voltage at the power supply. If there is voltage, verify continuity on the wires out to the keypad. Otherwise contact the power supply manufacturer or IEI, if there is a problem with the keypad. You also may try power the keypad with a 12V battery to verify operation.

DEALERS/INSTALLERS ONLY! End users must contact the dealer/installer for support. If the keypad still does not work after troubleshooting, please call IEI's techinal support department at 1-800-343-9502 (outside MA) or 1-800-733-9502 (inside MA).

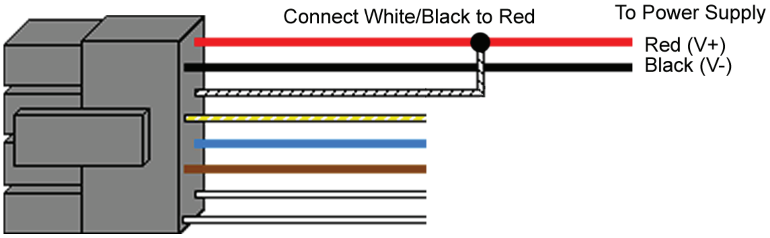
Testing the Keypad

After installing the keypad, IEI recommends that you perform the keypad self-test once a year, to ensure that the keypad is working properly.

- To perform the self-test, with the unit powered up, press the following keys on the keypad: 7890#123456*
- If all 12 key presses are accepted, the keypad enters self-test mode.
- The LEDs alternate three times followed by the sounder beeping three times.

Program Mode Loopback

If you've forgotten the master code use the following loopback connection to enter program mode. Power down the unit, short the white/black wire to the red wire, then power the unit back up. The yellow LED should be flashing. Now change your master code or reset the unit. Power the keypad down and reconnected the wire harness in the original configuration.



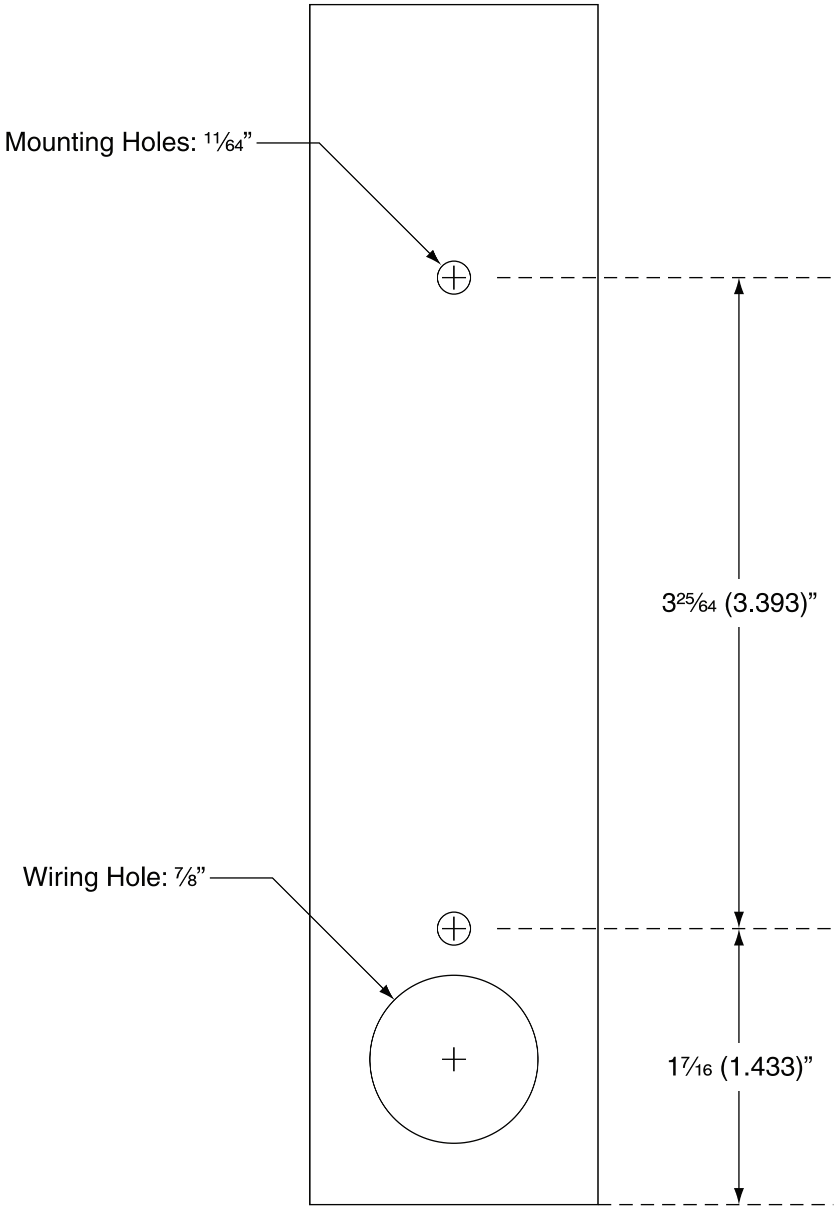
Warranty

International Electronics Inc. (IEI) warrants its products to be free from defects in material and workmanship when they have been installed in accordance with the manufacturer's instructions and have not been modified or tampered with. IEI does not assume any responsibility for damage or injury to person or property due to improper care, storage, handling, abuse, misuse, normal wear and tear, or an act of God.

IEI's sole responsibility is limited to the repair (at IEI's option) or the replacement of the defective product or part when sent to IEI's facility (freight and insurance charges prepaid) after obtaining IEI's Return Material Authorization. IEI will not be liable to the purchaser or any one else for incidental or consequential damages arising from any defect in, or malfunction of, its products.

Except as stated above, IEI makes no warranties, either expressed or implied, as to any matter whatsoever, including, and without limitation to, the condition of its products, their merchantability, or fitness for any particular purpose.

Keypad Mounting Template



The Schlage keypad is desingd for surface mount applications. You must drill a 7⁄8” hole for the wire harness connector, as shown, so the unit is flat against the mounting surface.

ALLEGION

Printed in U.S.A.

23852841

KP232 Keypad

Installation and Programming Instructions

Specifications

Case Dimensions:

6½”L x 1¾”W x 1⅛”D

Electrical:

Voltage: 5-12VDC (reader)
12-24VAC/DC (controller)

Current (max): 120mA

Relay Contacts:

Main Relay (controller): 2A

Aux Relays (controller): 1A

Bell Relay:
Form A; 1 Amp @ 30VDC;
500mA @ 125VAC

Environmental:

-20° F to 130° F

Description:

The KP232 Access Control unit consists of two pieces: an SSWiLM keypad front end and a 232 Access Control Module. Schlage’s Door-Gard Series SSWiLM keypad combines elegant looks with a mullion mount design in a rugged, vandal resistant case, which you can use for almost any application. The SSWiLM has hardened backlit keys designed to perform in medium to high traffic areas and in rough duty environments. The electronics are also conformal coated, which makes the keypad suitable for indoor or outdoor applications.

Basic Operation:

To gain access through the door enter your code (1-6 digits) followed by the * key on the keypad.

Packing List:

(1) SSWiLM Keypad

(1) Schlage 232 Controller

(1) Eight-Conductor Wire Harness

(4) Three-Conductor Wire Harness

(1) Controller Hardware Pack

(1) Mullion Hardware Pack

(1) 5⁄64” Allen Wrench

(1) Anti-Oxidant Grease Pack

(1) Installation/Programming Manual

(1) Self-Contained Access Control Programming Guide

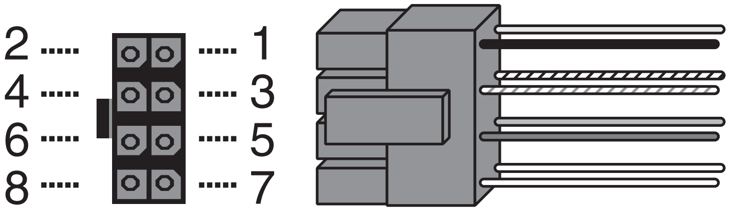
Features

- Vandal Resistant Case
- Sealed for Indoor or Outdoor Applications
- LED’s for Relay Status Indication
- Bell Output
- Surface Mount
- Illuminated Hardened Keys
- Rated for Greater than One Million Key Cycles

Applications

- Low to Medium/Heavy Traffic Areas
- Rough Service Environments
- Mullion Frame Mounting
- Dimly Lit Areas

Wire Harness Configuration:



Pin	Wire Color	Signal Name
1	Red	Power (+)
2	Black	Power (-)
3	White/Black	Data 0
4	White/Yellow	Data 1
5	Blue	Not Used
6	Brown	Not Used
7	White	Bell Relay Contact (A)
8	White	Bell Relay Contact (B)

Wiring Requirements:

18 AWG – 1000 Ft.

20 AWG – 500 Ft.

22 AWG – 250 Ft.

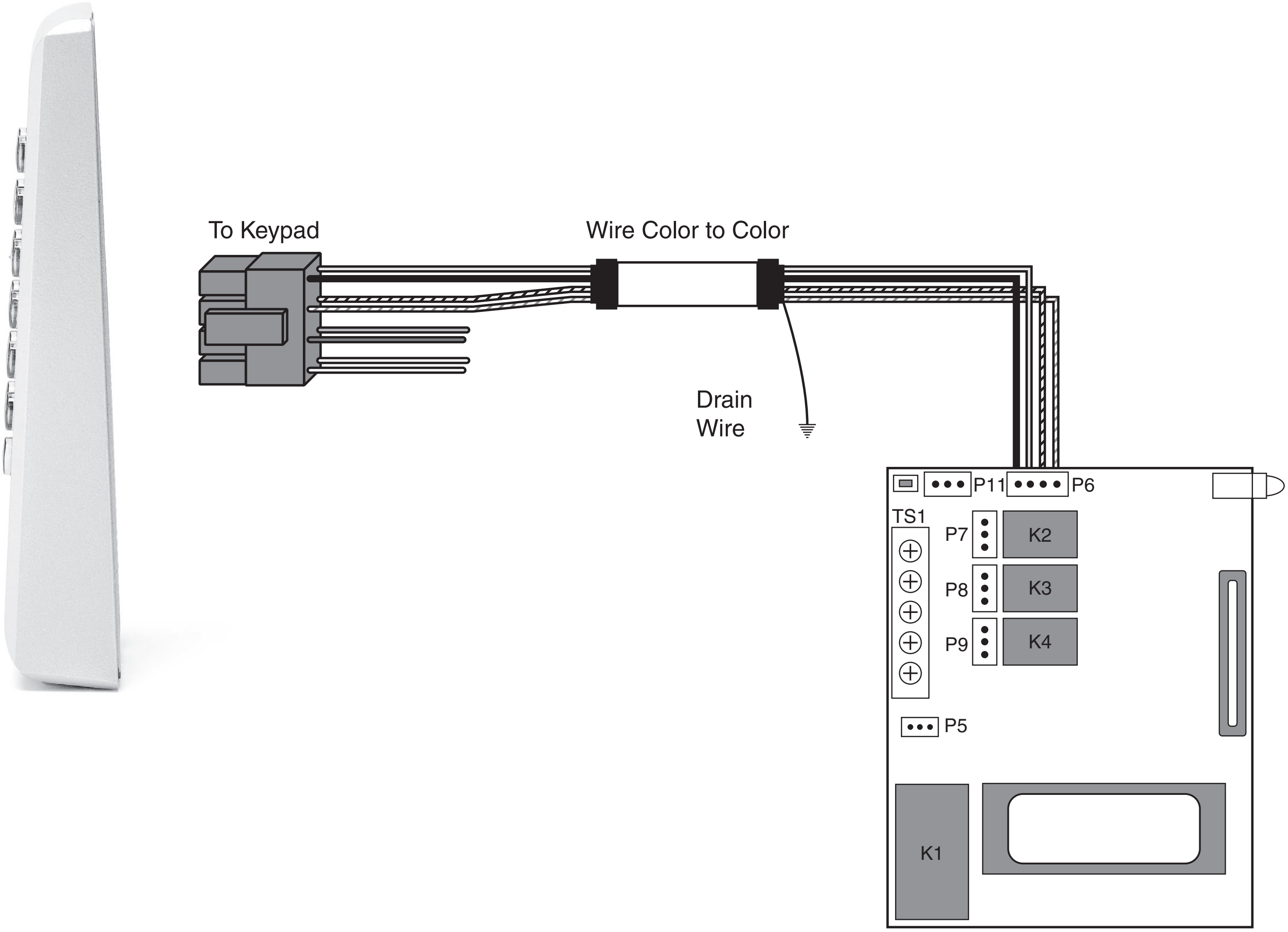
www.schlage.com

(877) 671-7011

Keypad Installation Procedure:

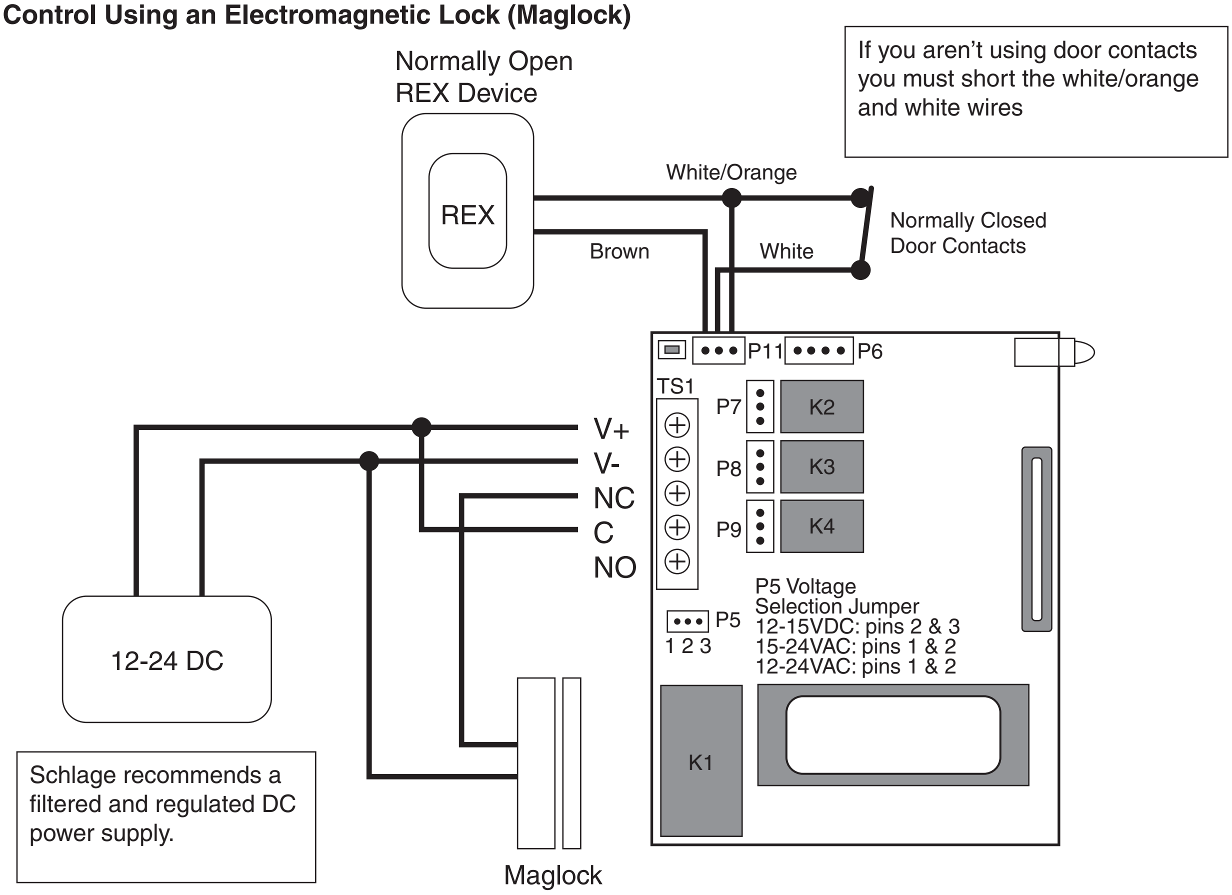
1. Drill through the back plate using a $\frac{11}{64}$” bit. Use the template on the back page to accurately mark the mounting holes before drilling. Then drill the mounting holes with a $\frac{9}{64}$” drill bit. Also drill the hole for the wires. This may vary depending on the number of conductors required.
2. On the keypad end, strip back the insulator from the wire and tape the drain wire (shield) to the jacket. Now connect the required wires to the 8-conductor wire harness provided. The wire harness plugs into the 8-position connector on the keypad. At the other end of your wire run, strip back the insulator from the wire but do not tape the drain wire to the jacket. The drain wire must be connected to ground at the controller end. See the diagrams below.
3. Finally mount the SSWiLM keypad onto the mounting surface using the provided screws. Do no over-tighten the screws, which may result in damage.

Wiring the SSWiLM to an Schlage 232 Access Control Module

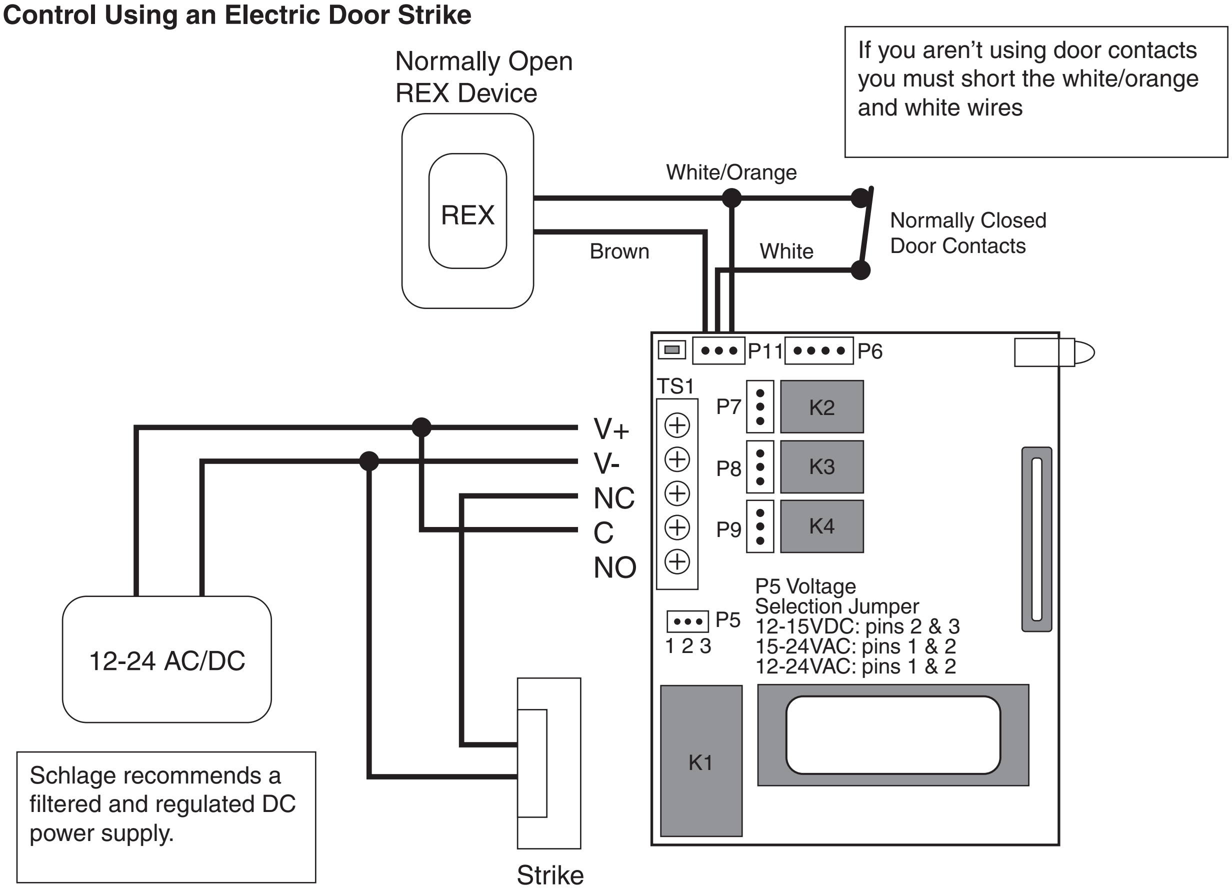


The connection between the SSWiLM and the 232 Controller requires a 4-conductor, stranded wire with overall foil shield. The 8-conductor wire harness from the keypad connects to connector P6 on the controller. Connect the wires, color to color (red to red, black to black, white/black to white/black and white/yellow to white/yellow). Refer to the wire lengths on the first page. As mentioned above, the drain wire must be attached to Ground on the controller side, which is the V- terminal or negative of your power supply.

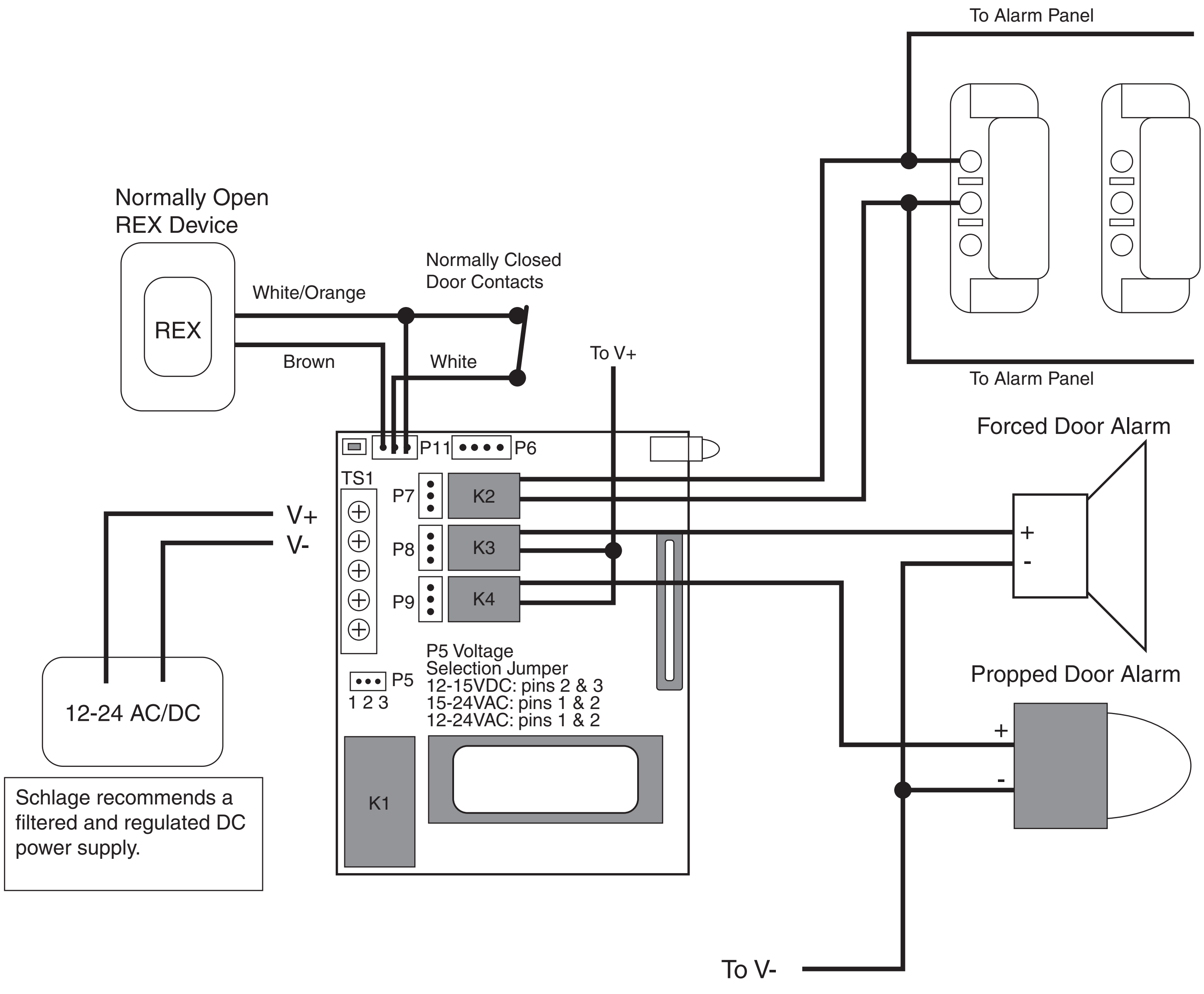
Basic Access Control Using an Electromagnetic Lock (Maglock)



Basic Access Control Using an Electric Door Strike



Integrated Access Control Wiring

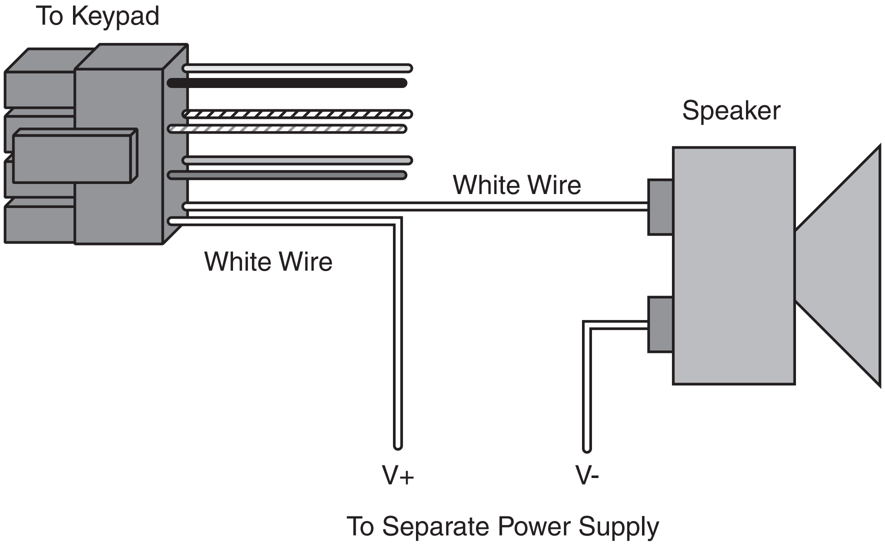


Schlage recommends a filtered and regulated DC power supply.

Wire Color	Relay Connection
Gray	Normally Closed
Blue	Common
Green	Normally Open

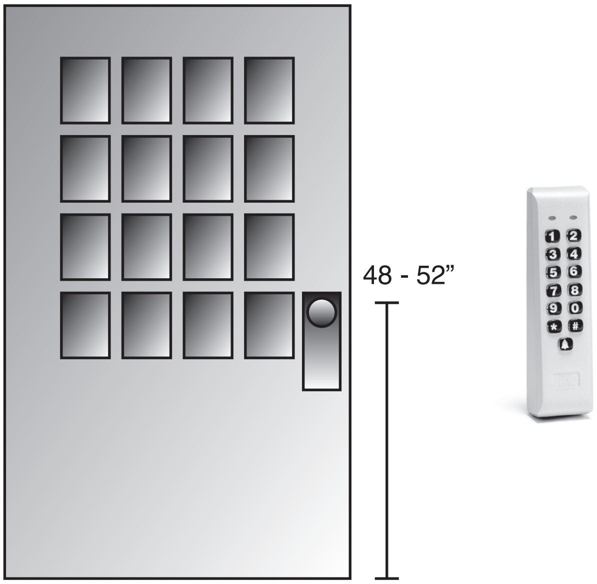
Wiring the Bell Output to a Speaker:

The SSWiLM keypad has a built in bell button, which triggers a relay output when pressed. This relay is normally open and the contact closes when triggered. You can use this relay output to trigger devices that require a momentary closure, such as a doorbell. The relay output provides a dry contact, but you can run up to 24 VDC or 125 VAC through it for devices that require power to operate. The diagram below shows these connections.



Keypad Mounting Height

Mounting height can vary depending on requirements. An appropriate range is typically between 48 and 52 inches on center off the floor.



Programming the SSWiLM Keypad

The SSWiLM keypad has it's own local programming options. All user codes and other access control features are programmed into the controller. Refer the Self-Contained Access Control Programming Guide for those features. The programming options chart below shows all the programming commands available in the SSWiLM.

To program the SSWiLM you first must enter program mode. To enter program mode enter the following on the keypad: **099 # program code ✱** (default program code is 6789).

Keypad Default Settings

Option	Default Setting	Option	Default Setting
Local Program Code	6789	Audio Keypress Feedback	Enabled
Visual Keypress Feedback	Enabled	Door Bell Select	Continuous
Keypad Illumination	Enabled	Keypad Dimming	Enabled

Programming Options Chart

Command/Action	Keys to Enter/Details	
Command 90 Change Local Program Code	**90 # 0 # 0 # new code ✱ new code ✱** (default = 6789)	
Command 91 Set/Clear Keypad Options (options below, **defaults in bold**)	**91 # option # set/clear # ✱✱**	
Option	**Clear**	**Set**
0 – Visual Keypress Feedback	0 = Disabled	**1 = Enabled**
1 – Audio Keypress Feedback	0 = Disabled	**1 = Enabled**
11 – Keypad Illumination	0 = Disabled	**1 = Enabled**
12 – Keypad Dimming	0 = Disabled (always bright)	**1 = Enabled**
13 – Door Bell Select	0 = Disabled	**1 = Enabled**
Command 92 Set Door Bell Duration	**92 # 4 # time # ✱✱**	Set timed output (1 – 99 seconds)
	92 # 4 # 0 # ✱✱	Set to continuous
Command 96 Reset Keypad to Default Settings	**96 # 0 # 0 # ✱✱**	
Exit Program Mode	**Press the ✱ Key**	

Testing the Keypad

After installing the keypad, Schlage recommends that you perform the keypad self-test once a year, to ensure that the keypad is working properly.

- To perform the self-test, with the unit powered up, press the following keys on the keypad: 7890#123456 ✱
- If all 12 key presses are accepted, the keypad enters self-test mode.
- The LEDs alternate three times followed by the sounder beeping three times.
- When finished the yellow LED starts flickering rapidly.
- Press ✱ to clear.

LED Indications

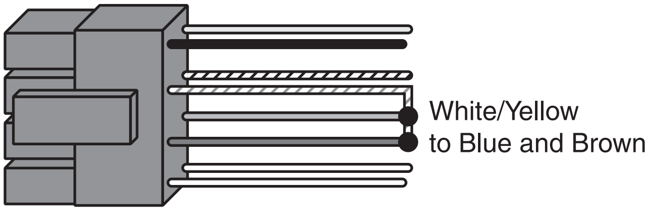
LED State	Description
Red Solid	Door Locked
Green Solid	Door Unlocked
Yellow Solid	Programming Error
Yellow Flashing Slowly (single flash)	Controller Program Mode
Yellow Flashing Slowly (double flash)	Front End Program Mode
Yellow Momentary Flash	Visual Keypress Feedback

Replacing the KP232m (discontinued) with an KP232

The KP232 is functionally equivalent to the KP232m keypad, which was discontinued. It's not, however, a direct physical replacement. They are both two piece units, but they use a different control boards. It is not possible to replace just the mullion keypad portion of the unit. You must replace the entire unit. Refer to the previous sections for wiring your new KP232 unit.

Program Mode Loopback

If you've forgotten the local program code use the following loopback connection to enter program mode. Power down the unit, short the wires in the configuration illustrated, then power the unit back up. The yellow LED should be flashing. Now change your local program code or reset the unit. Power the keypad down and reconnected the wire harness in the original configuration.



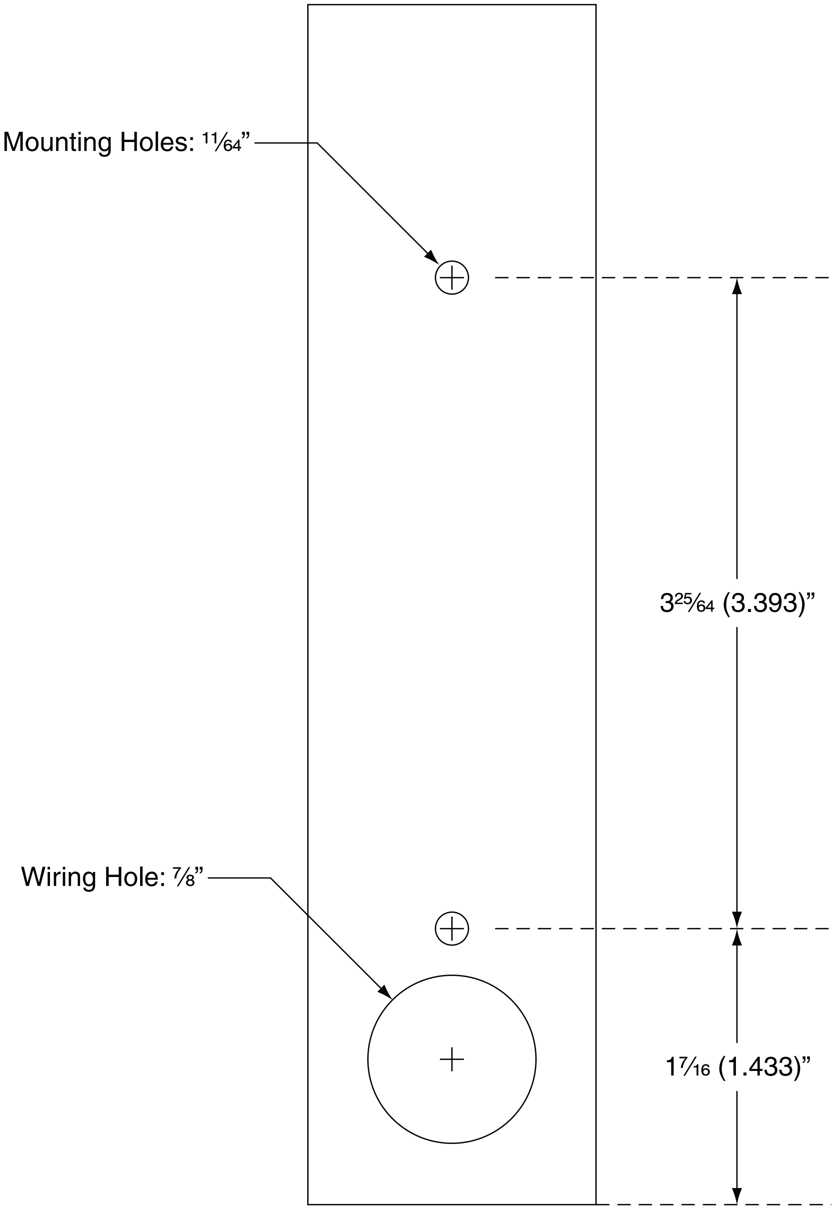
Warranty

Schlage Lock Company (Schlage) warrants its products to be free from defects in material and workmanship when they have been installed in accordance with the manufacturer's instructions and have not been modified or tampered with. Schlage does not assume any responsibility for damage or injury to person or property due to improper care, storage, handling, abuse, misuse, normal wear and tear, or an act of God.

Schlage's sole responsibility is limited to the repair (at Schlage's option) or the replacement of the defective product or part when sent to Schlage's facility (freight and insurance charges prepaid) after obtaining Schlage's Return Material Authorization. Schlage will not be liable to the purchaser or any one else for incidental or consequential damages arising from any defect in, or malfunction of, its products.

Except as stated above, Schlage makes no warranties, either expressed or implied, as to any matter whatsoever, including, and without limitation to, the condition of its products, their merchantability, or fitness for any particular purpose.

Keypad Mounting Template



The Schlage keypad is desingd for surface mount applications. You must drill a 7⁄8” hole for the wire harness connector, as shown, so the unit is flat against the mounting surface.

Ingersoll Rand
Security Technologies

Printed in U.S.A.

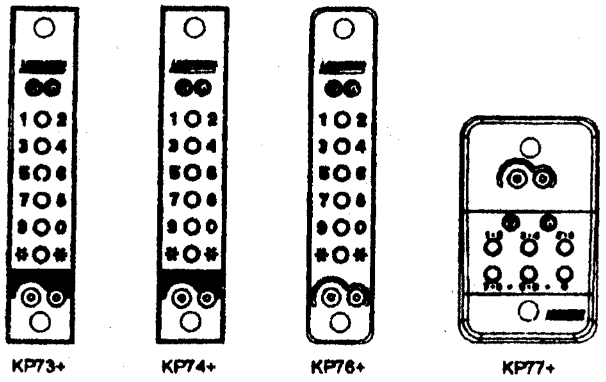
LOCKNETICS
Security Engineering

KEYPAD MOUNTING AND TEMPLATE INFORMATION

These mounting instruction are intended for use with all Locknetics keypad models.

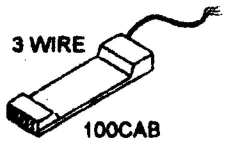
Model Description:

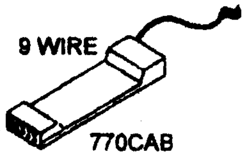
KP73+	6-3/4" x 1-3/8", available in special finishes
KP74+	6-3/4" x 1-3/8", Stainless finish
KP76+	7" x 1-3/8", Black Lexan
KP77+	4-1/2" x 2-3/4", Black Lexan *(single gang electrical box mount)*



Accessories:

100CAB	Connection cable, <u>three wire</u>, from one or two keypads to CT150SE controller.
770CAB	Connection cable, <u>nine wire</u>, from one or two keypads to CT150KP controller.
AUXCAB1	Auxiliary extension cable, one foot. Used for connecting keypad to adaptor cables, 770CAB or 100CAB.
AUXCAB16	Auxiliary extension cable, sixteen feet. Used for connecting keypad to adaptor cables, 770CAB or 100CAB.





Keypad Mounting:

<u>Step #1:</u> <u>Prep wall or frame as shown in ***Figure 1***.</u>

a) Drill two (2) mounting holes 6-1/8" from center to center to secure keypad as shown.

b) Drill one (1) wire access hole 1-1/8" DIA. for connection cable at 13/16" above center of lower mounting hole.

Note: *If mounting two keypads back to back, be sure hole locations are in alignment.*

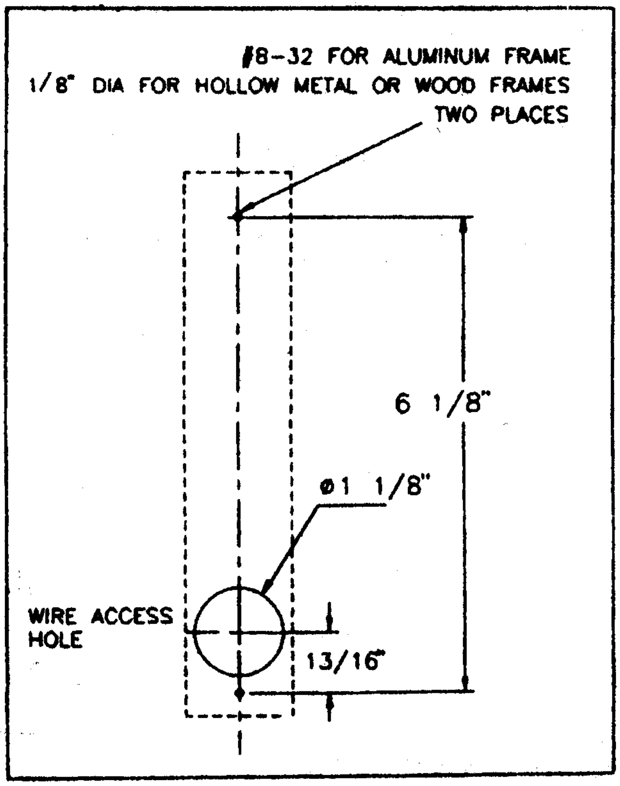


Figure 1 Mounting hole location.

Step #2: Connect keypad(s) to connection cable.

*For single keypad: **Figure 2.***

a) Pass module of connection cable through access hole.
b) Connect the keypads connector to module side of the connection cable.

*For two (2) keypads mounted back to back: **Figure 3.***

a) Pull connection cable through hole and connect first keypad to side **"A"** of the connection cable. Connecting the first keypad to side **"A"** of the connection cable allows access to cable for the second keypad.
b) Feed cable back though wire access hole and connect the second keypad to side **"B"** of the connection cable.

Notes: *1. If using the AUXCAB1 for connecting two (2) keypads on deep or non-standard frames, connect AUXCAB1 to the first keypad before connecting the connection cable.*

*For two (2) keypads, one local one remote: **Figure 4.***

a) Pull connection cable through hole and connect first keypad to one side of connection cable.
b) Connect one end of the AUXCAB16 to the remote keypad, connect the other end of the AUXCAB16 to the other side of the connection cable.

Step #3: Mount Keypad(s).

*For wall or frame mounting: **Figure 5.***

a) Secure the keypad to wall or frame using (2) #8-32 flat head screws.
b) Conceal screws with (2) anti-tamper plugs supplied.

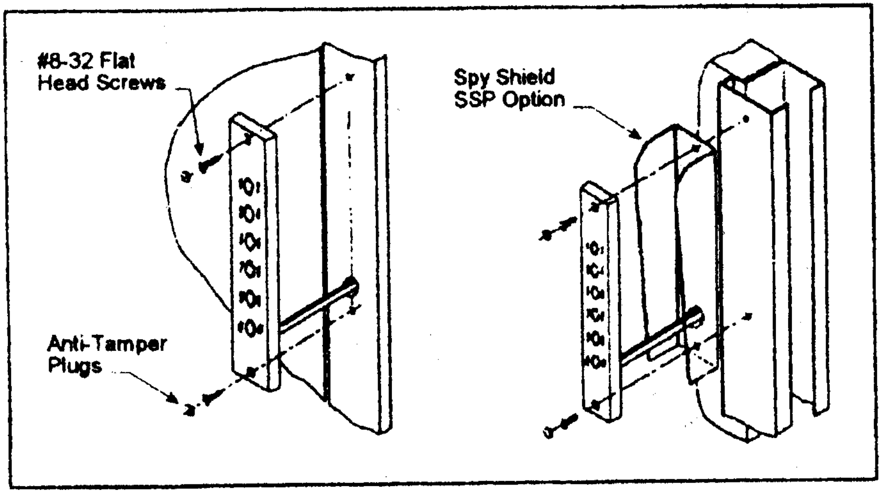


Figure 5 Mount keypad to wall or frame.

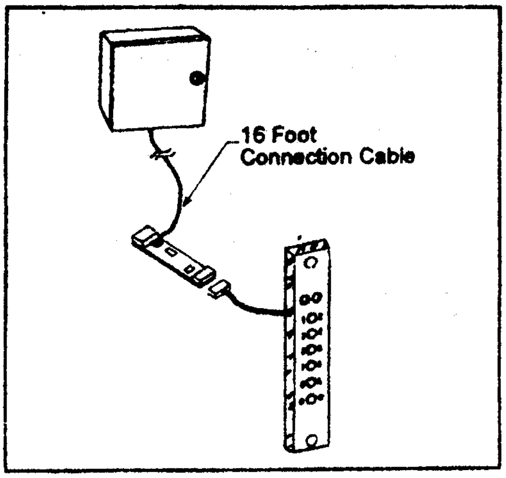


Figure 2 Connecting single keypad.

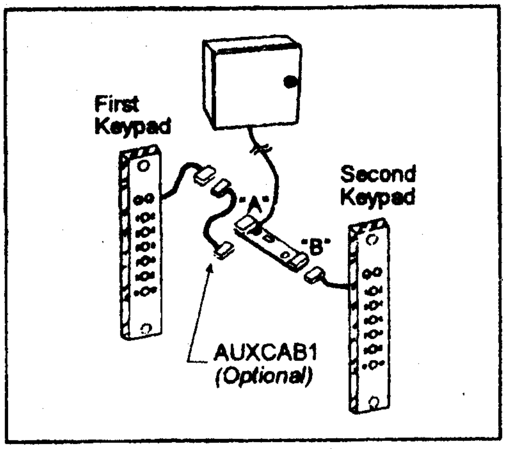


Figure 3 Connecting two local keypads.

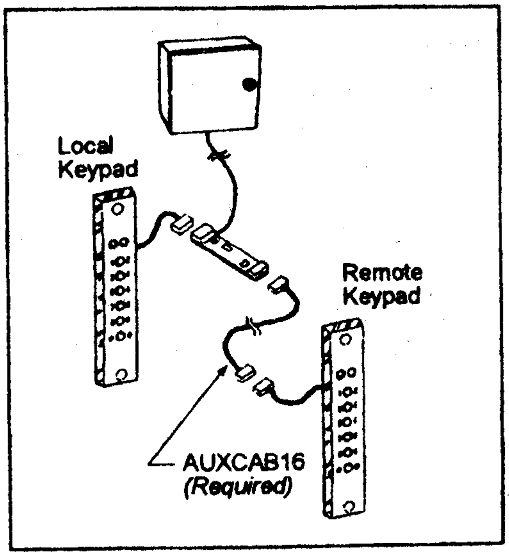


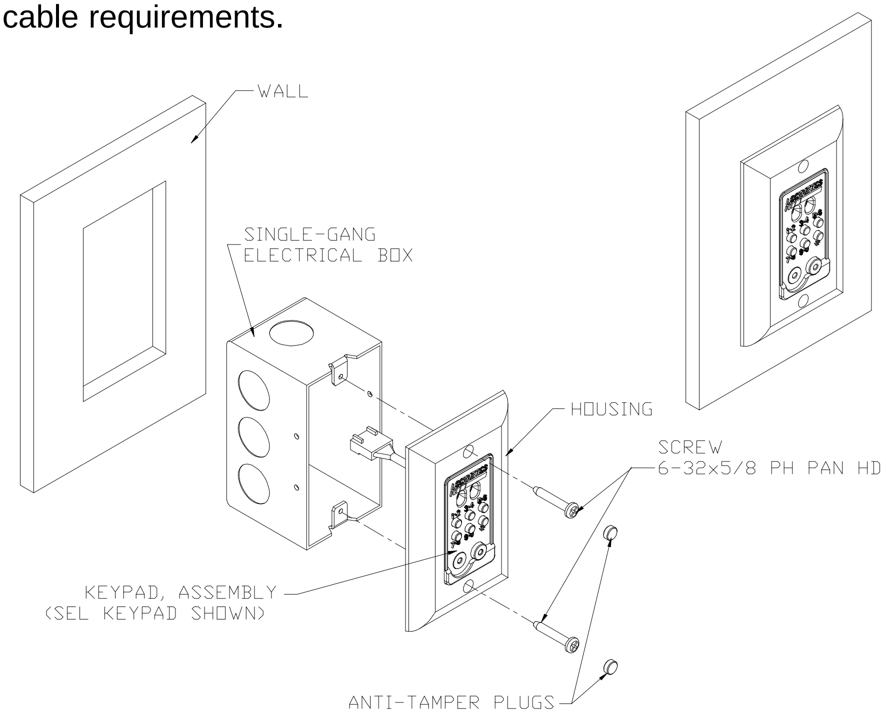
Figure 4 Connecting local and remote keypads.

575 Birch Street, Forestville, CT 06010
Phone (860) 584-9158   Fax (860) 584-2136
WWW. LOCKNETICS .COM

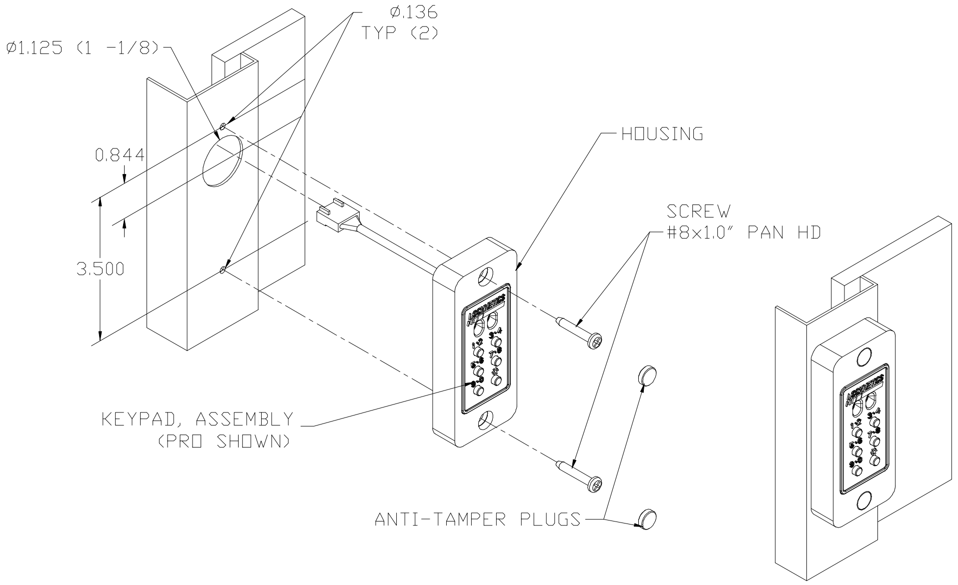
KP78+,KP79+,PRO78,PRO79,TR83,TR84
KEYPADS AND TOUCHENTRY^{TM} READERS
MOUNTING INSTRUCTIONS

Note: see controller/system manual with which keypad/touchentry key reader will be used for specific wiring and/or cable requirements.

KP79+
PRO79
TR84


WALL
SINGLE-GANG ELECTRICAL BOX
HOUSING
SCREW 6-32x5/8 PH PAN HD
KEYPAD, ASSEMBLY (SEL KEYPAD SHOWN)
ANTI-TAMPER PLUGS

KP78+
PRO78
TR83



PRO/PRO+ Series
Manual Programming Guide

For Programming User Codes into 20 Code Keypads/Trim (120 codes for PRO+)

LOCKNETICS
Security Engineering
575 Birch Street, Forestville, CT 06010
Phone (860) 584-9158 ▪ Fax (860) 584-2136
WWW.LOCKNETICS.COM

Code Functions / Factory Default Codes

Factory Code	*Function*	*Description*
13579	***Normal Use***	Normal Use codes will release a lock. While the lock is released the green LED will flash quickly. The lock remains released for a programmable amount of relock delay time.
135135	***Toggle***	Toggle codes will release a lock, the lock will remain released until any Toggle code is entered to reset the lock to a locked position.
9115 A Lockout code is also required to reset a lock that has been ignored beyond the initial low battery indication (see Low Batt. Indications)	***Lockout***	Lockout codes disable all codes from operating the lock until any Lockout code is entered to reset the lock to an accessible state. When a valid code is entered while a lock is in Lockout mode, the red LED will flash quickly twelve times (indicating that the code is valid but access is not permitted.) Think of the Lockout function as a “freeze” function, it will freeze the lock in its current state (locked or unlocked) not allowing any codes to operate the lock, until a Lockout code is entered to return the lock to an accessible state.
none	***One Time Use***	One Time Use codes will only release the lock one time.
none	***Supervised Access***	Supervised Access codes require two users to be present to release the lock, two Supervised Access codes must be entered within approximately five seconds to release the lock.
97531 **For security reasons the factory default Master Programming Code should be changed (refer to programming procedures for instructions).**	***Master Prog.***	A Master Programming Code allows access to programming functions. **The Master Programming Code will not release a lock**, it just initiates programming. When a Master Programming Code plus ✻ is entered, the LEDs alternately flash several times indicating the lock is in programming mode. If more than 30 seconds pass between programming entries, the lock returns to the normal operational state. **To automatically delete all default factory codes, change the default Master Programming Code.**

User Codes

When entering codes, if a wrong button is pressed, press ✻ to clear the keypad then reenter the entire code. The keypad will clear itself if no button is pressed within approximately five seconds.

If any keypad buttons are pressed forty times in succession, without a successful code being entered, the keypad will shutdown for approximately thirty seconds.

User codes must be 3-7 digits in length for Pro Series locks. Security increases as the number of digits in a user code increases. The chart below provides the total number of possible combinations, based upon the length of the user code.

User Code Length	*Possible Combinations*
3	125
4	625
5	3125
6	15625
7	78125

Keep in mind that the keypads contain 5 buttons, and each button represents two numbers, so the code 2468 is identical to code 1357 (as far as the lock is concerned). If you plan to administer and track codes manually, **issue codes exclusively with all odd or all even numbers**, this practice will make it easier to spot duplicate codes (the final page of this document provides space for you to record issued codes). An error code will occur during programming if a duplicate code is attempted.

Codes of varying length can be used in the same lock but this will effect the total number of possible combinations. For example, if you choose five digit User Codes to be the standard, and then add a three digit User Code such as 246, no other five digit code beginning with 246 can be used.

Programming User Codes

Using the keypad, follow the procedure tables below to program user codes

- After each step of a procedure, **the red and green LEDs will alternately flash several times**, indicating the step was performed successfully. WAIT for flashing to stop before continuing.
- **If at any time the red LED remains on while the green LED flashes, an error has occurred**. Refer to bottom of page for Error Code Descriptions.
- Entered codes must be 3-7 digits in length.

Add Normal Use Code ⇩	*Add Toggle Code* ⇩	*Add Lockout Code* ⇩	*Add One Time Use Code* ⇩	*Add Supervised Access* ⇩
MasterCode ✻	MasterCode ✻	MasterCode ✻	MasterCode ✻	MasterCode ✻
3 ✻	**3 3 ✻**	**3 3 ✻**	**3 3 ✻**	**3 3 ✻**
	1 9 1 ✻	**1 1 5 ✻**	**1 1 3 ✻**	**1 1 7 ✻**
▶ NewCode ✻	▶ NewCode ✻	▶ NewCode ✻	▶ NewCode ✻	▶ NewCode ✻
to add more	*to add more*	*to add more*	*to add more*	*to add more*
✻ to complete	✻ to complete	✻ to complete	✻ to complete	✻ to complete

Change a Code ⇩	*Delete a Code* ⇩	*Change Master Code* (5 digit min)⇩	*Change Relock Time* ⇩
MasterCode ✻	MasterCode ✻	MasterCode ✻	MasterCode ✻
1 ✻	**5 ✻**	**7 ✻**	**9 9 ✻**
OldCode ✻	▶ OldCode ✻	NewMaster ✻	Press and hold ✻ for the desired time (red LED blinks)
NewCode ✻	*delete more*	NewMaster ✻	
Automatically completed	✻ to complete	Automatically completed	Release ✻ to complete

Error Code Descriptions

If an error occurs during programming, the red LED remains lit while the green LED flashes an error code. **A flashing error code is repeated three times (with a pause in between each set of flashes).** Count the number of flashes to determine the error code, then consult the chart below.

Green Flashes	*Error Description*
2	Code entered is too long, 7 digits maximum
3	Memory full, more than 20 codes have been entered
4	Master Prog Code must be changed with *Change Master Code* procedure
5	The second entry for verification of a new Master Prog Code did not match the first
6	Invalid command, press ✻ and start over (previous programming, up to this error, may still be valid)
7	Code to be deleted does not exist
8	Code entered is too short (3 digits min. for User Code, a Master Prog Code must have at least 5 digits)
9	Duplication, the code entered already exists

Clearing / Resetting Memory

Clearing the memory of a lock **deletes all** programmed codes that were in the lock, and **restores** the four default factory codes: Master Prog., Normal, Toggle, and Lockout.

To clear memory and return to the default Factory Codes	A. Disconnect batteries or power. B. Push and hold any button on the keypad for about two seconds. C. Wait approximately 5 seconds. D. Reconnect the batteries/power and immediately proceed to the next step. *The green and red LEDs will alternately flash several times.* E. Immediately **after the LEDs stop flashing**, push the * button **three** times. *The green and red LEDs will alternately flash several times again, indicating the memory has been cleared – if not return to step A.* *Note: If more than 3 seconds pass before the * button is pressed, the green LED will blink only once, this indicates the memory was not cleared – return to step A.* **To Clear memory on older PRO Series battery operated models with an external electronics board containing a CLR(MEM) microswitch, perform the following:** 1. Remove the battery/electronics cover from the secure side of the door. 2. Press and release the microswitch pushbutton labeled **CLR**(MEM), **three** times. *The red LED will light for several seconds then go out.* 3. Replace the battery/electronics cover.

Low Battery Indications

Battery powered products have built-in low battery indications. A lock with low batteries will act differently, allowing the appropriate support personnel to be notified of the locks differing behavior. Changing batteries does not effect any programmed data.

Low Battery Indications Changing batteries does not effect programmed user codes.	There are two phases of low battery indications: **A.** When a valid code is entered on a lock with weak batteries (~75% of full power), the red LED will flash twelve times before the green LED flashes and the lock is released. This is an indication to **replace the batteries** at this time. The lock will operate in this manner for about 500 cycles. **B.** After 500 cycles of the lock operating as described in Step A, when a valid code is entered, the red LED will flash twelve times and the lock will not release – the lock automatically goes into a **Lockout** mode. A Lockout code must be entered to return the lock to an accessible state and then a Normal Use code must be entered to gain access. The lock will operate in this dual credential manner for about 200 cycles until the batteries fail completely. A mechanical override key can always gain access (if the lock is so equipped).

User Code Records

Master Code________________

User Code	Function	User Name / Notes

User Code Records

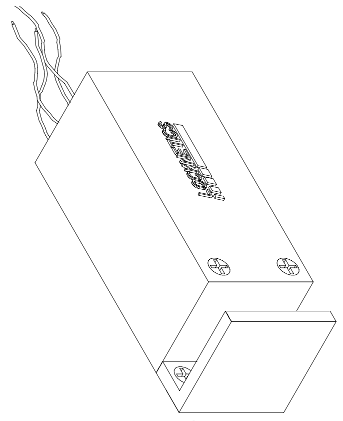
Master Code________________

User Code	Function	User Name / Notes

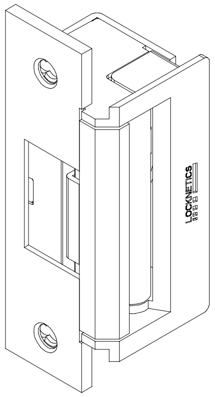
575 Birch Street, Forestville, CT 06010
Phone (860) 584-9158   Fax (860) 584-2136
www.locknetics.com

Pro Access System

BATTERY POWERED LOCK WITH ACCESS CONTROL
INSTALLATION AND WIRING INSTRUCTIONS

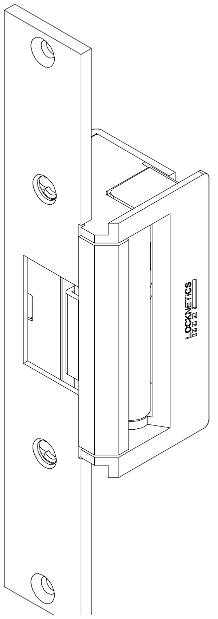


Pro 443 Series Cabinet Lock

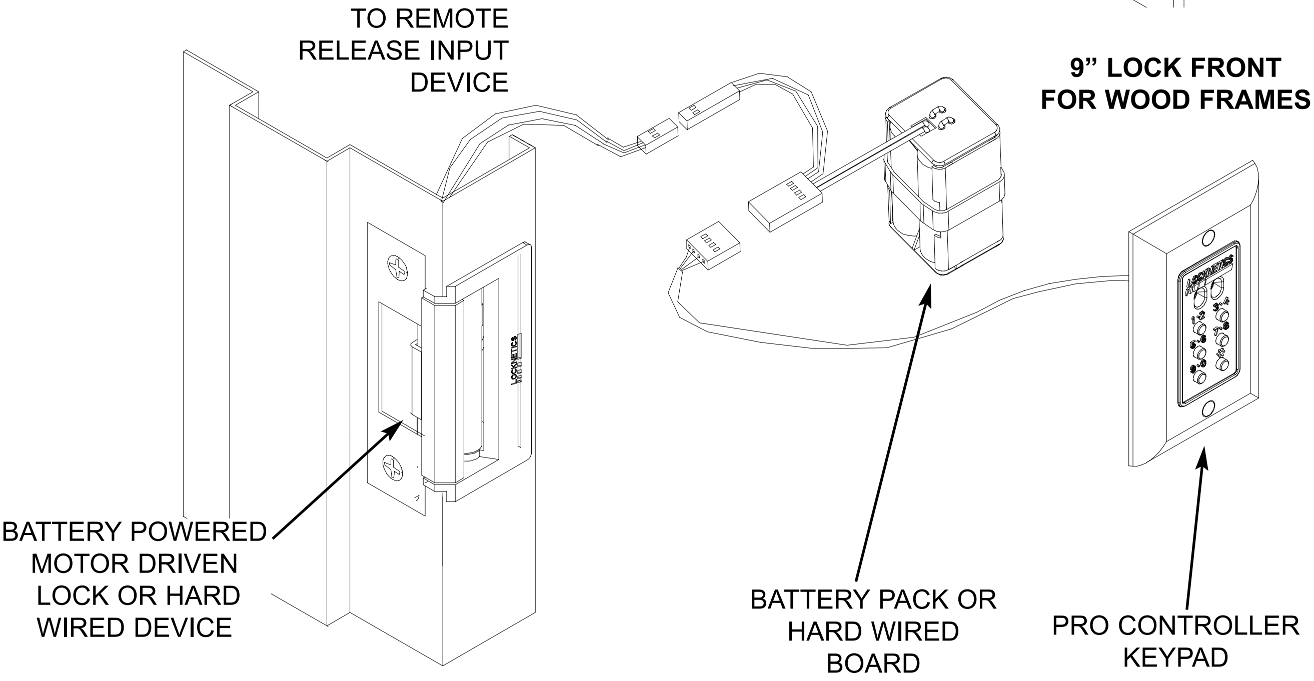


STANDARD

Pro 9100 Series Power Strike



9" LOCK FRONT FOR WOOD FRAMES


TO REMOTE RELEASE INPUT DEVICE
BATTERY POWERED MOTOR DRIVEN LOCK OR HARD WIRED DEVICE
BATTERY PACK OR HARD WIRED BOARD
PRO CONTROLLER KEYPAD

Description of Operation

The Pro Controller provides a simple solution to access control needs. Providing 20 user code capability through manual programming, this is a new and simple product to install and program. The Pro is available in hard wired or battery powered versions. The battery powered device may be used with any Locknetics motor driven locking device, such as the 9100BP or the 443 Cabinet Lock. The hard wired unit will work with any 12 or 24 VDC locking device, such as a magnetic lock or electric strike, not requiring any more current than 5 amps. Access control is now as easy as **1**) install locking device, **2**) install keypad, **3**) plug and play!

1. INSTALL MOTOR DRIVEN LOCKING DEVICE

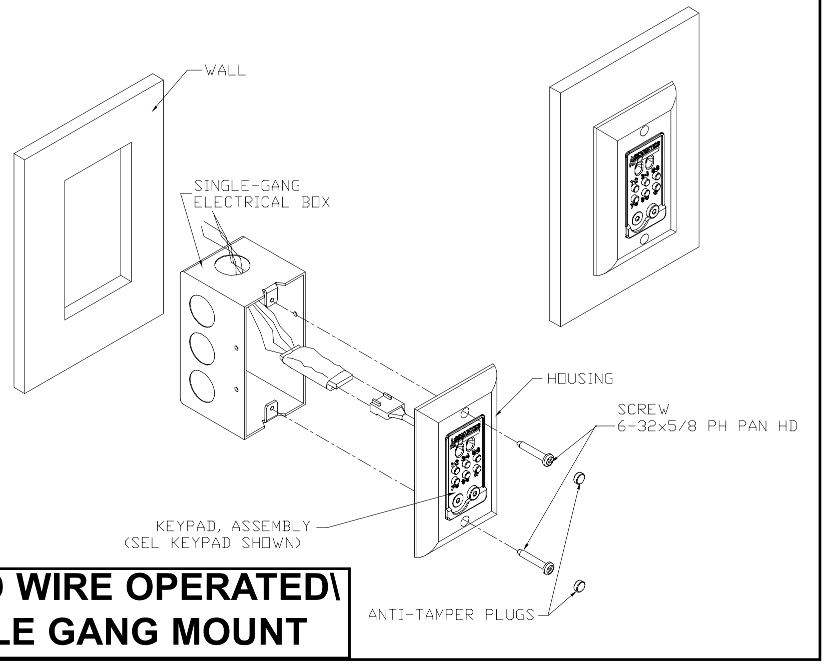
Follow the template and installation instructions provided with the locking device.

2. INSTALL SINGLE GANG BOX

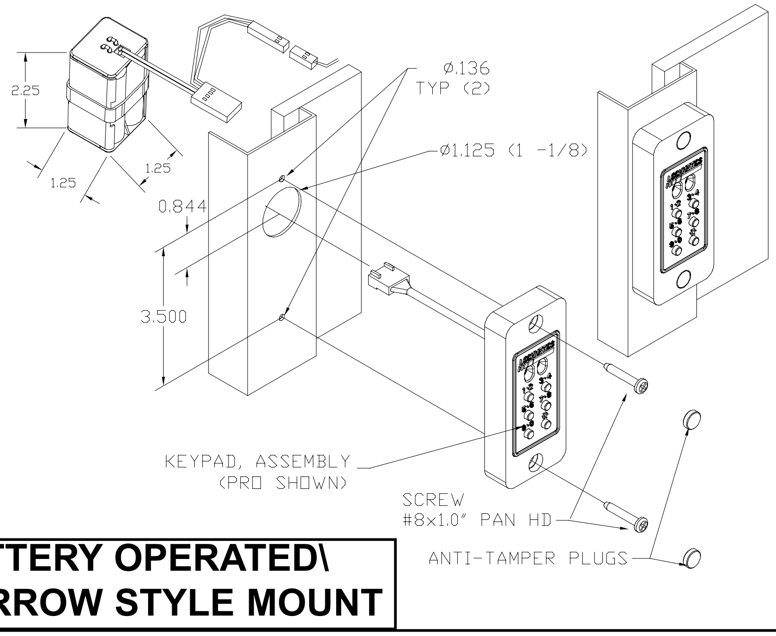
Install single gang box in wall. Run wiring from locking device to gang box. Secure battery pack inside the gang box.

3. INSTALL KEYPAD

Attach all wire connections as shown. Mount keypad to gang box.


WALL
SINGLE-GANG ELECTRICAL BOX
HOUSING
SCREW 6-32x5/8 PH PAN HD
KEYPAD, ASSEMBLY (SEL KEYPAD SHOWN)
ANTI-TAMPER PLUGS

HARD WIRE OPERATED\ SINGLE GANG MOUNT



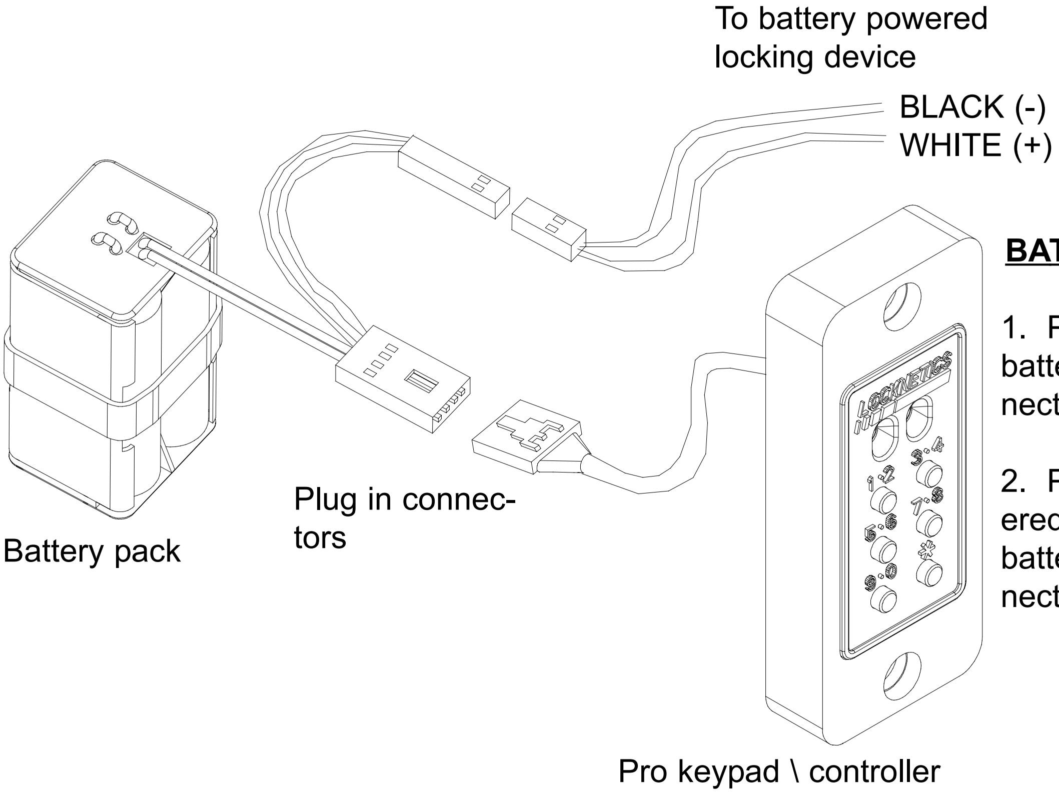
BATTERY OPERATED\ NARROW STYLE MOUNT

HELPFUL HINTS

Battery pack must be accessible after installation for battery replacement.

Both the single gang and narrow style pro keypads are capable of battery or hard wired operation.

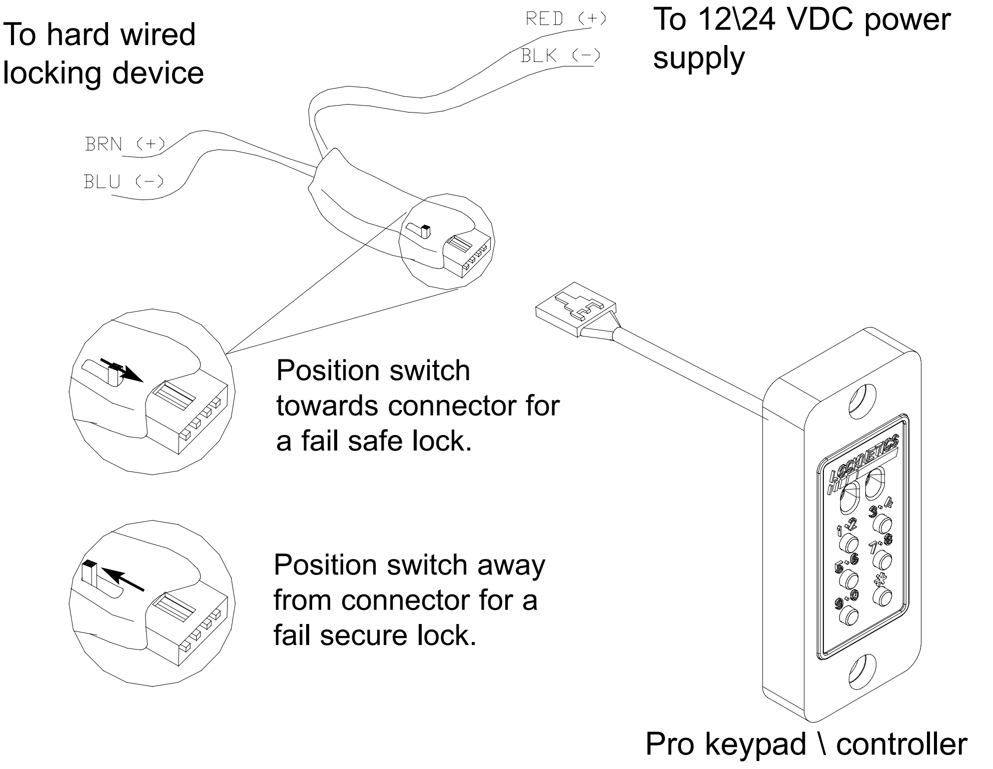
When the battery pack is being used in the installation, a gang box or similar device must be used to support the battery pack.



BATTERY OPERATED

1. Plug keypad into battery pack 4 pin connector.

2. Plug battery powered locking device into battery pack 2 pin connector.


To hard wired locking device
RED (+)
BLK (-)
To 12\24 VDC power supply
BRN (+)
BLU (-)
Position switch towards connector for a fail safe lock.
Position switch away from connector for a fail secure lock.
Pro keypad \ controller

HARD WIRED

1. Plug keypad into circuit board.

2. Apply 12 or 24 VDC to red and black wires. Be sure to observe polarity.

3. Connect blue and brown wires to locking device power. Again be sure to observe polarity.

4. Position switch as shown for fail safe or fail secure locking devices.

NOTES FOR BATTERY AND HARD WIRED SYSTEMS

1. The maximum current that can be put through the hard wired Pro Controller is 5 amps.
2. Battery life of the battery operated Pro Controller is 80,000 cycles.

DEFINITION OF CODE FUNCTIONS AND FACTORY DEFAULTS

	FACTORY DEFAULT	
MASTER	97531	Allows access to programming functions. Will not release lock.
NORMAL ACCESS	13579	Unlocks lock for relock time delay.
TOGGLE	135135	Unlocks the lock until same or another Toggle Code is entered.
LOCKOUT	9115	“Freezes” the lock in its present condition, either locked or unlocked, and will not accept any user codes until the same or another Lockout Code is entered.

ERASE MEMORY

Memory may be erased to conveniently return to default time delay settings or if an error was made.

1. Disconnect power.
2. Press any button one time.
3. Reapply power. Red and green LEDs flash alternately.
4. Press * key 3 times quickly immediately after LEDs stop flashing. Red and green LEDs flash alternately.

NOTES:

All programmed codes will be erased. Factory default codes and time settings will be restored.

PROGRAMMING INSTRUCTIONS

TO CHANGE MASTER CODE

Master Code *...7 *...New Master Code (5-8 digits)*...New Master Code *

TO ADD NORMAL ACCESS CODES - Will unlock door for relock time delay period. Will also reset lock after an alarm condition.

Master Code *...3 *...New Code (3-5 digits) *...* (to end)

UP TO 20 NEW CODES CAN BE
ADDED BY RETURNING HERE.

TO CHANGE CODES

Master Code *...1 *...Old Code*...New Code (3-8 digits) *...* (to end)

MORE CODES CAN BE CHANGED BY
RETURNING HERE.

TO DELETE CODES

Master Code *...5 *...Old Code *...* (to end)

MORE CODES CAN BE DELETED
BY RETURNING HERE.

TO ADD FUNCTION CODES (Note that a three digit function code sets the function of the user code)

MORE CODES CAN BE ADDED BY RETURNING HERE.

Master Code *...33*...111*...New *Access* Code (3-7 digits) * ...* (to end)

OR

191*...New *Toggle* Code

OR

115*...New *Lockout* Code

OR

113*...New *One-Time Access* Code

DOUBLE USE CODES (The two codes programmed must both be entered before access will be granted)

Master Code *...33*...117*...First user code (3-7 digits) * Second user code (3-7 digits)..*

RELOCK DELAY

1. Enter master code.
2. Enter 9 9 *.
3. Press * key for the desired relock time. The red LED will blink once for each second.

Battery Operating Information

Low Battery Indication:

When a valid code or is entered the green LED will flash during the unlock time. If the batteries are weak, the red LED will flash for several seconds before the green LED flashes. This is the indication to change the batteries.

Checking the Batteries:

Set the voltmeter for DC voltage at a scale above 6 volts. Place the meter probes onto the two outer connectors of the four pin battery harness.

Voltmeter Reading	**Battery Condition**
6.2 Volts	Fresh Batteries -Full Strength
4.5 Volts or Less	Replace Batteries

Replacing the Batteries:

1. Remove the four dead batteries and replace with four new batteries.

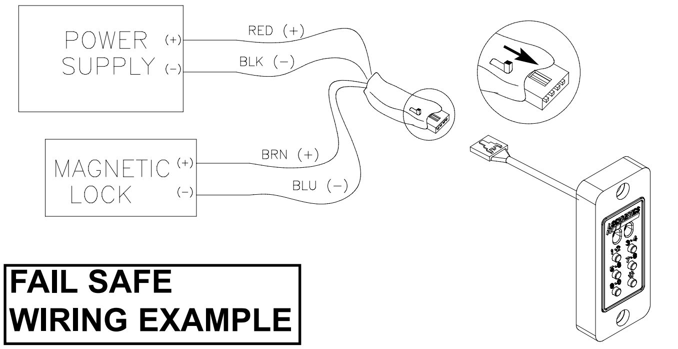
NOTES:

- **Always replace batteries as a set.**
- **Use only quality alkaline batteries.**

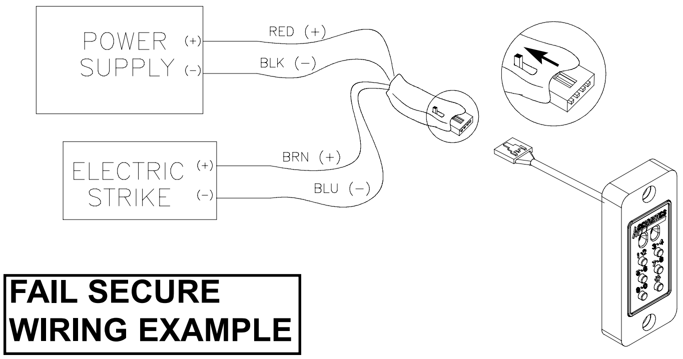
ERROR CODE CHART

An error has occurred when the red LED stays on solid and the green led flashes N times. Count the green flashes and refer to the chart below.

N	ERROR DESCRIPTION
2	CODE TOO LONG
3	MEMORY FULL
4	CAN'T DELETE MASTER CODE
5	2nd MASTER ENTRY NOT SAME AS 1st
6	INVALID COMMAND
7	NOT USED
8	CODE TOO SHORT
9	DUPLICATE CODE
12	LOCKOUT



FAIL SAFE WIRING EXAMPLE



FAIL SECURE WIRING EXAMPLE

LOCKNETICS
Security Engineering

575 Birch Street, Forestville, CT 06010
Phone (860) 584-9158 Fax (860) 584-2136
www.locknetics.com

PRO+ INSTALLATION INSTRUCTIONS

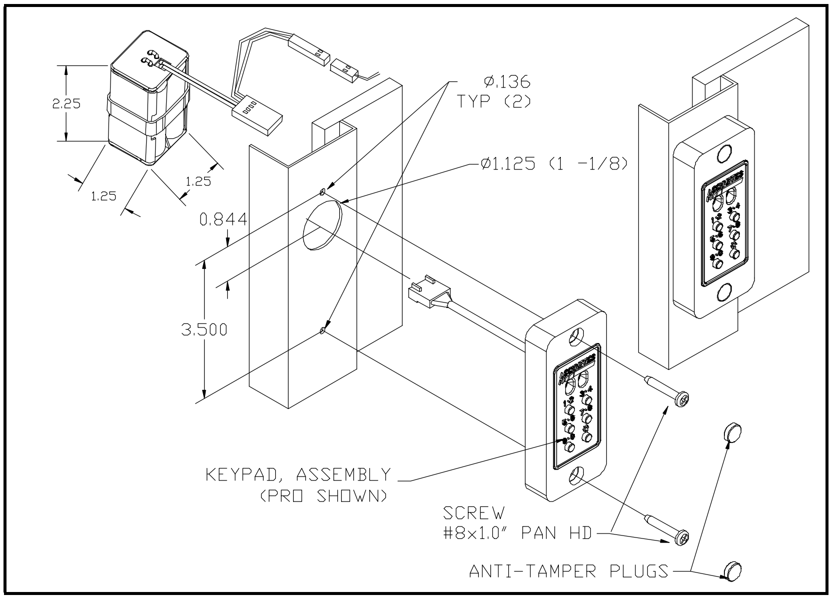
PRO+ SYSTEM:

The PRO78+ and PRO79+ access control systems are easy to install easy to configure systems which can be used in conjunction with virtually any locking device on the market. Magnetic locks, electric strikes, solenoid-driven deadbolts, automatic operators, and even electric latch retraction devices can be controlled by the PRO+ system. The hard wired units provide the ability to operate up to 5 amps at 12/24 volts. They can also be used to interface to equipment requiring a dry contact input. A request to exit input can be used to release the locking device with a momentary button or exit device switch, etc. When used with a door contact, the lock will cancel the remaining time delay once the door is opened for “anti-tailgate” function.

The PRO78+BP and PRO79+BP systems are designed to operate Locknetics motor-driven electric strikes and cabinet locks, providing a very easy to install system with no hard wiring to AC power. They are convenient for remote locations or mobile applications where hard wiring is difficult. The battery powered unit does not provide for remote release or “anti-tailgate” features.

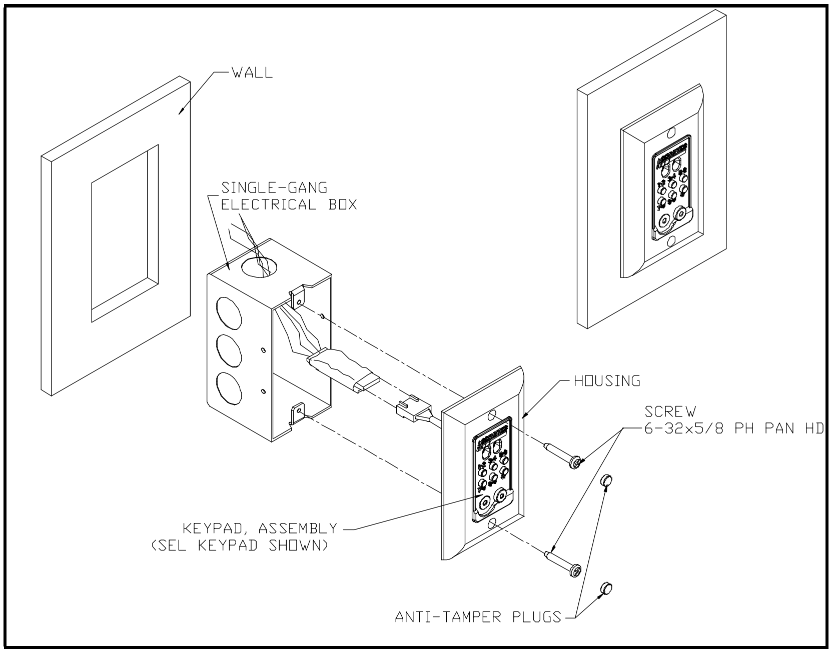
MULLION/FRAME INSTALLATION:

The PRO78+ unit is intended to be mounted on a door frame or where a single gang box is not to be used. The drawing to the right shows a PRO78+BP unit. The mechanical installation for the hard wired PRO78+ is the same. Note that when installing a battery powered unit, the batteries must be accessible for replacement.



SINGLE GANG BOX INSTALLATION:

The PRO79+ unit is intended to be mounted in a single gang box. The drawing to the right shows a PRO79+ hardwired unit. The mechanical installation for the battery powered PRO79+BP is the same. Note that when installing a battery powered unit, the batteries must be accessible for replacement. (If the anti-tamper plugs will be used, the batteries should be installed on the opposite side in their own box so they can be accessed without drilling out the plugs.)



HARD WIRED PRO78+/PRO79+:

1. **PULL WIRES**
See example wiring diagrams in this manual, and information included with the locking device, door contact (if used), and request to exit device (if used), to determine the type of system being installed. Determine the number of wires needed to be pulled to each device and the correct routing for the wires. Pull wires appropriate for the voltage and current required by the devices in accordance with local building codes.

2. **INSTALL SYSTEM COMPONENTS**
Install power supply, locking device, and PRO+ controller (as shown on page1). Install exit device (if used), door contact (if used) and request to exit device (if used). NOTE: do not install anti-tamper plugs at this time.

3. **CONFIGURE SYSTEM**
After all wires are connected and checked power up the system. A fail safe the lock should be locked at this time. If the lock is fail secure, it should be unlocked. (The factory default condition of the relay is normally closed (N.C.)) If this is not the case, check wiring. If wiring is OK continue.

There are two configuration steps which must be done at this time:

A. CONFIGURE RELAY OUTPUT:
The relay in the system has only two wires. They can be configured to operate normally open (N.C.) or normally closed (N.C.) If the system is powered up and the locking device requires you to change from N.O. to N.C. or back again, follow this procedure:

On the keypad, enter the following sequence. **(The factory default master programming code is 97531.)** Note that whenever the asterisk (*) is entered, the LEDs will flash. Wait until they stop flashing before entering the next number.

TO CHANGE RELAY OUTPUT STATE: <MASTER CODE> * ... 33* ... 175* <END>

The output wires should change state. This can be observed with a meter. The lock should now be locked. To verify proper operation test the system by entering a valid code. **(The factory default access code is 13579.)** The lock should unlock for the factory default time delay of 8 seconds. Then it should relock.

B. CONFIGURE REQUEST TO EXIT DEVICE FUNCTION (IF USED):
There are two types of functions which can be configured for the request to exit device. If one is not used, disregard this step and insulate the request to exit wire (brown) and the ground wire (white/orange) if it is not used for the door contact.

MOMENTARY UNLOCK MODE: When a momentary contact closure occurs between the white and white/orange wires the lock will unlock for the relock time delay (8 seconds, default).

TOGGLE UNLOCK MODE: When a momentary contact closure occurs between the white and white/orange wires the lock will unlock and remain unlocked until the momentary contact closure occurs again. This allows for a Lock/Unlock input from a control console, etc.

The unit is shipped from the factory in the “momentary unlock mode”. If it is necessary to change the state of the function follow this sequence. **(The factory default master programming code is 97531.)** Note that whenever the asterisk (*) is entered, the LEDs will flash. Wait until they stop flashing before entering the next number.

TO CHANGE REQUEST TO EXIT FUNCTION: <MASTER CODE> * ... 33* ... 173* <END>

TEST: activate the request to exit device, momentarily. The lock should operate according to the mode you set it for. If not, change the function by following the steps above.

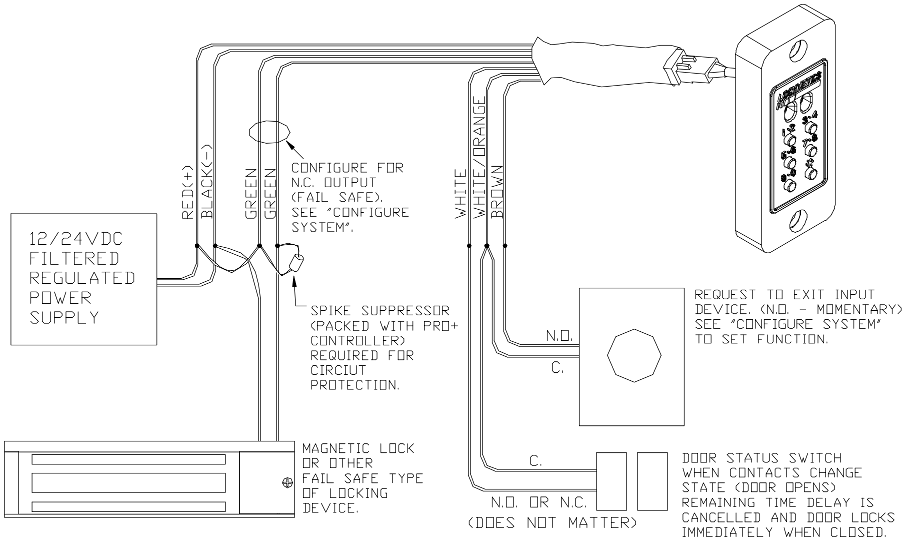
NOTES:
1. DOOR STATUS SWITCH CAN BE WIRED EITHER N.O. OR N.C.. THE CONTROLLER IS ONLY LOOKING TO SEE A CHANGE OF STATE.
2. REQUEST TO EXIT DEVICE MUST BE N.O.. LOCK WILL REMAIN UNLOCKED AS LONG AS REQUEST TO EXIT DEVICE IS ACTIVATED.

4. **PROGRAM LOCK**
Refer to the programming guide included with the unit for complete programming instructions (Form 58000).

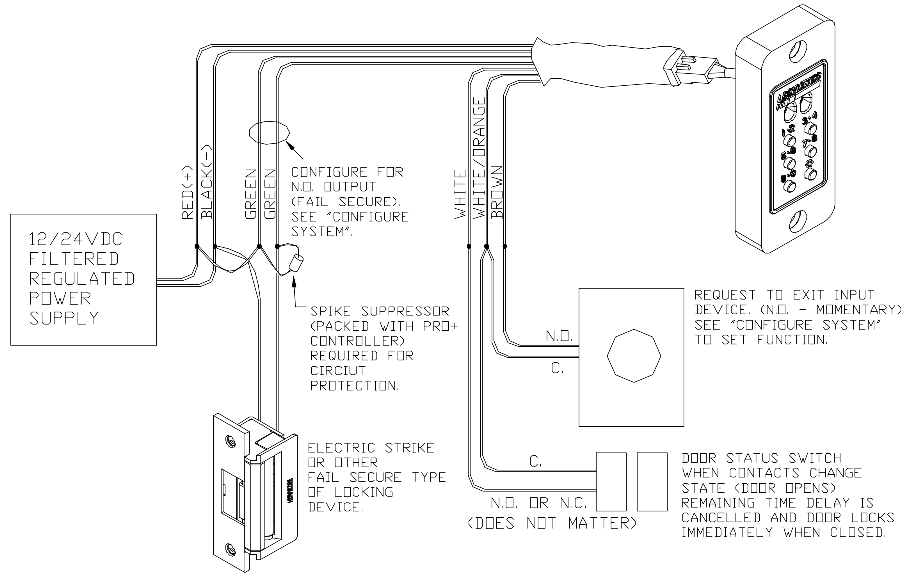
FAIL SAFE LOCKS

IMPORTANT NOTE:

WHEN INTERFACING SYSTEM TO SUPERVISED FIRE ALARM SYSTEM FOR EMERGENCY EGRESS APPLICATIONS IT IS NECESSARY TO CUT POWER TO THE LOCK ITSELF, NOT TO THE PRO+ CONTROLLER (UNLESS THEY SHARE THE SAME SUPPLY).

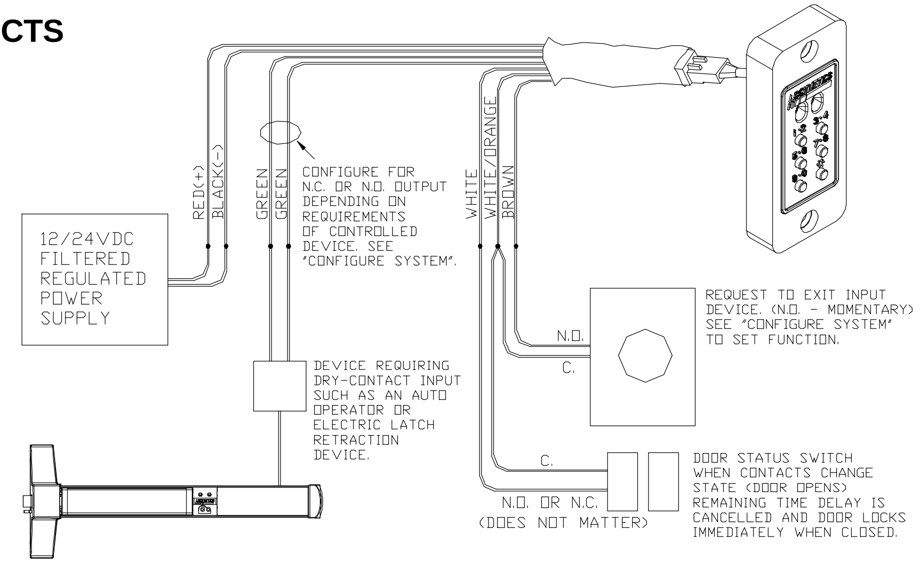

RED(+)
BLACK(-)
GREEN
GREEN
CONFIGURE FOR N.C. OUTPUT (FAIL SAFE). SEE "CONFIGURE SYSTEM".
WHITE
WHITE/ORANGE
BROWN
12/24VDC FILTERED REGULATED POWER SUPPLY
SPIKE SUPPRESSOR (PACKED WITH PRO+ CONTROLLER) REQUIRED FOR CIRCUIT PROTECTION.
REQUEST TO EXIT INPUT DEVICE. (N.O. - MOMENTARY) SEE "CONFIGURE SYSTEM" TO SET FUNCTION.
N.O.
C.
MAGNETIC LOCK OR OTHER FAIL SAFE TYPE OF LOCKING DEVICE.
C.
N.O. OR N.C.
(DOES NOT MATTER)
DOOR STATUS SWITCH WHEN CONTACTS CHANGE STATE (DOOR OPENS) REMAINING TIME DELAY IS CANCELLED AND DOOR LOCKS IMMEDIATELY WHEN CLOSED.

FAIL SECURE LOCKS


RED(+)
BLACK(-)
GREEN
GREEN
CONFIGURE FOR N.O. OUTPUT (FAIL SECURE). SEE "CONFIGURE SYSTEM".
WHITE
WHITE/ORANGE
BROWN
12/24VDC FILTERED REGULATED POWER SUPPLY
SPIKE SUPPRESSOR (PACKED WITH PRO+ CONTROLLER) REQUIRED FOR CIRCUIT PROTECTION.
REQUEST TO EXIT INPUT DEVICE. (N.O. - MOMENTARY) SEE "CONFIGURE SYSTEM" TO SET FUNCTION.
N.O.
C.
ELECTRIC STRIKE OR OTHER FAIL SECURE TYPE OF LOCKING DEVICE.
C.
N.O. OR N.C.
(DOES NOT MATTER)
DOOR STATUS SWITCH WHEN CONTACTS CHANGE STATE (DOOR OPENS) REMAINING TIME DELAY IS CANCELLED AND DOOR LOCKS IMMEDIATELY WHEN CLOSED.

INTERFACE WITH DRY CONTACTS

For locking devices/door controllers which require dry contact input such as electric latch retraction devices, automatic door operators, etc. Consult the technical documentation supplied with that product to determine the correct setting for the output relay and set it accordingly.


RED(+)
BLACK(-)
GREEN
GREEN
CONFIGURE FOR N.C. OR N.O. OUTPUT DEPENDING ON REQUIREMENTS OF CONTROLLED DEVICE. SEE "CONFIGURE SYSTEM".
WHITE
WHITE/ORANGE
BROWN
12/24VDC FILTERED REGULATED POWER SUPPLY
DEVICE REQUIRING DRY-CONTACT INPUT SUCH AS AN AUTO OPERATOR OR ELECTRIC LATCH RETRACTION DEVICE.
REQUEST TO EXIT INPUT DEVICE. (N.O. - MOMENTARY) SEE "CONFIGURE SYSTEM" TO SET FUNCTION.
N.O.
C.
C.
N.O. OR N.C.
(DOES NOT MATTER)
DOOR STATUS SWITCH WHEN CONTACTS CHANGE STATE (DOOR OPENS) REMAINING TIME DELAY IS CANCELLED AND DOOR LOCKS IMMEDIATELY WHEN CLOSED.

BATTERY POWERED PRO78+BP/PRO79+BP:

1.

SELECT BEST LOCATION FOR COMPONENTS

Batteries must be accessible for replacement. Therefore they should not be located in the same box as the PRO+BP keypad if the anti-tamper plugs are to be used. A single gang box with a blank cover plate located inside the locked room is a good idea.

2.

INSTALL SYSTEM COMPONENTS

Battery pack, locking device, and PRO+ controller (as shown on page1).
NOTE: do not install anti-tamper plugs at this time.

3.

TEST SYSTEM

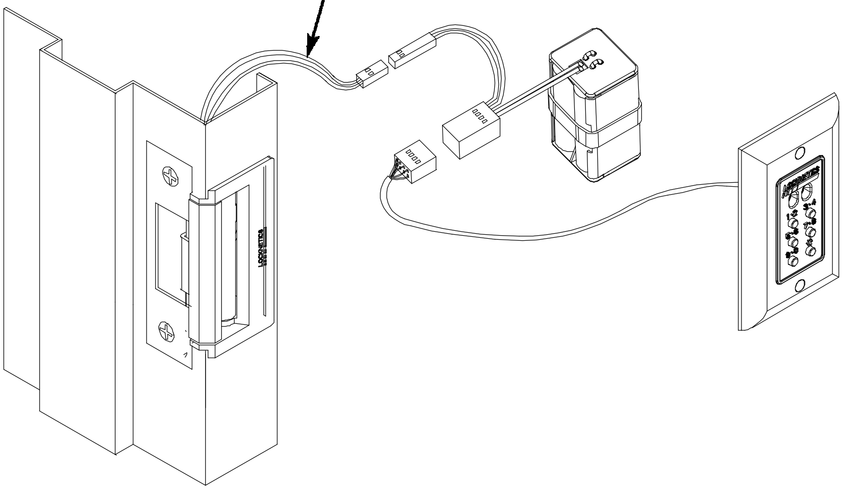
On the PRO+ keypad, enter **13579 (the factory default access code)**. The lock should unlock for 8 seconds, then relock. If not, check wiring and mechanical installation for accuracy and good connection.

4.

PROGRAM LOCK

Refer to the programming guide (Form 58000) included with the unit for complete programming instructions and information on low battery indication, memory reset and time delay setting.

NOTE: the PRO+BP does not support the use of request to exit device or door contact. Therefore, there is no need to configure the system as in the hard wired version.



When making connections to battery powered lock connect black to black and white to white (or red).

Px 95

MiniProx Reader Installation Manual

Installation Requirements

The following instructions will explain the installation procedure for the MiniProx Reader. The instructions include these sections:

Mounting Instructions (hazardous & nonhazardous)

Connecting the Reader to the Host

Testing & Operation of the MiniProx Reader

Parts List (included)	Quantity
1) MiniProx	1
2) #6-32 x 1" self tapping, Type T or 232	2
3) This Installation Sheet	1
4) Box, Hazardous unit only	1
Parts Recommended (not included)	
1) Wire Splice	9
2) Grommet	1
3) DC Power Supply 4.75 to 16VDC, 50mA	1
4) Cable, 10 conductor , 22 AWG	

Mounting Instructions

1. Determine an appropriate mounting position for the Reader.

Tolerances .xx =/- .03"
.xxx =/- .010"

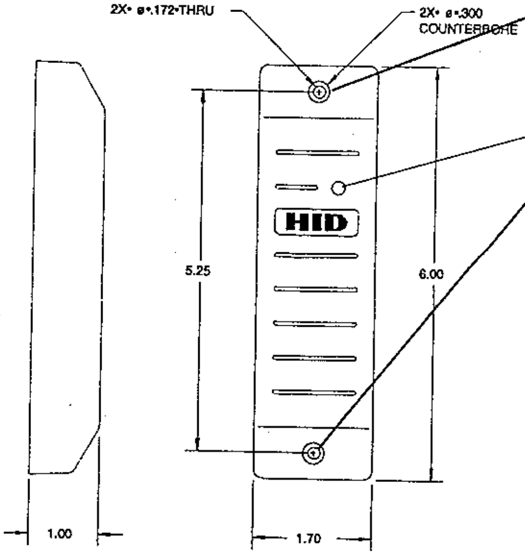


Figure 1

2. Drill two 7/64th (.109) Inch holes for mounting the Reader to the surface.

3. Drill a 3/8 to 1.0 Inch hole for the cable. If you are mounting on metal place a grommet around the edge of the hole.

4. Route the interface cable from the Reader and/or power supply to the Host. ***Linear type power supply is recommended.***

Check all electrical codes for proper cable installation

Mount the Reader with the screws provided when mounting onto metal mullions or junction boxes. On other materials use appropriate fasteners.

Connecting the Reader to the Host

The MiniProx is available with an 18" **Pigtail** with a 10 conductor cable and a 10 conductor **terminal strip.**

a. **Pigtail** - Prepare the new cable by cutting the cable jacket back 1-1/4" and strip the wires ¼".
b. Splice the cable and the pigtail together and seal the splice if the Thin Line will be an outdoor unit. **Trim and cover all conductors that are not used.**
c. **Terminal Strip** - Loosen the terminal strip screws until the top of the screw is flush with the back surface of the Reader. **Be careful not turn them further; they are not captive and will fall out.**

d. Prepare the new cable by cutting the cable jacket back 1-1/4 inches and strip the wire ¼ ". **Twist the ends of the wires to eliminate stray strands.**
e. Form each wire into a hook and install each wire by wrapping it around the screw.

Connect the Reader to the Host according to this wiring diagram and the Host installation guide.

The legend for wiring is color coded according to the "Wiegand Standard" for the recommended cable.

The numbering for the terminals is shown on the back label and in Figure 2

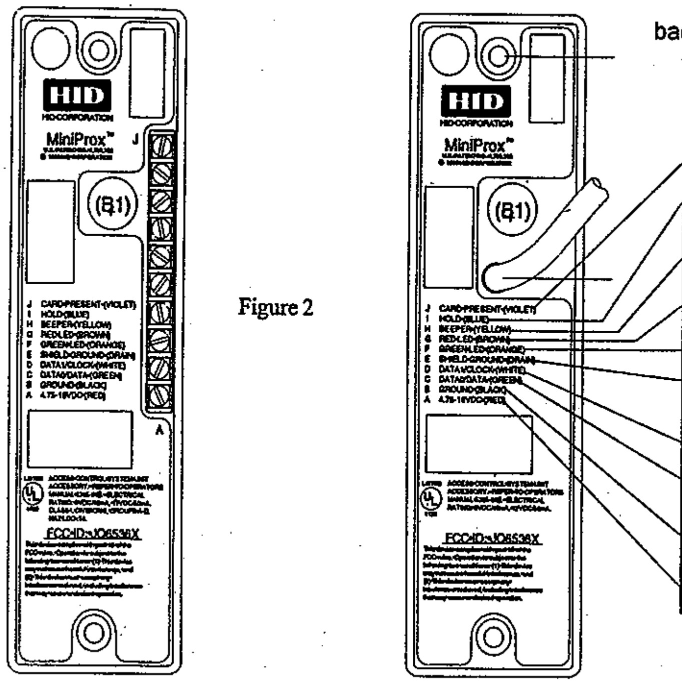


Figure 2

Terminal Strip

Pigtail

Color	Wiegand	Clock & Data
Violet	---	Card Present
Blue	*Hold	*Hold
Yellow	*Beeper	*Beeper
Brown	*Red LED	*Red LED
Orange	*Green LED	*Green LED
Drain	Shield Ground	Shield Ground
White	Data 1	Clock
Green	Data 0	Data
Black	Ground	Ground
Red	+DC	+DC

* These connections are OPTIONAL.
All other connections are required.

Marking the wires will make future maintenance easier.

Cable Notes

1) When using a separate power supply for the Thin Line II, the power supply and Host should have a common ground (voltage reference).

2) If the Host is controlling the beeper, Hold, or the LEDs are configured for the dual LED mode, additional conductors will be required. The recommended cables are Alpha 1295C, 1296C, 1297C, 1298C and 1299C that are five, six, seven, eight and nine conductors respectively. Larger wire gauges are acceptable. The wire is to be stranded with an overall shield, either foil or braided.

3) The Cable shield should be connected to the Shield Ground on Reader TB1- E, and left floating at the panel or power supply end of the cable. This configuration is the best for shielding the reader cable from external interference and reducing the likelihood of the Reader causing interference.

Testing & Operation of the MultiProx Reader

After wiring the Reader and power supply, the Reader is ready to be tested.

1. Power up the Reader and the LED and Beeper will flash and beep 3 times in a sequence of two short delays and one long delay. This indicates that the micro-controller unit is working properly.
2. Present an ID card to the Reader and the LED should momentarily turn green, indicating a read of the card.
3. If the Reader LED is controlled by the Host refer to the Host description of the LED operation.

NOTES:
THE ABOVE ARE RECOMMENDED INSTALLATION PROCEDURES. ALL LOCAL, STATE AND NATIONAL ELECTRICAL CODES TAKE PRECEDENCE.

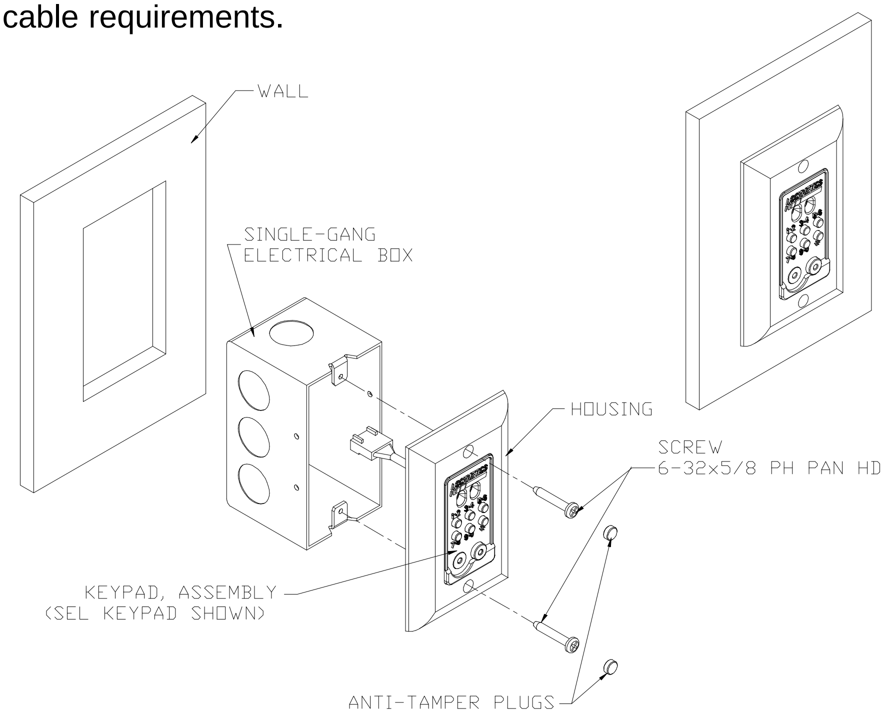
LOCKNETICS
Security Engineering

575 Birch Street, Forestville, CT 06010
Phone (860) 584-9158   Fax (860) 584-2136
WWW. LOCKNETICS .COM

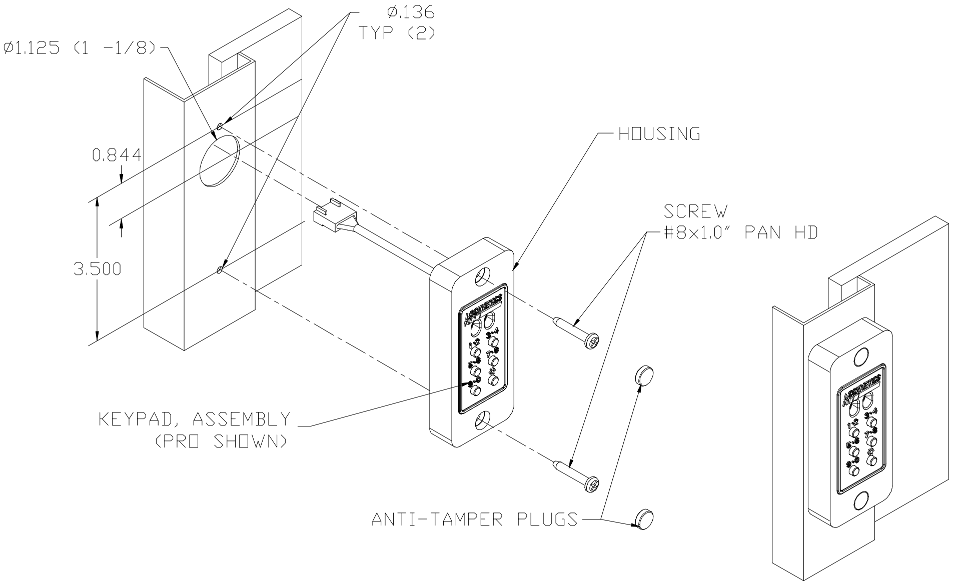
KP78+,KP79+,PRO78,PRO79,TR83,TR84
KEYPADS AND TOUCHENTRY™ READERS
MOUNTING INSTRUCTIONS

Note: see controller/system manual with which keypad/touchentry key reader will be used for specific wiring and/or cable requirements.

KP79+
PRO79
TR84



KP78+
PRO78
TR83


Ø.136
TYP (2)
Ø1.125 (1 -1/8)
0.844
3.500
HOUSING
SCREW
#8x1.0" PAN HD
KEYPAD, ASSEMBLY
(PRO SHOWN)
ANTI-TAMPER PLUGS