EntryPoint™ & TrustPoint™ Smart Card Readers Installation & Operation Guide

IDFACTORS™, Inc
2621 5th Street
Berkeley, CA 94710
(510) 346 1510

Revision: 3.0
Release Date: August 2020

Contents

Description

EntryPoint and TrustPoint one and two-factor smart card readers operate seamlessly with all physical access control systems (PACS), allowing legacy PACS to be upgraded to operate with all government issued PIV and CAC credentials. Based on the model, readers support both ISO 7816 contact and/or ISO14443 contactless mode. In addition, TrustPoint authenticating readers perform a cryptographic challenge-response to the smart card for High Security Level III facilities.

Features

- Support Federal PIV, PIV-I and all DoD CAC Cards
- Support contact, contactless and dual-interface visitor cards
- Vertical card slot with protective shutter resists foreign objects and wind driven rain
- Durable weatherized telephone keypad
- Illuminated card slot and keypad for night use
- Support “Card plus PIN” and “Card Only” operating modes
- Terminal block. RJ-45 & USB connectors
- Wiegand and RS-485 communication
- Field flash programmable
- PKI challenge (up to ECC P512 & RSA 3072 key size)*
  * *TrustPoint readers only*

Specifications

Input Voltage	9 to 18VDC (12V nominal)
Power Consumption	300mA idle, 420mA peak @ 12 VDC
Operating Temperature Range	-25ºF to + 150ºF (-32ºC to + 66º)
Relative Humidity	5% to 95% (non-condensing)
Physical Dimensions	6.7 in H x 4.6 in W x 2.25 in D
Contact Interface	ISO 7816-3: T=0, T=1
Connector Rating	500,000 insertions*
Contact Reading Speed	9.6K – 480K bits per second
Contactless Interface	ISO 14443: Type A, Type B
Contactless Read Range	95+% at 1.5 inch (4 cm)
Maximum Read Range	Less than 4 inches (10 cm)
Contactless Reading Speed	106K, 212K, 424K, 847K bps

* UL tested for 100,000 insertions

Supported Access Cards

Readers support a wide range of contact only, contactless only and dual-interface smart cards. These include military access cards, government access cards, and many common industry smart cards. Dependant on the reader model and card type, readers support smart card access in 1-factor, 2-factor and 3-factor modes.

DoD Common Access Cards (CAC)

Common Access Cards or CAC cards are issued by the US Department of Defense to all military personnel.

Government Personal Identity Verification Cards (PIV)

Personal Identity Verification or PIV cards are issued by the US Federal Government to government employees.

PIV Interoperable Cards (PIV-I)

PIV interoperable cards are issued by government contractors who have certified their credentials with the Federal Government PKI Bridge.

PIV Compatible Cards (PIV-C)

PIV compatible cards are issued by enterprise companies who wish to implement secure access control equivalent to Federal PIV standards.

Transport Worker Identification Credential (TWIC)

TWIC cards are issued by the Transport Security Administration to workers requiring access to maritime ports and other secure locations.

Visitor Cards

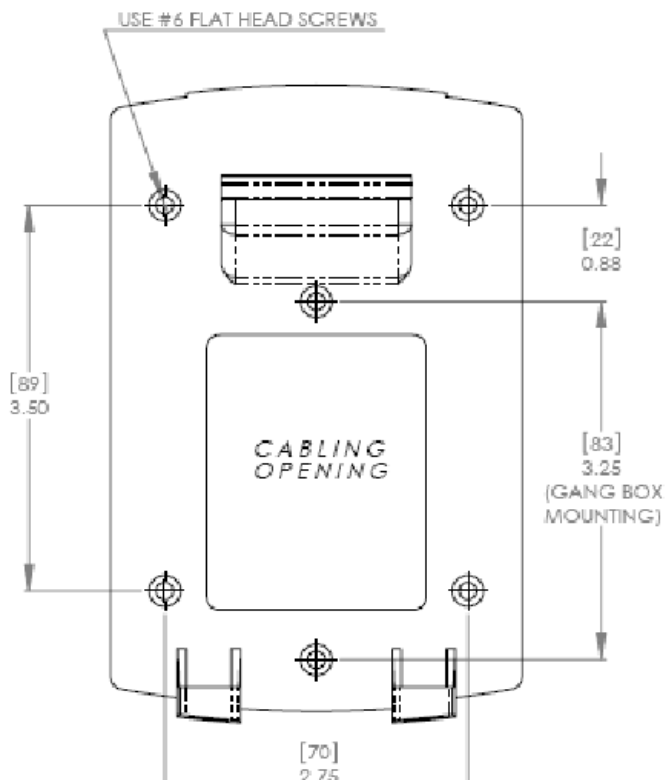
Compatible visitor cards are available in several forms including contact only, contactless only and dual-interface smart cards.

Cryptographic Validation

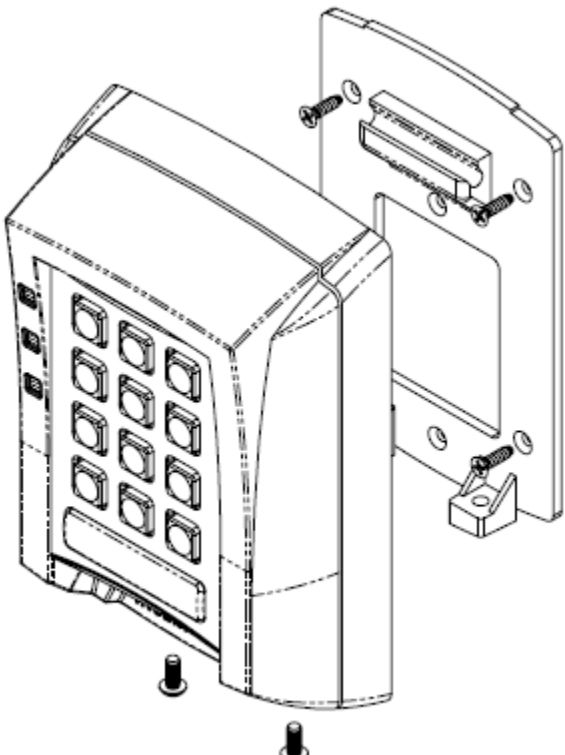
Cryptographic reader models are uniquely capable of performing a PKI challenge-response against a private key stored on smart cards including CAC, PIV and TWIC cards. When used in conjunction with enabling PACS software this ensures that the cards have not been duplicated or tampered with.

Reader Installation

The readers come with a backplate suitable for mounting directly onto a standard electrical gang box or onto a hollow wall. Recommended reader mounting height from the floor is "shoulder height" or about 60 inches. If necessary reader height may be lowered to accommodate disability requirements.



Securing the Reader

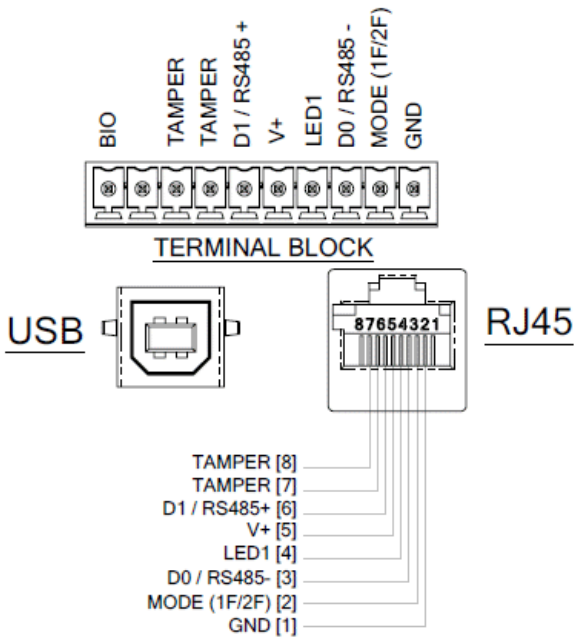


Once power and signal connections to the reader have been made (see Connector Wiring) the reader hooks on to the mounting plate and is secured from below using two 8-32 x ⅜" screws. BridgePoint recommends and supplies tamper-resistant security screws. The supplied screws require a Torx Wrench #T15.

An optional integrated tamper switch maybe wired to signal to the PACS when the reader is detached from the mounting plate.

Connector Wiring

For maximum installation convenience, reader connections are provided on both a screw terminal block and an RJ-45 socket suitable for a pre-terminated cable, as shown in the diagram below. The terminal block is detachable for easy wiring.



V+	9 -18VDC (12V nominal)	**D0/D1**	Wiegand/RS485 data
LED1	Panel grant/deny signal	**MODE**	1 or 2 factor mode select

Wire Gauge	22AWG	20AWG	18AWG	CAT5
Cable Distance	200 feet (60m)	300 feet (90m)	500 feet (150m)	150 feet (45m)

Reader Configuration

Readers can be field configured through a command interface accessed through a built-in USB port. The USB port is connected to a host computer via a standard USB A/B cable and outputs a CMD> command prompt. A convenient Windows configuration utility, ReaderConfig.exe, can be downloaded to simplify reader setup.

Configuration commands, which are case-insensitive, comprise a keyword, which can be abbreviated to a 2-letter equivalent, plus a variable number of command parameters. A "??" command lists all available configuration commands. Entering a command with a "?" parameters displays a brief of summary of the command parameters. Entering a command without parameters will display the current configuration.

Command	**Abr.**	**Description**
COMMANDS	??	Show commands and syntax
CONTACTLESS	CL	Set maximum C/L speed
DATETIME	DT	Set date and/or time*
DEBUG	DB	Set debug level
DESKEY	DK	Set DESFire key
DURESS	DU	Set duress mode
FACILITY	FN	Set Facility Code
FICAM	FC	Set FICAM compatibility
HEARTBEAT	HB	Set reader heartbeat
LEDMODE	LM	Set LED mode
PINMODE	PM	Set Pin mode
PINTYPE	PT	Set Pin type
PKI	PK	Set PKI mode†
REFLASH	RF	Reflash reader firmware
RESET	RS	Reset reader
RESTORE	RD	Restore default settings
SECMODE	SM	Set security mode
VERSION	VV	Show firmware version
WIEGDEF	WD	Define Wiegand format
WIEGFMT	WF	Select Wiegand format

* *Deprecated option*
† *TrustPoint readers only*

Wiegand Data Formats

Readers can be configured to generate Wiegand data formats to match common PACS and government issue or compliant smart cards. The Wiegand format number is configured via the WF command. If required different Wiegand formats can be selected according to the mode and/or card type.

e.g. **CMD>WF 05**
CMD>WF PIV 03

Dependant upon the card type, data is generated from fields in the FASC-N (Federal Agency Smart Credential Number), CSN (card serial number) or GUID (globally unique ID). A range of standard Wiegand formats is built-in and additional formats can be user defined.

#	Format
00	No Wiegand format
01	64-bit Card Serial Number
02	32-bit FASC-N (SY12:CN20)
03	64-bit FASC-N (AG16:SY16:CN32)
04	48-bit FASC-N (AG14:SY14:CN20)
05	75-bit GSA PIV
06	75-bit GSA PIV no parity
08	26-bit H10301 (8-bit site code)
09	37-bit H10304 (16-bite site code)
10	41-bit ACOE (CSN)
11	41-bit ACOE (FASC-N)
15	64-bit FASC-N (AG16:SY16:CN24:ERR)
16	200-bit Raw FASC-N
17	96-bit eFASC-N (32-bit certificate hash)
19	56-bit FASC-N (AG14:SY14:CN20:CS4:IC4)
20	48-bit BCD FASC-N (AG:SY:CN)
21	54-bit BCD FASC-N (AG:SY:CN:CS:IC)
25	32-bit Mifare UID

AG	Agency Code	SY	System Code
CN	Credential Number	CS	Credential Series
IC	Individual Issue Code	CSN	Card Serial Number
ERR	Error Code	GUID	Globally Unique ID

Security Mode

The reader security mode can be configured as 1-factor (card only), 2-factor (card plus PIN or card plus biometric) or 3-factor (card plus PIN plus biometric) dependant on the reader model and required security level. Default security mode is 2-factor card plus pin. The security mode can be configured via the SM command with parameters of 1F, 2F, 2B or 3F (or NO to reset the security mode setting).

e.g. **CMD>SM 1F**

When no security mode is configured the mode can alternatively be controlled from the MODE input on the reader's signal connector. If the MODE input is +5V or unconnected the reader defaults to 2-factor mode. If the MODE input is GND the reader switches to 1-factor mode (strapping between positions 1 and 2 on the terminal block selects 1-factor mode).

The MODE input also allows the mode to be controlled via a signal from the PACS panel. This enables the mode to be dynamically switched according to, for example, the time of day, day of the week, or threat level.

PIN Mode

PIN entry is normally determined according to the security mode, where 2-factor and 3-factor mode require PIN entry. Dependant on the card type, the PIN can be between 4 and 8 digits. PIN entry is indicated when the reader illuminates the yellow LED. The PIN is entered via they reader keypad and terminated by a # or ETR key. The PIN is then verified by the card and if correct triggers the card data to be sent to the PACS panel for access control.

Although it is not Federal policy, readers can be configured to send the PIN to the panel for verification via the PM command. PIN digits can be buffered until # or ETR (PB mode) or sent to the panel as entered (PP mode). Most common pin-to-panel PIN types can be specified via the PT command.

e.g. **CMD>PM PP**
CMD>PT 4B

It is also possible to configure readers to send PIN digits to the panel" at

any time using “pin-pass-thru” (PT mode). This mode can be used to configure PIN verification by the panel in contactless mode

e.g. **CMD>PM PT**

Note that CAC and PIV cards only allow a small number of failed PIN entry attempts before locking the card to prevent further use. Unlocking a locked card can only be performed by the card issuing authority. For this reason the readers first check the number of retry attempts left and do not present a PIN for verification if there is only one attempt remaining. This allows the PIN to be entered correctly using a desktop reader in order to reset the card’s PIN retry counter.

Reader Heartbeat

When idle the reader is configured to generate a brief red LED flash every few seconds to indicate that it is powered on. This can be disabled or overridden by a heartbeat signal from the panel via the HB command.

e.g. **CMD>HB PN**

Debug Levels

Readers can be configured to output various levels of debug information while processing a presented card. This can be useful for example when testing a specific card type or a Wiegand format. Debug levels can be specified as a list or added to or subtracted from the current levels using a preceding ‘+’ or ‘-‘ sign. “User” and “Feedback” debug levels are enabled by default

e.g. **CMD>DB +AT**
CMD>DB US FB

Default Configuration

Readers can be restored to their default configuration using the RD command.

e.g. **CMD>RD**

Reader Operation

When a card is presented to a reader either contact or contactless it reads and validates the data on the card and optionally verifies the PIN. If this succeeds the reader briefly flashes its green LED to indicate card processing was successful. The reader then selects the card data according to the configured Wiegand format, sends it to the PACS panel, waits for the panel to indicate access granted or denied, then indicates accordingly on its red or green LED.

Access Grant/Deny

After a card has been presented and the card data sent to the PACS panel for access control, the reader monitors the LED1 input signal used by the PACS to indicate access granted or access denied. Depending on the signal received the reader will indicate the panel response via its green (granted) or red (denied) LEDs.

The reader supports three configurable signaling modes for the LED input: Red/Green Zero (RGZ), which is the default, Red/Green Pulsed (RGP) or Green/Red Pulsed (GRP) which can be configured via the LM command.

e.g. **`CMD>LM RGP`**

The meaning of the LED control signal sampled by the reader is as follows:

- Red/Green Zero (RGZ) Mode (default)
- Red/Green Pulsed (RGP) Mode
- Green/Red Pulsed (GRP) Mode

LED Status Indicators

In addition to signaling access granted or access denied, readers use the red, yellow and green LEDs to indicate reader status as shown in the following table:

Red	Yellow	Green	Meaning	Behavior
☼ S	☼ S	☼ S	Power On/Reset	All LEDs flash in sequence
☼ F	☼ F	○	Card Reset Error	Red and yellow flash rapidly
○	○	○	Card Inserted	All LEDs off
○	○	☼ 1	Card Good	Green flash briefly
☼ A	☼ A	○	Card Error	Red and yellow toggle rapidly
☼	○	○	Card Expired	Red on solid
☼ A	☼ A	○	Pin Locked	Red and yellow toggle rapidly
○	☼	○	Pin Request	Yellow on solid
☼ 1	○	○	Pin Key Press	One red flash per key-press
○	○	☼ 1	Pin Good	Green flash briefly
☼ A	☼ A	○	Pin Bad	Red and yellow toggle rapidly
○	☼ 1	○	Pin Restart	One yellow flash per key-press
○	○	☼	Access Granted	Green on solid
☼	○	○	Access Denied	Red on solid

○	LED off	☼	LED on (solid)
☼ 1	LED flash once	☼ F	LED flashing
☼ A	LEDs alternating	☼ S	LEDs flashing in sync

PKI Validation

TrustPoint reader models can perform a cryptography challenge-response to a PKI private key stored on the smart card to ensure that the card has not been copied or cloned. This process uses the public key extracted from a certificate read from the card. RSA key sizes up to 3072-bits and Elliptic curve keys to P384 are supported. The certificate and key used depend upon the type of card and the security mode.

	High security – 2 Factor (Card plus PIN)		**Low security – 1 Factor (Card only)**	
	Contact	**Contactless**	**Contact**	**Contactless**
CAC Card	PIV Auth Certificate	N/A [1]	No [2] Challenge	No [2] Challenge
PIV Card	PIV Auth Certificate	N/A [1]	Card Auth [3,4] Certificate	Card Auth [3,4] Certificate

Note 1: Cards only support PIN verification in contact mode
Note 2: CAC cards do not contain a Card Authentication Certificate
Note 3: Access to the PIV certificate requires PIN entry
Note 4: Certificate challenge in low security mode is configurable for PIV cards

FICAM Compliance

ID Factors offers powerful Federal Identity Credential and Access Management (FICAM) compliant reader hardware and enrollment software. This can be used to upgrade legacy PACS solutions to full conformance with Federal Information Processing Standard FIPS-201, NIST Special Publication SP800-116 and Presidential Directive HSPD-12, without requiring expensive overlay networks or additional Internet connections.

A variety of PACS vendors support IDFACTORSFICAM compliant PKI PACS architecture. Check with IDFACTORS for details of compatible FICAM approved PACS systems.

Copyrights and Trademarks

EntryPoint™ & TrustPoint™
Smart Card Readers
Installation, Configuration & Operation Guide
Revision: 3.0
Release Date: August 2020