



PNI DK220

Access control keypad/Клавиатура за контрол на достъпа/

Zugangskontrolltastatur/Teclado de control de acceso

Clavier de contrôle d'accès/Beléptető billentyűzet

Tastiera controllo accessi/Toegangscontrole toetsenbord

Klawiatura kontroli dostępu/Tastatura control acces



EN	User manual	3
BG	Ръководство за употреба	25
DE	Benutzerhandbuch	50
ES	Manual de usuario	74
FR	Manuel utilisateur	98
HU	Használati utasítás	122
IT	Manuale utente	146
NL	Handleiding	170
PL	Instrukcja obsługi	194
RO	Manual de utilizare	218

Description

PNI DK220 is a stand-alone access control device and proximity reader. It is equipped with two relays for two-door control and supports a maximum of 2000 users, each user can have a PIN code and an access card.

The keypad can be connected to an electromagnetic key, an alarm system, a doorbell, an access button or a door sensor.

The device has 7 operating modes: Wiegand card reader, access control for one door, access control for two doors, access control with external card reader for two doors, two interconnected units for two doors, anti-passback for one door and two-door anti-passback.

Main features

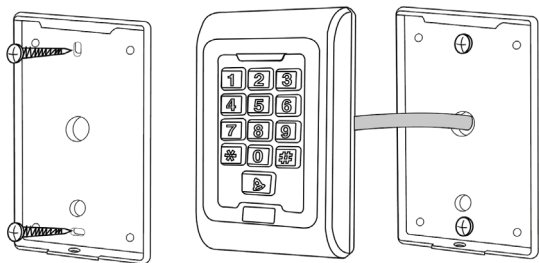
- Aluminum alloy housing with IP65 water resistance class
- Built-in 125KHz card reader
- Illuminated numeric keys. The key light can be programmed as follows: Normal ON, Normal OFF or Human-Approach ON (lights up when it detects motion).
- Tamper alarm, door sensor trigger alarm, duress code alarm This code can be used when the user is forced to threaten to open the door. When typing this code, the door will open but will activate a silent alarm).
- Add and delete cards with the administrator card.
- Register and delete users by keys.

Technical specifications

Supply voltage	12V AC/DC
Standby consumption	<25mA
Electric lock output load	<1A
Alarm output load	<1A
Doorbell output load	<1A
Card reading distance	maximum 40 mm
User capacity	maximum 2000
Compatible cards	EM 125Khz/HID 125KHz
Card transmission format	26-37 bit Wiegand
Keypad transmission format	4 bit and 8 bit and virtual card number
Working temperature	-26°C ~ +80°C

Installation

Choose the installation location and make holes in the wall that match the holes in the mounting bracket. Secure the wall bracket with the screws included in the package. Pass the cables through the slot in the middle of the holder. Connect the cables. Insulate unused cables to avoid short circuit.



Wiring

Zone 1		
BELL_A	Pink	Doorbell button
BELL_B	Pink	Doorbell button
ALARM+	Red	Alarm connector
AC2	Black	AC input
OPEN2	Yellow	Access button
D_IN2	Brown	Door contact
ALARM2-	Gray	Alarm 2
NO2	Blue	Relay 2 NO
COM2	Purple	Relay 2 COM
NC2	Orange	Relay 2 NC

Zone 2

D0	Green	Wiegand output D0
D1	White	Wiegand output D1
AC1	Red	AC1 (+ 12V)
GND	Black	GND
OPEN1(LED)	Yellow	Access button (for green LED)
D_IN1(BZ)	Brown	Door contact (for buzzer)
ALARM1-	Gray	Alarm 1
NO1	Blue	Relay 1 NO
COM1	Purple	Relay 1 Com
NC1	Orange	Relay 1 NC

Audible and luminous warnings

Status	LED	Buzzer
Standby	Red blinks	
Press key		Di
Read card	Green	Di.
Door 1 open	Green	Di.
Door 2 open	Green blinks	Di.
Successful operation	Green	Di.
Operation failed		DiDiDi
PIN input	Red	
Read card & PIN	Red	
Multiple card reading	Red	
Under menu	Red	
Under settings	Orange	
Administrator card enter	Orange	DiDi
Administrator card exit	Red blinks	Di.
Alarm	Red blinks quickly	Alarm

Quick Programming Guide

1. Administrator settings

* Master code #	00	<i>Input the new Master code # Repeat the new Master code #</i>	Change Master code. <i>Note: The default master code is 999999. The master code must have between 6 and 8 digits.</i>
	01	<i>Read the card</i>	Master card registration for adding cards. <i>Note: Default: zone 1.</i>
	02	<i>Read the card</i>	Master card registration for deleting cards. <i>Note: Default: zone 1</i>
	03	<i>Read the card</i>	“Duress” alarm card registration for zone 1
	04	<i>Read the card</i>	“Duress” alarm card registration for zone 2

<i>* Master code #</i>	05	<i>Input the 8-digit PIN</i>	Input the “duress” PIN code for zone1 Note: The first digit of the PIN must be 1 for zone 1.
	06	<i>Input the 8-digit PIN</i>	Input the “duress” PIN code for zone2 Note: The first digit of the PIN must be 2 for zone 2.
	07	0000 #	Delete all users
	51	Master open Lock 1	
	52	Master open Lock 2	

Note:

The “duress” PIN and the “duress” card can be used when the user is forced to open the door. When typing this code or reading this card, the door will open but at the same time it will send an alarm signal.

2. User settings for Zone 1 and Zone 2

Add user card

<i>* Master code #</i>	11 (for Zone 1)	<i>Read the card</i>
		<i>Input ID # Read the card</i>
	21 (for Zone 2)	<i>Input card number #</i>
		<i>Input ID # Input card number #</i>

Note: Users can be added one after the other without leaving programming mode. User ID can contain between 1 and 4 digits, in the range 1 - 2000. 1, 01, 001 and 0001 all means 1.

Add user PIN

<i>* Master code #</i>	11 (for Zone 1) 21 (for Zone 2)	<i>Input ID # Input PIN #</i>
------------------------	--	-------------------------------

Note: The PIN can have 4 to 6 digits. The first digit must be 1 for Zone 1 and 2 for Zone 2. "1234" is reserved, cannot be set as PIN.

Delete user

<i>* Master code #</i>	12 (for Zone 1)	<i>Read the card</i>
	22 (for Zone 2)	<i>Input ID #</i>
		<i>Input card number #</i>

Note: Users can be deleted one after the other without leaving the programming mode.

Delete all users

<i>* Master code #</i>	07	0000 #
------------------------	----	--------

Note: This command deletes all users in Zone 1 and Zone 2.

Access modes

<i>* Master code #</i>	13 (for Zone 1)	0 #	By card
	23 (for Zone 2)	1 #	By card + PIN
		2 #	By card or PIN (default setting)

Open door delay

<i>* Master code #</i>	14 (for Zone 1) 24 (for Zone 2)	0 - 99 #	Default setting 5
------------------------	--	----------	-------------------

Set door closing modes

* <i>Master code #</i>	15 (for Zone 1) 25 (for Zone 2)	0 #	Pulse mode (default setting). Each time a code is entered or a valid card has been read, the door will open and close automatically after the set time interval (between 0.05 sec. and 99 sec).
		1 #	Toggle mode. Each time a code is entered or a valid card has been read, the door will open but will not close until the code is entered again or the card will be read.

Open the door with several cards

* <i>Master code #</i>	16 (for Zone 1) 26 (for Zone 2)	1 - 10 #	Default setting 1
------------------------	--	----------	-------------------

Note: The door will only open after all the cards have been read. For example, by order * **Master code # 16 3 #**, you have to read 3 cards in a row to open the door. This setting is only useful if you have set the keypad to card access mode.

Add user cards in series

<i>* Master code #</i>	17 (for Zone 1) 27 (for Zone 2)	<i>Input ID #, Input card number #, Input quantity #</i>
------------------------	--	--

Note: Card numbers must be consecutive (between 8 and 10 characters). Card quantity is between 1 and 2000.

3. System settings

<i>* Master code #</i>	30	0-15 #	Setting the unit code (Facility Code). Default: 0
	31	0 #	Reader Wiegand
		1 #	One-door stand-alone access control (default setting)
		2 #	Stand-alone access control for two doors
		3 #	With external reader for two doors
		4 #	Two interconnected units for two doors (protection when opening multiple doors)

<i>* Master code #</i>	31	5 #	Anti-passback for a door
		6 #	Anti-passback for two doors
	32	26-37 #	Wiegand format setting 26 34 37. Default 26.
	33	0-2 #	Keypad transmission format setting: 0 1 2 After resetting, this setting keeps unchanged.

<i>* Master code #</i>	34	1-3 #	Set alarm duration (default setting 1 minute) After resetting, this setting keeps unchanged.
		0 #	Safe mode 1. Normal mode. (default setting)
	35	1 #	Safe mode 2. If the wrong code is entered or an invalid card is read 10 times in a row within 10 minutes, as a safety precaution, the system shuts down.

* Master code #	35	2 #	Safety mode 3. Alarm mode. If the wrong code is entered or an invalid card is read 10 times in a row within 10 minutes, as a precaution, the external alarm (if connected) and the buzzer built into the keypad will be triggered.
-----------------	----	-----	---

4. Optional user settings

* Master code #	41	0 #	Buzzer off. The buzzer remains active only when the device enters programming mode.
		1 #	Active key sound (default setting)
	42	0 #	Key backlight off
		1 #	Key backlight on
		2 #	Automatic mode. Normally, the key light is off but turns on when human presence is detected.

* <i>Master code #</i>	43	0 #	LED off when the device is in standby.
		1 #	The LED flashes when the device is in standby mode. (default setting)

Important notes

1. The master code must have 6-8 digits.
2. The code “duress” must have 8 digits. The first digit of the code must be 1 for Zone 1 and 2 for Zone 2.
3. User PIN must have 4-6 digits. The first digit of the PIN must be 1 for Zone 1 and 2 for Zone 2.
4. User ID can be any number between 1 and 2000.
5. The card number must have between 8 and 10 digits. If the card number contains less than 8 digits, add 0 in front of the code.
6. Open door delay time: between 0 and 99 seconds. 0 = 50mS
7. When a user card is registered in the device, the device will automatically generate a PIN 1234 that cannot unlock the door.
8. If an invalid master PIN is entered, the device enters standby after 5 seconds. If a valid master PIN is entered, the device enters standby mode after 30 seconds.
9. When using the keypad, pressing the # key confirms the previously executed key command. When adding or deleting cards one after the other, pressing the # key indicates the end of the cycle, and pressing the * key indicates exit from this operation.
10. When you add cards in series, the device automatically assigns an ID number and a card number. The ID number and card number increase automatically with each card added, up to a maximum of 2000.

11. The operating mode and transmission format of the keypad are set at the factory. The user can change these settings as needed. After resetting the device, this setting remains unchanged.

12. After successfully registering users in Zone 1, the LED turns green. After successfully registering users in Zone 2, the green LED flashes.

5. Master card operations

Add user for Zone 1

Read the master add card, then Read the user cards one after the other, and finally Read the master add card again.

Delete user for Zone 1

Read the master delete card, then Read the user cards one after the other, and finally Read the master delete card again.

6. User operations

By card

Read the card. The lock will unlock.

If you have set multiple cards for the door opening (between 2 and 10), read all the cards one after another within 5 seconds, after which the lock will unlock.

By card + PIN

Read the card, input the PIN (4 or 6 digits) +#. The lock will unlock.

By card or PIN

Read the card. The lock will unlock. Or input the PIN +#. The lock will unlock.

Change PIN without entering programming mode

** read user card, input old PIN #, input new PIN # repeat new PIN*

or

** input ID number # input old PIN #, input new PIN # repeat new PIN*

Note: The PIN for Zone 1 must start with 1, and the PIN for Zone 2 must start with 2.

7. Alarm function

Tamper alarm

If the device is disassembled by burglary, the internal buzzer and external alarm (if connected) will sound.

Open door alarm

If you have connected a wired door sensor to the access control keypad and this sensor will trigger, the internal buzzer and external alarm (if connected) will sound.

To turn off the alarm:

Read the user card or master card, or input the master PIN.

If you do not perform any operation, the alarm will turn off automatically after 1 minute.

“Duress” alarm

If the “duress” card is read or the “duress” PIN code is entered on Zone 1 or Zone 2, the lock will open and, at the same time, the external alarm will be triggered (if connected). The internal buzzer will not be triggered.

8. Operating modes

Wiegand card reader

In this mode, the keypad functions as a card reader connected to an access control device.

Supported orders:

- Change master PIN
- Set facility code
- Card transmission format setting
- Keypad transmission format setting
- Optional settings
- Tamper alarm

Stand-alone access control for a single door

Under this mode, the keypad opens a single door. The door can be opened by card or PIN or card + PIN. The keypad supports connecting an external card reader or an access button to exit the building.

Stand-alone access control for two doors

Under this mode, the keypad can control two doors. Read the card or input the PIN for Zone 1 and door 1 will open. Read the card or input

the PIN code for Zone 2 and door 2 will open.

With external card reader to open two doors

Under this mode, the keypad allows access for door 1, and the external card reader allows access for door 2.

Read the card or input the code for Zone 1 on the access control keypad. Door 1 will open. Read the card or input the code for Zone 2 on the external card reader. Door 2 will open.

Two interconnected devices to open two doors

This mode is more suitable for locations such as banks, prisons or for situations that require an advanced level of security. Only after door 2 is closed, read the card or input the code on the keypad to open door 1. And only after door 1 is closed, read the card or input the code on the card reader to open door 2.

Anti-passback for a single door

In this mode of operation, the keypad must be installed outdoor to allow the access inside the building, and the external card reader must be mounted indoor to allow the exit out of the building.

If the user's entry into the building has not been registered, the user cannot exit by reading the card on the card reader. Also, the user cannot enter the building a second time if his exit has not been registered.

Note: The door can only be opened by reading the card for Zone 1. All other Zone 1 and Zone 2 access modes are invalid.

Anti-passback for two doors

In this mode, the keypad on door 1 is the anti-passback master unit, and the external card reader on door 2 is the secondary anti-passback unit. Thus, an anti-passback system suitable for installation in parking lots is created.

The user can enter the building on door 1 by reading the card on the access control keypad and can only exit on door 2 by reading the card on the external card reader. If the user's entry has not been registered on door 1, he will not be able to exit on door 2. Also, the user cannot enter a second time if his exit has not been registered.

Note: The door can only be opened by reading the card for Zone 1. All other Zone 1 and Zone 2 access modes are invalid.

Troubleshooting

Problem	Cause	Solution
Card reading distance too short	Low card quality	Use original cards
PIN setting problems	<ol style="list-style-type: none">1. The PIN does not comply the standard2. You are in card reading mode, set the password	<ol style="list-style-type: none">1. The first digit of the PIN must be 1 or 2, according to the Zone.2. The PIN must not be 1234. The PIN must be 4 or 6 digits long.

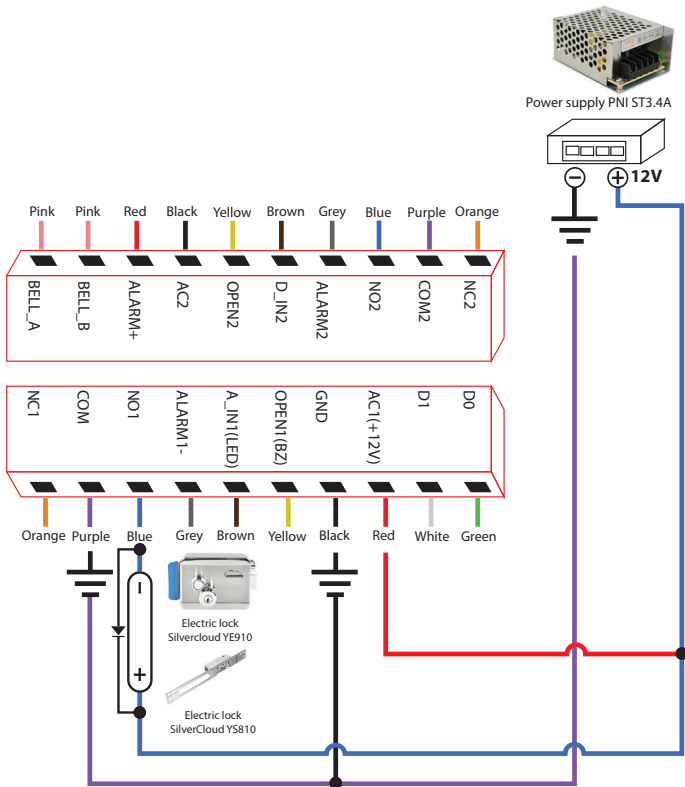
The PIN does not open the door	<ol style="list-style-type: none"> 1. You have used PIN 1234 2. The set access mode does not allow PIN access 	<ol style="list-style-type: none"> 1. Change your PIN. 2. Change the access mode: card or PIN.
No answer after reading the card	The keypad is not in standby, it can be in programming mode	Press the * key, the LED flashes. The keypad is now in standby mode.
The keypad does not light up	Wrong keypad settings	<ol style="list-style-type: none"> 1. Set the key backlight to on or on. In auto mode, the keys only light up after they are pressed and remain lit for 30 seconds.
Invalid master code	You forgot the master code	<p>Reset the device. The master code returns to 999999. By reset the user data is not deleted.</p>

Reset the master code

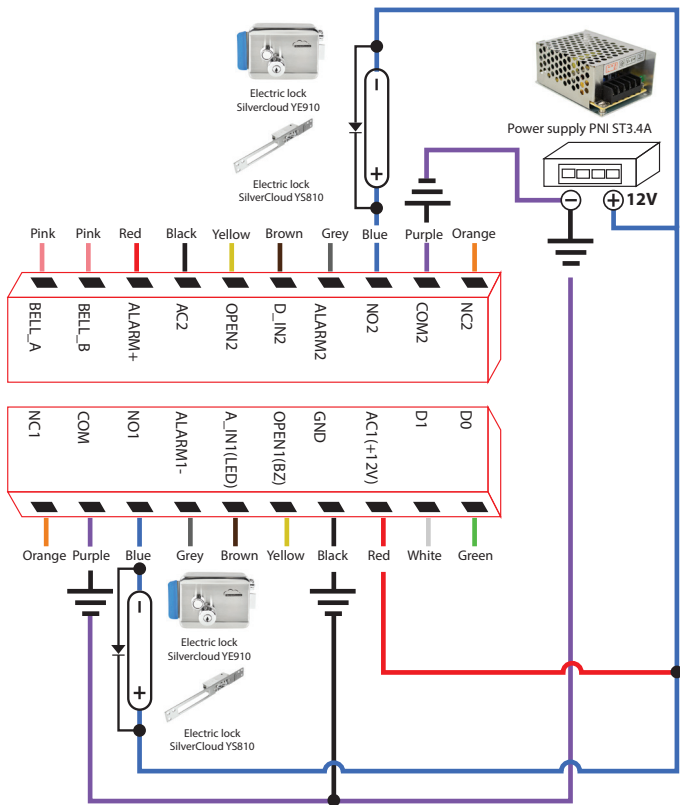
1. Turn off the power to the access control keypad.
2. Hold down the # key while restarting the power.
3. After hearing two Di . sounds, release the # key.
4. The keypad has returned to the factory settings. The master password returns to 999999. The user data has not been deleted.

Connection examples for one and two doors

Access control for one door with Silvercloud YE910 or Silvercloud YS810 electromagnetic lock and PNI ST3.4A power supply.



Access control for two doors with Silvercloud YE910 or Silvercloud YS810 electromagnetic lock and PNI ST3.4A power supply.



Описание

PNI DK220 е самостоятелно устройство за контрол на достъпа и четец за близост. Снабден е с две релета за управление на две врати и поддържа максимум 2000 потребители, всеки потребител може да има ПИН код и карта за достъп.

Клавиатурата може да бъде свързана към електромагнитен ключ, алармена система, звънец, бутон за достъп или сензор за врата.

Устройството има 7 режима на работа: четец на карти Wiegand, контрол на достъпа за една врата, контрол на достъпа за две врати, контрол на достъпа с външен четец на карти за две врати, две взаимосвързани единици за две врати, анти-passback за една врата и две врати анти-passback.

Основните функции

- Корпус от алуминиева сплав с клас водоустойчивост IP65
- Вграден четец на карти 125KHz
- Осветени цифрови клавиши. Ключовата светлина може да бъде програмирана по следния начин: Нормално ВКЛЮЧЕНО, Нормално ИЗКЛЮЧЕНО или ВКЛЮЧЕНО Човешки подход (светва, когато засече движение).
- Аларма за подправяне, аларма за задействане на сензор за врата, аларма за код за принуда Този код може да се използва, когато потребителят е принуден да заплашва да отвори вратата. Когато въведете този код, вратата ще се отвори, но ще активира тиха аларма).
- Добавяне и изтриване на карти с администраторската карта.
- Регистрирайте и изтривайте потребители по ключове.

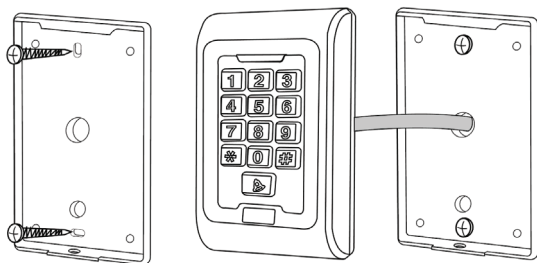
Технически спецификации

Захранващо напрежение	12V AC/DC
Консумация в режим на готовност	<25mA
Изходно натоварване на електрическата брва	<1A
Натоварване на алармен изход	<1A
Задача за извеждане на звънене	<1A
Разстояние за четене на карти	максимум 40 мм
Потребителски капацитет	максимум 2000г
Съвместими карти	EM 125Khz/HID 125KHz
Формат за предаване на карта	26-37 бита Wiegand
Формат за предаване на клавиатурата	4-битова и 8-битова и номер на виртуална карта
Работна температура	-26°C ~ +80°C

Инсталация

Изберете мястото за монтаж и направете дупки в стената, които съвпадат с дупките в монтажната скоба. Закрепете скобата за стена с винтовете, включени в опаковката. Прекарайте кабелите през слота в средата на държача.

Свържете кабелите. Изолирайте неизползваните кабели, за да избегнете късо съединение.



Електрически инсталации

Зона 1		
BELL_A	Розово	Бутон за звънец на вратата
BELL_B	Розово	Бутон за звънец на вратата
ALARM+	Червен	Конектор за аларма
AC2	Черен	ВХОД ЗА ПРОМЕНЛИВ ТОК
OPEN2	Жълт	Бутон за излизане
D_IN2	Кафяв	Контакт на вратата
ALARM2-	Сив	Аларма 2
NO2	Син	РЕЛЕ 2 NO
COM2	Лилаво	РЕЛЕ 2 КОМ
NC2	Оранжево	РЕЛЕ 2 NC

Зона 2

D0	Зелено	Изход на Wiegand D0
D1	Бяла	Изход на Wiegand D1
AC1	Червен	AC1 (+ 12V)
GND	Черен	GND
OPEN1(LED)	Жълт	Бутон за излизане (за зелен светодиод)
D_IN1(BZ)	Кафяв	Контакт на вратата (за зумер)
ALARM1-	Сив	Аларма 1
NO1	Син	РЕЛЕ 1 NO
COM1	Лилаво	РЕЛЕ 1 КОМ
NC1	Оранжево	РЕЛЕ 1 NC

Звукови и светлинни предупреждения

Status	LED	Buzzer
В готовност	Червеното мига	
Натиснете клавиша		Di
Прочетете картата	Зелено	Di.
Врата 1 е отворена	Зелено	Di.
Врата 2 е отворена	Зеленото мига	Di.
Успешна операция	Зелено	Di.
Операцията се провали		DiDiDi
Въвеждане на пин	Червен	
Прочетете картата и пин кода	Червен	
Многократно четене на карти	Червен	
Под менюто	Червен	
Под настройки	Оранжево	
Въведете картата на администратор	Оранжево	DiDi
Изход от администраторска карта	Червеното мига	Di.
Аларма	Червеното мига бързо	Аларма

Ръководство за бързо програмиране

1. Настройки на администратора

* Майсторска треска #	00	Въведете новата Майсторска треска # Повторете новата Майсторска треска #	Смяна Майсторска треска. Забележка: Майсторската треска по подразбиране е 999999. Майсторската треска трябва да има между 6 и 8 цифри.
	01	Прочетете картата	Регистрация на главна карта за добавяне на карти.
	02	Прочетете картата	Регистрация на администраторска карта за изтриване на карти.
	03	Прочетете картата	“Dugess” регистрация на алармена карта за зона 1
	04	Прочетете картата	“Dugess” регистрация на алармена карта за зона 2

* Майсторска треска #	05	Въведете 8-цифрения ПИН	Въведете ПИН кода „принуда“ за зона 1 Първата цифра на ПИН кода трябва да е 1 за зона 1.
	06	Въведете 8-цифрения ПИН	Въведете ПИН кода „принуда“ за зона 2 Първата цифра на ПИН кода трябва да е 1 за зона 2.
	07	0000 #	Изтрийте всички потребители
	51	Администратор отваря заключване 1	
	52	Администратор отваря заключване 2	

Забележка:

ПИН кодът „duress“ и картата „duress“ могат да се използват, когато потребителят е принуден да отвори вратата. Когато въведете този код или прочетете тази карта, вратата ще се отвори, но в същото време ще изпрати алармен сигнал.

2. Потребителски настройки за Зона 1 и Зона 2

Добавете потребителска карта

* Майсторска треска #	11 (за зона 1) 21 (за зона 2)	Прочетете картата
		Въведете ID # Прочетете картата
		Въведете номера на картата #
		Въведете ID # Въведете номера на картата #

Забележка: Потребителите могат да се добавят един след друг, без да се излиза от режима на програмиране. User ID може да съдържа между 1 и 4 цифри, в диапазона 1 - 2000. 1, 01, 001 и 0001 всички означава 1.

Добавете потребителски ПИН

* Майсторска треска #	11 (за зона 1) 21 (за зона 2)	Въведете ID # Въведете ПИН #
-----------------------	--	------------------------------

Забележка: ПИН кодът може да има от 4 до 6 цифри. Първата цифра трябва да бъде 1 за зона 1 и 2 за зона 2. "1234" е запазен, не може да бъде зададен като ПИН.

Изтриване на потребител

* Майсторска треска #	12 (за зона 1)	Прочетете картата
	22 (за зона 2)	Въведете ID #
		Въведете номера на картата #

Забележка: Потребителите могат да бъдат изтривани един след друг, без да излизат от режима на програмиране.

Изтрийте всички потребители

* Майсторска треска #	07	0000 #
-----------------------	----	--------

Забележка: Тази команда изтрива всички потребители в Зона 1 и Зона 2.

Режими на достъп

* Майсторска треска #	13 (за зона 1)	0 #	С карта
	23 (за зона 2)	1 #	С карта + ПИН
		2 #	С карта или ПИН (имплицитно)

Закъснение при отваряне на вратата

* Майсторска треска #	14 (за зона 1) 24 (за зона 2)	0 - 99 #	Имплицитно 5
-----------------------	--	----------	--------------

Задайте режими на затваряне на вратите

* Майсторска треска #	15 (за зона 1) 25 (за зона 2)	0 #	Импулсен режим (имплицитно). Всеки път, когато бъде въведен код или е прочетена валидна карта, вратата ще се отваря и затваря автоматично след зададения интервал от време (между 0,05 сек. и 99 сек.).
		1 #	Превключване на режима. Всеки път, когато бъде въведен код или е прочетена валидна карта, вратата ще се отвори, но няма да се затвори, докато кодът не бъде въведен отново или картата ще бъде прочетена.

Отворете вратата с няколко карти

* Майсторска треска #	16 (за зона 1) 26 (за зона 2)	1 - 10 #	Имплицитно 1
-----------------------	--	-------------	--------------

Забележка: Вратата ще се отвори само след като всички карти бъдат прочетени. Например, по поръчка * Майсторска треска # 16 3 #, трябва да прочетете 3 карти подред, за да отворите вратата. Тази настройка е полезна само ако сте задали клавиатурата в режим за достъп до карта.

Добавете потребителски карти последователно

* Майсторска треска #	17 (за зона 1) 27 (за зона 2)	Въведете ID #, Въведете номера на картата #, Входящо количество #
-----------------------	--	---

Забележка: Номерата на картите трябва да са последователни (между 8 и 10 знака). Количеството на картата е между 1 и 2000.

3. Системни настройки

* Майсторска треска #	30	0-15 #	Задаване на кода на единицата (Facility Code). Имплицитно: 0
	31	0 #	Читател Виганд
		1 #	Самостоятелен контрол на достъпа с една врата (имплицитно)
		2 #	Самостоятелен контрол на достъпа за две врати
		3 #	С външен четец за две врати
		4 #	Две взаимосвързани единици за две врати (защита при отваряне на няколко врати)

* Майсторска треска #	31	5 #	Анти-passback за врата
		6 #	Анти-passback за две врати
	32	26-37 #	Настройка на формат на Wiegand 26 34 37. Имплицитно 26
	33	0-2 #	Настройка на формата за предаване на клавиатурата: 0 1 2 След нулиране тази настройка остава непроменена.

* Майсторска треска #	34	1-3 #	Задайте продължителност на алармата (неявно 1 минута) След нулиране тази настройка остава непроменена.
	35	0 #	Безопасен режим 1. Нормален режим. (имплицитно)
		1 #	Безопасен режим 2. Ако бъде въведен грешен код или невалидна карта бъде прочетена 10 пъти подред в рамките на 10 минути, като предпазна мярка, системата се изключва.

* Майсторска треска #	35	2 #	Безопасен режим 3. Режим на аларма. Ако бъде въведен грешен код или невалидна карта бъде прочетена 10 пъти подред в рамките на 10 минути, като предпазна мярка, външната аларма (ако е свързана) и зумерът, вграден в клавиатурата, ще се задействат.
-----------------------	----	-----	--

4. Опционални потребителски настройки

* Майсторска треска #	41	0 #	Зумерът е изключен. Зумерът остава активен само когато устройството влезе в режим на програмиране.
		1 #	Звук на активен клавиш (имплицитно)
	42	0 #	Подсветката на клавиша е изключена
		1 #	Подсветката на клавиша е включена
		2 #	Автоматичен режим. Обикновено индикаторът на клавиша е изключен, но се включва, когато се установи човешко присъствие.

* Майсторска треска #	43	0 #	Светодиодът изгасва, когато устройството е в режим на готовност.
		1 #	Светодиодът мига, когато устройството е в режим на готовност. (неявно)

Важни бележки

1. Майсторската треска трябва да има 6-8 цифри.
2. Кодът “принуда” трябва да има 8 цифри. Първата цифра на кода трябва да бъде 1 за зона 1 и 2 за зона 2.
3. ПИН на потребителя трябва да има 4-6 цифри. Първата цифра на ПИН кода трябва да бъде 1 за зона 1 и 2 за зона 2.
4. User ID може да бъде произволно число между 1 и 2000.
5. Номерът на картата трябва да съдържа между 8 и 10 цифри. Ако номерът на картата съдържа по-малко от 8 цифри, добавете 0 пред кода.
6. Време за закъснение при отваряне на вратата: между 0 и 99 секунди. 0 = 50 mS
7. Когато потребителска карта е регистрирана в устройството, устройството автоматично ще генерира ПИН 1234, който не може да отключи вратата.
8. Ако бъде въведен невалиден главен ПИН, устройството влиза в режим на готовност след 5 секунди. Ако бъде въведен валиден главен ПИН, устройството влиза в режим на готовност след 30 секунди.
9. Когато използвате клавиатурата, натискането на клавиша # потвърждава предишно изпълнената клавишна команда. Когато добавяте или изтривате карти една след друга, натискането на клавиша # показва края на цикъла, а натискането на клавиша * показва изход от тази операция.
10. Когато добавяте карти последователно, устройството автоматично присвоява идентификационен номер и номер на карта. Идентификационният номер и номерът на картата се увеличават автоматично с всяка добавена карта, до максимум 2000.

11. Режимът на работа и форматът на предаване на клавиатурата се задават фабрично. Потребителят може да промени тези настройки според нуждите. След нулиране на устройството тази настройка остава непроменена.

12. След успешно регистриране на потребители в зона 1, светодиодът светва зелено. След успешно регистриране на потребители в зона 2, зеленият светодиод мига.

5. Операции с Mastercard

Добавяне на потребител за зона 1

Прочетете главната карта за добавяне, след това прочетете потребителските карти една след друга и накрая прочетете отново главната карта за добавяне.

Изтриване на потребител за зона 1

Прочетете основната карта за изтриване, след това прочетете картите на потребителя една след друга и накрая прочетете отново основната карта за изтриване.

6. Потребителски операции

С карта

Прочетете картата. Ключалката ще се отключи.

Ако сте задали няколко карти за отваряне на вратата (между 2 и 10), прочетете всички карти една след друга в рамките на 5 секунди, след което ключалката ще се отключи.

С карта + ПИН

Прочетете картата, въведете ПИН (4 или 6 цифри) +#. Ключалката ще се отключи.

С карта или ПИН

Прочетете картата. Ключалката ще се отключи. Или въведете ПИН +#. Ключалката ще се отключи.

Променете ПИН без да влизате в режим на програмиране

* прочетете картата на потребителя, въведете стар ПИН #, въведете нов ПИН # повторете нов ПИН

или

* Въведете ID номер # въведете стар ПИН #, въведете нов ПИН # повторете нов ПИН

Забележка: ПИН за зона 1 трябва да започва с 1, а ПИН за зона 2 трябва да започва с 2.

7. Функция за аларма

Аларма за подправяне

Ако устройството е разглобено чрез кражба с взлом, ще прозвучат вътрешният зумер и външната аларма (ако е свързана).

Аларма за отворена врата

Ако сте свързали кабелен сензор за врата към клавиатурата

за контрол на достъпа и този сензор ще се задейства, ще прозвучат вътрешният зумер и външната аларма (ако е свързана).

За да изключите алармата:

Прочетете потребителската или главната карта или въведете главния ПИН.

Ако не извършите никаква операция, алармата ще се изключи автоматично след 1 минута.

“Duress“ аларма

Ако картата „принуда“ бъде прочетена или ПИН кодът „принуда“ бъде въведен в зона 1 или зона 2, ключалката ще се отвори и в същото време ще се задейства външната аларма (ако е свързана). Вътрешният зумер няма да се задейства.

8. Режими на работа

Четец на карти Wiegand

В този режим клавиатурата функционира като четец на карти, свързан към устройство за контрол на достъпа.

Поддържани поръчки:

- Промяна на главния ПИН
- Задайте код на съоръжението
- Настройка на формата за предаване на картата
- Настройка на формата за предаване на клавиатурата
- Опционални настройки
- Аларма за подправяне

Самостоятелен контрол на достъпа за една врата

В този режим клавиатурата отваря една врата. Вратата може да се отвори с карта или ПИН или карта + ПИН. Клавиатурата поддържа свързване на външен четец на карти или бутон за достъп за излизане от сградата.

Самостоятелен контрол на достъпа за две врати

В този режим клавиатурата може да управлява две врати. Прочетете картата или въведете ПИН за зона 1 и вратата 1 ще се отвори. Прочетете картата или въведете ПИН кода за зона 2 и вратата 2 ще се отвори.

С външен четец на карти за отваряне на две врати

В този режим клавиатурата позволява достъп за врата 1, а външният четец на карти позволява достъп до врата 2. Прочетете картата или въведете кода за зона 1 на клавиатурата за контрол на достъпа. Врата 1 ще се отвори. Прочетете картата или въведете кода за зона 2 на външния четец на карти. Врата 2 ще се отвори.

Две взаимосвързани устройства за отваряне на две врати

Този режим е по-подходящ за места като банки, затвори или за ситуации, които изискват по-високо ниво на сигурност. Само след затваряне на врата 2, Прочетете картата или въведете кода на клавиатурата, за да отворите врата 1. И само след затваряне на врата 1, Прочетете картата или въведете кода на четеца на карти, за да отворите врата 2.

Анти-passback за една врата

При този режим на работа клавиатурата трябва да бъде монтирана на открито, за да позволи достъп вътре в сградата, а външният четец на карти трябва да бъде монтиран на закрито, за да позволи изход от сградата.

Ако влизането на потребителя в сградата не е регистрирано, потребителят не може да излезе, като прочете картата на четеца на карти. Също така, потребителят не може да влезе в сградата втори път, ако изходът му не е регистриран.

Забележка: Вратата може да се отвори само чрез прочитане на картата за зона 1. Всички останали режими за достъп до Зона 1 и Зона 2 са невалидни.

Анти-passback за две врати

В този режим клавиатурата на врата 1 е главен блок против обратно преминаване, а външният четец на карти на врата 2 е вторичният блок против обратно преминаване. Така се създава система против обратно преминаване, подходяща за монтаж на паркинги.

Потребителят може да влезе в сградата на врата 1, като прочете картата на клавиатурата за контрол на достъпа и може да излезе само на врата 2, като прочете картата на външния четец на карти. Ако влизането на потребителя не е регистрирано на врата 1, той няма да може да излезе на врата 2. Също така, потребителят не може да влезе втори път, ако изходът му не е регистриран.

Забележка: Вратата може да се отвори само чрез прочитане на картата за зона 1. Всички останали режими за достъп до Зона 1 и Зона 2 са невалидни.

Troubleshooting

проблем	Cause	Решение
Разстоянието за четене на картата е твърде кратко	Low card quality	Използвайте оригинални карти
Проблеми с настройката на ПИН	<ol style="list-style-type: none">1. ПИН не отговаря на стандарта2. Вие сте в режим на четене на карти, задайте паролата	<ol style="list-style-type: none">1. Първата цифра на ПИН трябва да бъде 1 или 2, според зоната.2. ПИН кодът не трябва да е 1234. ПИН трябва да е дълъг 4 или 6 цифри.
ПИН не отваря вратата	<ol style="list-style-type: none">1. Използвали сте ПИН 12342. Зададеният режим на достъп не позволява ПИН достъп	<ol style="list-style-type: none">1. Променете своя ПИН.2. Променете режима на достъп: карта или ПИН.
Няма отговор след прочитане на картата	Клавиатурата не е в режим на готовност, може да е в режим на програмиране	Натиснете клавиша *, светодиодът мига. Клавиатурата вече е в режим на готовност.

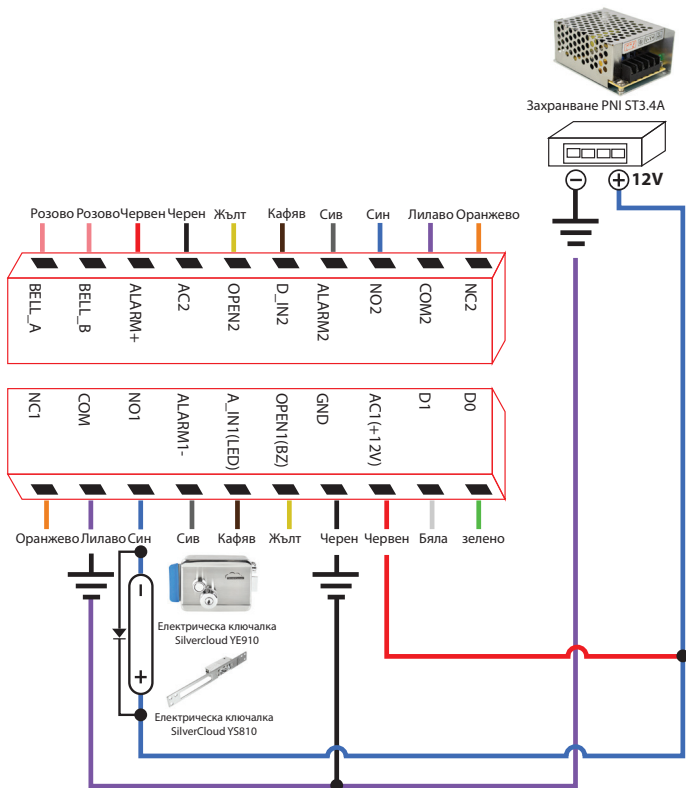
Клавиатурата не свети	Грешни настройки на клавиатурата	1. Включете или включете подсветката на клавиша. В автоматичен режим клавишите светват само след натискане и остават светещи за 30 секунди.
Невалидна Майсторска треска	Забравихте Майсторската треска	Нулирайте устройството. Майсторската треска се връща на 999999. При нулиране потребителските данни не се изтриват.

Нулирайте Майсторската треска

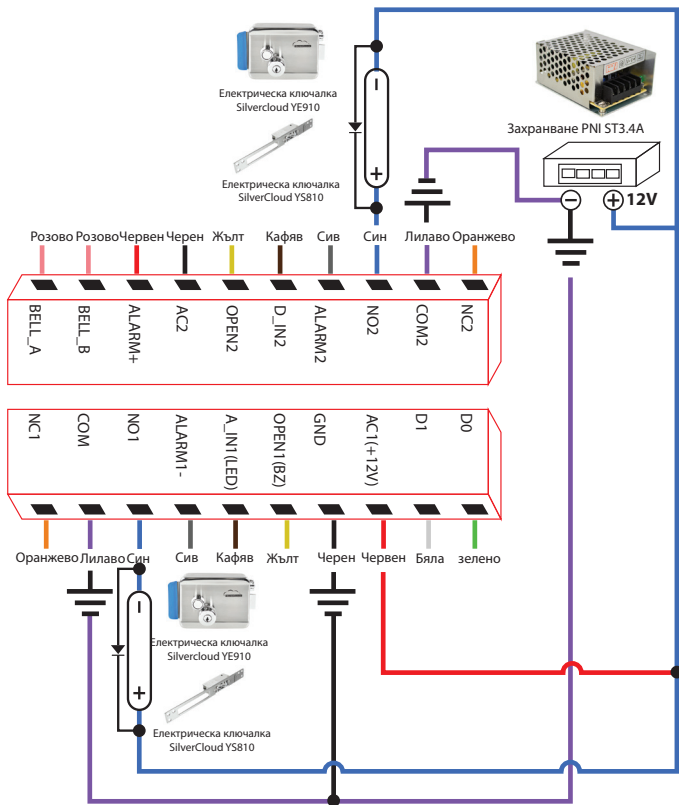
1. Изключете захранването на клавиатурата за контрол на достъпа.
2. Задръжте натиснат клавиш #, докато рестартирате захранването.
3. След като чуете два звука Di ., отпуснете клавиша #.
4. Клавиатурата се върна към фабричните настройки. Главната парола се връща на 999999. Потребителските данни не са изтрети.

Примери за свързване за една и две врати

Контрол на достъпа за една врата с електромагнитна бртва Silvercloud YE910 или Silvercloud YS810 и захранване PNI ST3.4A.



Контрол на достъпа за две врати с електромагнитна брава Silvercloud YE910 или Silvercloud YS810 и захранване PNI ST3.4A.



Beschreibung

PNI DK220 ist ein eigenständiges Zutrittskontrollgerät und Proximity-Leser. Es ist mit zwei Relais für die Zweitürsteuerung ausgestattet und unterstützt maximal 2000 Benutzer, jeder Benutzer kann einen PIN-Code und eine Zugangskarte haben.

Die Tastatur kann mit einem elektromagnetischen Schlüssel, einem Alarmsystem, einer Türklingel, einer Zugangstaste oder einem Türsensor verbunden werden.

Das Gerät verfügt über 7 Betriebsarten: Wiegand-Kartenleser, Zutrittskontrolle für eine Tür, Zutrittskontrolle für zwei Türen, Zutrittskontrolle mit externem Kartenleser für zwei Türen, zwei miteinander verbundene Einheiten für zwei Türen, Anti-Passback für eine Tür und zwei Türen Anti-Passback.

Haupteigenschaften

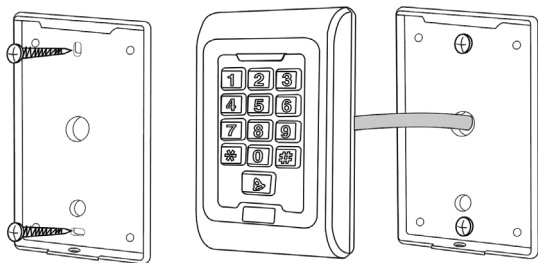
- Gehäuse aus Aluminiumlegierung mit IP65-Wasserbeständigkeitsklasse
- Eingebauter 125-kHz-Kartenleser
- Beleuchtete Zifferntasten. Das Tastenlicht kann wie folgt programmiert werden: Normal EIN, Normal AUS oder Mensch-Annäherung EIN (leuchtet auf, wenn es eine Bewegung erkennt).
- Sabotagealarm, Türsensor-Auslösealarm, Bedrohungscode-Alarm Dieser Code kann verwendet werden, wenn der Benutzer gezwungen ist, mit dem Öffnen der Tür zu drohen. Wenn Sie diesen Code eingeben, öffnet sich die Tür, aktiviert aber einen stillen Alarm).
- Hinzufügen und Löschen von Karten mit der Administratorkarte.
- Registrieren und Löschen von Benutzern nach Schlüssel.

Technische Spezifikationen

Versorgungsspannung	12V AC/DC
Standby-Verbrauch	<25mA
Ausgangslast des Elektroschlusses	<1A
Alarmausgangslast	<1A
Ausgangslast der Türklingel	<1A
Kartenleseabstand	maximal 40 mm
Benutzerkapazität	maximal 2000
Kompatible Karten	EM 125KHz/HID 125KHz
Kartenübertragungsformat	26-37-Bit-Wiegand
Übertragungsformat der Tastatur	4 Bit und 8 Bit und virtuelle Kartennummer
Arbeitstemperatur	-26°C ~ +80°C

Installation

Wählen Sie den Installationsort und bohren Sie Löcher in die Wand, die mit den Löchern in der Montagehalterung übereinstimmen. Befestigen Sie die Wandhalterung mit den im Lieferumfang enthaltenen Schrauben. Führen Sie die Kabel durch den Schlitz in der Mitte des Halters. Schließen Sie die Kabel an. Isolieren Sie nicht verwendete Kabel, um Kurzschlüsse zu vermeiden.



Verdrahtung

Zone 1		
BELL_A	Rosa	Klingeltaste
BELL_B	Rosa	Klingeltaste
ALARM+	Rot	Alarmanschluss
AC2	Schwarz	AC-EINGANG
OPEN2	Gelb	Exit-Taste
D_IN2	Braun	Türkontakt
ALARM2-	Grau	Alarm 2
NO2	Blau	RELAIS 2 NO
COM2	Violett	RELAIS 2 COM
NC2	Orange	RELAIS 2 NC

Zone 2

D0	Grün	Wiegand-Ausgang D0
D1	Weiß	Wiegand-Ausgang D1
AC1	Rot	AC1 (+ 12V)
GND	Schwarz	Masse
OPEN1(LED)	Gelb	Exit-Taste (für grüne LED)
D_IN1(BZ)	Braun	Türkontakt (für Summer)
ALARM1-	Grau	Alarm 1
NO1	Blau	RELAIS 1 NO
COM1	Violett	RELAIS 1 COM
NC1	Orange	RELAIS 1 NC

Akustische und leuchtende Warnungen

Status	LED	Buzzer
Bereithalten	Rot blinkt	
drücken Sie die Taste		Di
Karte lesen	Grün	Di.
Tür 1 offen	Grün	Di.
Tür 2 offen	Grün blinkt	Di.
Erfolgreicher Betrieb	Grün	Di.
Operation fehlgeschlagen		DiDiDi
PIN-Eingabe	Rot	
Karte & PIN lesen	Rot	
Mehrfaches Kartenlesen	Rot	
Unter Menü	Rot	
Unter Einstellungen	Orange	
Administratorkarte eingeben	Orange	DiDi
Beenden der Administratorkarte	Rot blinkt	Di.
Alarm	Rot blinkt schnell Alarm	Alarm

Kurzanleitung zur Programmierung

1. Administratoreinstellungen

* Hauptkennziffer #	00	<i>Geben Sie die neue Hauptkennziffer # ein Wiederholen Sie die neue Hauptkennziffer #</i>	Veränderung Hauptkennziffer. <i>Der Standard-Mastercode ist 999999. Der Mastercode muss zwischen 6 und 8 Stellen haben.</i>
	01	<i>Lesen Sie die Karte</i>	Masterkarten registrierung zum Hinzufügen von Karten. <i>Hinweis: Standard: Zone 1.</i>
	02	<i>Lesen Sie die Karte</i>	Masterkarten registrierung zum Löschen von Karten.
	03	<i>Lesen Sie die Karte</i>	Registrierung der Alarmkarte „Duess“ für Zone 1
	04	<i>Lesen Sie die Karte</i>	Registrierung der Alarmkarte „Duess“ für Zone 2

* Hauptkennziffer #	05	Geben Sie die 8-stellige PIN ein	Geben Sie den „duress“-PIN-Code für Zone1 ein Hinweis: Die erste Ziffer der PIN muss 1 für Zone 1 sein.
	06	Geben Sie die 8-stellige PIN ein	Geben Sie den „duress“-PIN-Code für Zone1 ein Hinweis: Die erste Ziffer der PIN muss 2 für Zone 2 sein.
	07	0000 #	Alle Benutzer löschen
	51	Master offen Schloss 1	
	52	Master offen Schloss 2	

Notiz:

Die „nöss“-PIN und die „nöss“-Karte können verwendet werden, wenn der Benutzer gezwungen ist, die Tür zu öffnen. Beim Eingeben dieses Codes oder Lesen dieser Karte öffnet sich die Tür, sendet aber gleichzeitig ein Alarmsignal.

2. Benutzereinstellungen für Zone 1 und Zone 2

Benutzerkarte hinzufügen

<i>* Hauptkennziffer #</i>	<i>11 (für Zone 1) 21 (für Zone 2)</i>	<i>Lesen Sie die Karte</i>
		<i>Eingabe-ID # Lesen Sie die Karte</i>
		<i>Kartenummer eingeben #</i>
		<i>Eingabe-ID # Kartenummer eingeben #</i>

Hinweis: Benutzer können nacheinander hinzugefügt werden, ohne den Programmiermodus zu verlassen. Die Benutzer-ID kann zwischen 1 und 4 Ziffern im Bereich 1 - 2000 enthalten. 1, 01, 001 und 0001 bedeuten alle 1.

Benutzer-PIN hinzufügen

<i>* Hauptkennziffer #</i>	<i>11 (für Zone 1) 21 (für Zone 2)</i>	<i>Eingabe-ID # PIN eingeben #</i>
------------------------------------	--	------------------------------------

Hinweis: Die PIN kann 4- bis 6-stellig sein. Die erste Ziffer muss 1 für Zone 1 und 2 für Zone 2 sein. „1234“ ist reserviert, kann nicht als PIN eingestellt werden.

Benutzer löschen

* Hauptkennziffer #	12 (für Zone 1)	Lesen Sie die Karte
	22 (für Zone 2)	Eingabe-ID #
		Kartenummer eingeben #

Hinweis: Benutzer können nacheinander gelöscht werden, ohne den Programmiermodus zu verlassen.

Alle Benutzer löschen

* Hauptkennziffer #	07	0000 #
---------------------------	----	--------

Hinweis: Dieser Befehl löscht alle Benutzer in Zone 1 und Zone 2.

Zugriffsmodi

* Hauptkennziffer #	13 (für Zone 1) 23 (für Zone 2)	0 #	Per Karte
		1 #	Per Karte + PIN
		2 #	Per Karte oder PIN (Voreinstellung)

Verzögerung Tür öffnen

<p>* Hauptkennziffer #</p>	<p>14 (für Zone 1) 24 (für Zone 2)</p>	<p>0 - 99 #</p>	<p>Voreinstellung 5</p>
------------------------------------	--	-----------------	-------------------------

Türschließmodi einstellen

<p>* Hauptkennziffer #</p>	<p>15 (für Zone 1)</p>	<p>0 #</p>	<p>Pulse mode (Voreinstellung). Each time a code is entered or a valid card has been read, the door will open and close automatically after the set time interval (between 0.05 sec. and 99 sec).</p>
	<p>25 (für Zone 2)</p>	<p>1 #</p>	<p>Modus umschalten. Jedes Mal, wenn ein Code eingegeben oder eine gültige Karte gelesen wurde, öffnet sich die Tür, schließt aber nicht, bis der Code erneut eingegeben oder die Karte gelesen wird.</p>

Open the door with several cards

<i>*</i> <i>Hauptkennziffer</i> <i>#</i>	<i>16</i> (für Zone 1) <i>26</i> (für Zone 2)	<i>1 - 10 #</i>	Voreinstellung 1
--	--	-----------------	------------------

Hinweis: Die Tür öffnet sich erst, nachdem alle Karten gelesen wurden. Zum Beispiel bei der Bestellung * Hauptkennziffer # 16 3 # müssen Sie 3 Karten hintereinander lesen, um die Tür zu öffnen. Diese Einstellung ist nur sinnvoll, wenn Sie die Tastatur auf den Kartenzugriffsmodus eingestellt haben.

Benutzerkarten in Serie hinzufügen

<i>*</i> <i>Hauptkennziffer</i> <i>#</i>	<i>17</i> (für Zone 1) <i>27</i> (für Zone 2)	<i>Eingabe-ID #, Kartenummer eingeben #, Eingabemenge #</i>
--	--	---

Hinweis: Kartennummern müssen fortlaufend sein (zwischen 8 und 10 Zeichen). Kartenanzahl liegt zwischen 1 und 2000.

3. Systemeinstellungen

* Hauptkennziffer #	30	0-15 #	Einstellen des Gerätecodes (Facility Code). Standard: 0
	31	0 #	Leser Wiegand
		1 #	Eintürige Stand-alone-Zutrittskontrolle (Voreinstellung)
		2 #	Eigenständige Zutrittskontrolle für zwei Türen
		3 #	Mit externem Leser für zwei Türen
		4 #	Zwei miteinander verbundene Einheiten für zwei Türen (Schutz beim Öffnen mehrerer Türen)

* Hauptkennziffer #	31	5 #	Anti-Passback für eine Tür
		6 #	Anti-Passback für zwei Türen
	32	26-37 #	Wiegand-Formateinstellung 26 34 37. Standard 26
	33	0-2 #	Einstellung des Tastaturübertragungsformats: 0 1 2 Nach dem Zurücksetzen bleibt diese Einstellung unverändert.

* Hauptkennziffer #	34	1-3 #	Weckdauer einstellen (Voreinstellung 1 Minute) Nach dem Zurücksetzen bleibt diese Einstellung unverändert
	35	0 #	Abgesicherter Modus 1. Normaler Modus. (Voreinstellung)
		1 #	Abgesicherter Modus 2. Wenn der falsche Code eingegeben oder eine ungültige Karte innerhalb von 10 Minuten 10 Mal hintereinander gelesen wird, schaltet das System als Sicherheitsvorkehrung ab.

* Hauptkennziffer #	35	2 #	Sicherheitsmodus 3. Alarmmodus. Wenn der falsche Code eingegeben oder eine ungültige Karte innerhalb von 10 Minuten 10 Mal hintereinander gelesen wird, werden vorsichtshalber der externe Alarm (sofern angeschlossen) und der in die Tastatur eingebaute Summer ausgelöst.
---------------------------	----	-----	---

4. Optionale Benutzereinstellungen

* Hauptkennziffer #	41	0 #	Summer aus. Der Summer bleibt nur aktiv, wenn das Gerät in den Programmiermodus wechselt.
		1 #	Aktiver Tastenton (Voreinstellung)
	42	0 #	Tastenbeleuchtung aus
		1 #	Tastenbeleuchtung an
		2 #	Automatischer Modus. Normalerweise ist die Tastenbeleuchtung ausgeschaltet, schaltet sich jedoch ein, wenn eine menschliche Anwesenheit erkannt wird

* Hauptkennziffer #	43	0 #	LED aus, wenn sich das Gerät im Standby befindet.
		1 #	Die LED blinkt, wenn sich das Gerät im Standby-Modus befindet. (Voreinstellung)

Wichtige Notizen

1. Der Mastercode muss 6-8 Stellen haben.
2. Der Code „Not“ muss 8-stellig sein. Die erste Ziffer des Codes muss 1 für Zone 1 und 2 für Zone 2 sein.

3. Die Benutzer-PIN muss 4-6 Ziffern haben. Die erste Ziffer der PIN muss 1 für Zone 1 und 2 für Zone 2 sein.
4. Die Benutzer-ID kann eine beliebige Zahl zwischen 1 und 2000 sein.
5. Die Kartenummer muss zwischen 8 und 10 Stellen haben. Wenn die Kartenummer weniger als 8 Ziffern enthält, fügen Sie vor dem Code eine 0 hinzu.
6. Verzögerungszeit Tür öffnen: zwischen 0 und 99 Sekunden. 0 = 50mS
7. Wenn eine Benutzerkarte im Gerät registriert ist, generiert das Gerät automatisch eine PIN 1234, die die Tür nicht entriegeln kann.
8. Bei Eingabe einer ungültigen Master-PIN geht das Gerät nach 5 Sekunden in den Standby-Modus. Bei Eingabe einer gültigen Master-PIN geht das Gerät nach 30 Sekunden in den Standby-Modus.
9. Bei Verwendung der Tastatur bestätigt das Drücken der #-Taste den zuvor ausgeführten Tastaturbefehl. Wenn Sie Karten nacheinander hinzufügen oder löschen, bedeutet das Drücken der Taste # das Ende des Zyklus und das Drücken der Taste * das Verlassen dieses Vorgangs.
10. Wenn Sie Karten in Serie hinzufügen, weist das Gerät automatisch eine ID-Nummer und eine Kartenummer zu. Die ID-Nummer und die Kartenummer erhöhen sich automatisch mit jeder hinzugefügten Karte, bis maximal 2000.
11. Die Betriebsart und das Übertragungsformat der Tastatur sind werkseitig eingestellt. Der Benutzer kann diese Einstellungen nach Bedarf ändern. Nach dem Zurücksetzen des Geräts bleibt diese Einstellung unverändert.
12. Nach erfolgreicher Registrierung von Benutzern in Zone 1 wird die LED grün. Nach erfolgreicher Registrierung von Benutzern in

Zone 2 blinkt die grüne LED.

5. Mastercard-Betrieb

Benutzer hinzufügen für Zone 1

Lesen Sie die Master-Add-Karte, dann die Benutzerkarten nacheinander lesen und schließlich die Master-Add-Karte erneut lesen.

Benutzer löschen für Zone 1

Lesen Sie die Master-Delete-Karte, dann die Benutzerkarten nacheinander lesen und schließlich die Master-Delete-Karte erneut lesen.

6. Benutzervorgänge

Per Karte

Lesen Sie die Karte. Das Schloss wird entriegelt.
Wenn Sie mehrere Karten für die Türöffnung eingestellt haben (zwischen 2 und 10), lesen Sie alle Karten nacheinander innerhalb von 5 Sekunden, danach wird das Schloss entriegelt.

Per Karte + PIN

Lesen Sie die Karte, geben Sie die PIN (4- oder 6-stellig) +# ein.
Das Schloss wird entriegelt.

Per Karte or PIN

Lesen Sie die Karte. Das Schloss wird entriegelt. Oder geben Sie die PIN +# ein. Das Schloss wird entriegelt.

PIN ändern, ohne in den Programmiermodus zu gelangen

** Benutzerkarte lesen, alte PIN eingeben, neue PIN eingeben # neue PIN wiederholen*

oder

** ID-Nummer eingeben # alte PIN eingeben #, neue PIN eingeben # neue PIN wiederholen*

Hinweis: Die PIN für Zone 1 muss mit 1 beginnen und die PIN für Zone 2 muss mit 2 beginnen.

7. Alarmfunktion

Sabotagealarm

Wird das Gerät durch Einbruch zerlegt, ertönt der interne Summer und der externe Alarm (sofern angeschlossen).

Alarm bei offener Tür

Wenn Sie einen kabelgebundenen Türsensor an die Zutrittskontrolltastatur angeschlossen haben und dieser Sensor ausgelöst wird, ertönen der interne Summer und der externe Alarm (sofern angeschlossen).

Um den Wecker auszuschalten:

Lesen Sie die Benutzerkarte oder Masterkarte oder geben Sie die Master-PIN ein.

Wenn Sie keinen Vorgang ausführen, wird der Alarm nach 1 Minute automatisch ausgeschaltet.

“Duress“ alarm

Wird die „duress“-Karte gelesen oder der „duress“-PIN-Code in Zone 1 oder Zone 2 eingegeben, öffnet sich das Schloss und gleichzeitig wird der externe Alarm ausgelöst (sofern angeschlossen). Der interne Summer wird nicht ausgelöst.

8. Betriebsarten

Wiegand-Kartenleser

In diesem Modus fungiert die Tastatur als Kartenleser, der mit einem Zugangskontrollgerät verbunden ist.

Unterstützte Bestellungen:

- Master-PIN ändern
- Einrichtungscode einstellen
- Einstellung des Kartenübertragungsformats
- Einstellung des Übertragungsformats der Tastatur
- Optionale Einstellungen
- Sabotagealarm

Eigenständige Zutrittskontrolle für eine einzelne Tür

In diesem Modus öffnet die Tastatur eine einzelne Tür. Die Tür kann per Karte oder PIN oder Karte + PIN geöffnet werden. Die Tastatur unterstützt den Anschluss eines externen Kartenlesers oder einer Zutrittstaste zum Verlassen des Gebäudes.

Eigenständige Zutrittskontrolle für zwei Türen

In diesem Modus kann die Tastatur zwei Türen steuern. Lesen Sie die Karte oder geben Sie die PIN für Zone 1 ein und Tür 1 öffnet sich.

Lesen Sie die Karte oder geben Sie den PIN-Code für Zone 2 ein und Tür 2 öffnet sich.

Mit externem Kartenleser zum Öffnen von zwei Türen

In diesem Modus ermöglicht die Tastatur den Zugang für Tür 1, und der externe Kartenleser ermöglicht den Zugang für Tür 2.

Lesen Sie die Karte oder geben Sie den Code für Zone 1 über die Zutrittskontrolltastatur ein. Tür 1 wird geöffnet. Lesen Sie die Karte oder geben Sie den Code für Zone 2 am externen Kartenleser ein. Tür 2 wird geöffnet.

Zwei miteinander verbundene Geräte zum Öffnen von zwei Türen

Dieser Modus eignet sich eher für Orte wie Banken, Gefängnisse oder für Situationen, die ein höheres Sicherheitsniveau erfordern.

Lesen Sie die Karte erst nach dem Schließen der Tür 2 oder geben Sie den Code über die Tastatur ein, um die Tür 1 zu öffnen. Und erst nachdem die Tür 1 geschlossen ist, lesen Sie die Karte oder geben Sie den Code am Kartenleser ein, um die Tür 2 zu öffnen.

Anti-Passback für eine einzelne Tür

In dieser Betriebsart muss die Tastatur im Freien installiert werden, um den Zugang innerhalb des Gebäudes zu ermöglichen, und der externe Kartenleser muss im Innenbereich montiert werden, um den Ausgang aus dem Gebäude zu ermöglichen.

Wenn der Zutritt des Benutzers in das Gebäude nicht registriert wurde, kann der Benutzer das Gebäude nicht durch Lesen der Karte am Kartenleser verlassen. Außerdem kann der Benutzer das Gebäude nicht ein zweites Mal betreten, wenn sein Ausgang nicht registriert wurde.

Hinweis: Die Tür kann nur durch Auslesen der Karte für Zone 1 geöffnet werden. Alle anderen Zutrittsmodi für Zone 1 und Zone 2 sind ungültig.

Anti-Passback für zwei Türen

In diesem Modus ist die Tastatur an Tür 1 die Anti-Passback-Master-Einheit und der externe Kartenleser an Tür 2 ist die sekundäre Anti-Passback-Einheit. Somit wird ein für die Installation auf Parkplätzen geeignetes Anti-Passback-System geschaffen.

Der Benutzer kann das Gebäude an Tür 1 betreten, indem er die Karte auf der Zutrittskontrolltastatur liest, und kann das Gebäude nur an Tür 2 verlassen, indem er die Karte auf dem externen Kartenleser liest. Wenn der Eingang des Benutzers nicht an Tür 1 registriert wurde, kann er an Tür 2 nicht austreten. Außerdem kann der Benutzer kein zweites Mal eintreten, wenn sein Ausgang nicht registriert wurde.

Hinweis: Die Tür kann nur durch Auslesen der Karte für Zone 1 geöffnet werden. Alle anderen Zutrittsmodi für Zone 1 und Zone 2 sind ungültig.

Fehlerbehebung

Problem	Weil	Lösung
Kartenleseabstand zu kurz	Niedrige Kartenqualität	Originalkarten verwenden
Probleme mit der PIN-Einstellung	1. Die PIN entspricht nicht dem Standard 2. Sie befinden sich im Kartenlesemodus, legen Sie das Passwort fest	1. Die erste Ziffer der PIN muss je nach Zone 1 oder 2 sein. 2. Die PIN darf nicht 1234 sein. Die PIN muss 4 oder 6 Stellen lang sein.
Die PIN öffnet die Tür nicht	1. Sie haben PIN 1234 verwendet 2. Der eingestellte Zugriffsmodus lässt keinen PIN-Zugriff zu	1. Ändern Sie Ihre PIN. 2. Ändern Sie den Zugangsmodus: Karte oder PIN.
Keine Antwort nach dem Lesen der Karte	Die Tastatur befindet sich nicht im Standby, sie kann sich im Programmiermodus befinden	Drücken Sie die *-Taste, die LED blinkt. Die Tastatur befindet sich jetzt im Standby-Modus.

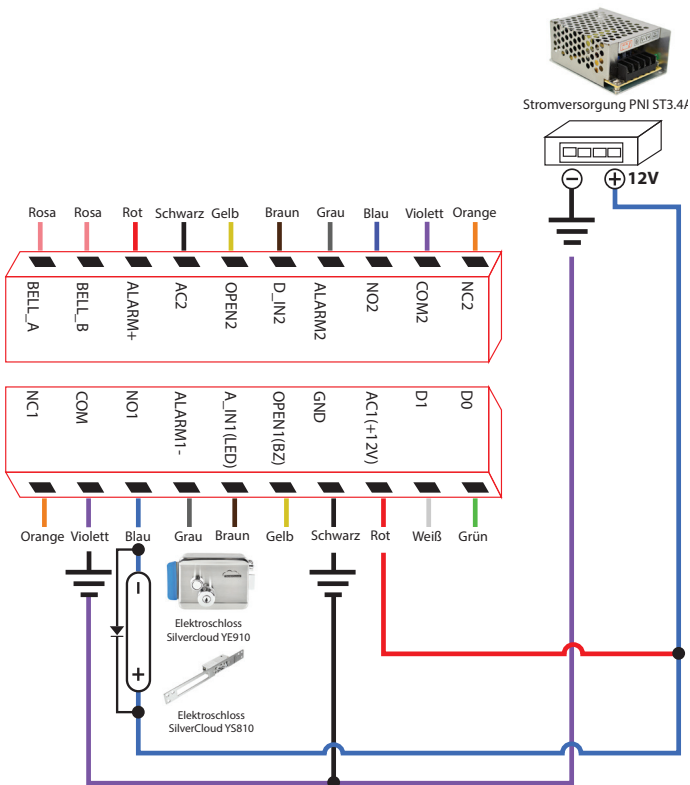
Die Tastatur leuchtet nicht	Falsche Tastatureinstellungen	1. Stellen Sie die Tastenbeleuchtung ein oder ein. Im Auto-Modus leuchten die Tasten erst nach dem Drücken auf und leuchten 30 Sekunden lang.
Ungültiger Mastercode	Du hast den Mastercode vergessen	Setzen Sie das Gerät zurück. Der Mastercode kehrt auf 999999 zurück. Durch Reset werden die Benutzerdaten nicht gelöscht.

Mastercode zurücksetzen

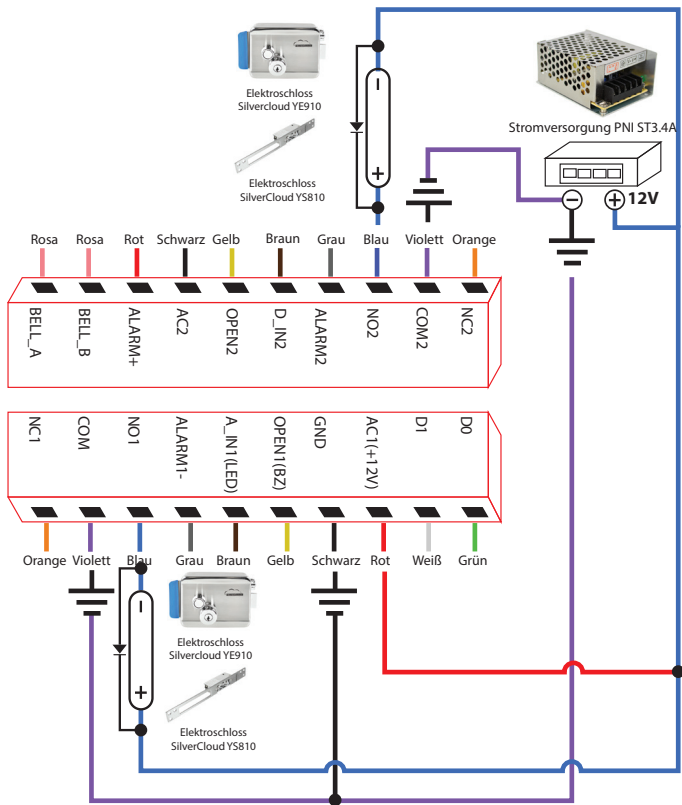
1. Schalten Sie die Stromversorgung der Zugangskontrolltastatur aus.
2. Halten Sie die #-Taste gedrückt, während Sie das Gerät neu starten.
3. Lassen Sie die #-Taste los, nachdem Sie zwei Di.-Klänge gehört haben.
4. Die Tastatur ist auf die Werkseinstellungen zurückgesetzt. Das Master-Passwort wird auf 999999 zurückgesetzt. Die Benutzerdaten wurden nicht gelöscht.

Anschlussbeispiele für eine und zwei Türen

Zutrittskontrolle für eine Tür mit elektromagnetischem Schloss Silvercloud YE910 oder Silvercloud YS810 und Netzteil PNI ST3.4A.



Zutrittskontrolle für zwei Türen mit elektromagnetischem Schloss Silvercloud YE910 oder Silvercloud YS810 und Netzteil PNI ST3.4A



Descripción

PNI DK220 es un dispositivo de control de acceso independiente y un lector de proximidad. Está equipado con dos relés para control de dos puertas y admite un máximo de 2000 usuarios, cada usuario puede tener un código PIN y una tarjeta de acceso.

El teclado se puede conectar a una llave electromagnética, un sistema de alarma, un timbre, un botón de acceso o un sensor de puerta.

El dispositivo tiene 7 modos de funcionamiento: lector de tarjetas Wiegand, control de acceso para una puerta, control de acceso para dos puertas, control de acceso con lector de tarjeta externo para dos puertas, dos unidades interconectadas para dos puertas, anti-passback para una puerta y dos puertas. anti-passback.

Principales características

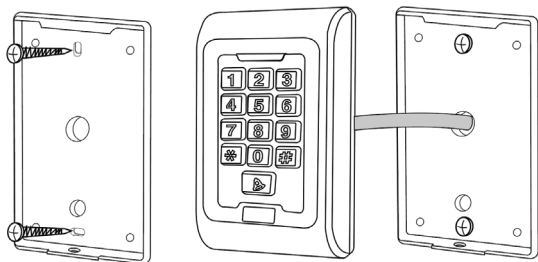
- Carcasa de aleación de aluminio con clase de resistencia al agua IP65
- Lector de tarjetas integrado de 125 KHz
- Teclas numéricas iluminadas. La luz de la tecla se puede programar de la siguiente manera: Normal ON, Normal OFF o Human-Approach ON (se enciende cuando detecta movimiento).
- Alarma de manipulación, alarma de activación del sensor de puerta, alarma de código de coacción Este código se puede utilizar cuando el usuario se ve obligado a amenazar con abrir la puerta. Al escribir este código, la puerta se abrirá pero activará una alarma silenciosa).
- Agregue y elimine tarjetas con la tarjeta de administrador.
- Registrar y eliminar usuarios por claves.

Especificaciones técnicas

Tensión de alimentación	12V AC/DC
Consumo en espera	<25mA
Carga de salida de cerradura eléctrica	<1A
Carga de salida de alarma	<1A
Carga de salida del timbre	<1A
Distancia de lectura de la tarjeta	máximo 40 mm
Capacidad de usuario	máximo 2000
Tarjetas compatibles	EM 125Khz/HID 125KHz
Formato de transmisión de la tarjeta	Wiegand de 26-37 bits
Formato de transmisión del teclado	4 bits y 8 bits y número de tarjeta virtual
Temperatura de trabajo	-26°C ~ +80°C

Instalación

Elija la ubicación de instalación y haga orificios en la pared que coincidan con los orificios del soporte de montaje. Asegure el soporte de pared con los tornillos incluidos en el paquete. Pase los cables a través de la ranura en el medio del soporte. Conecta los cables. Aísle los cables no utilizados para evitar cortocircuitos.



Alambrado

Zona 1		
BELL_A	Rosa	Botón de timbre
BELL_B	Rosa	Botón de timbre
ALARM+	Rojo	Conector de alarma
AC2	Negro	ENTRADA AC
OPEN2	Amarillo	Botón de salida
D_IN2	Marrón	Contacto de puerta
ALARM2-	Gris	Alarma 2
NO2	Azul	Relé 2 NO
COM2	Púrpura	RELÉ 2 COM
NC2	Naranja	RELÉ 2 NC

Zona 2

D0	Verde	Salida Wiegand D0
D1	Blanco	Salida Wiegand D1
AC1	Rojo	AC1 (+ 12V)
GND	Negro	GND
OPEN1(LED)	Amarillo	Botón de salida (para LED verde)
D_IN1(BZ)	Marrón	Contacto de puerta (para zumbador)
ALARM1-	Gris	Alarma 1
NO1	Azul	Relé 2 NO
COM1	Púrpura	RELÉ 2 COM
NC1	Naranja	RELÉ 2 NC

Avisos sonoros y luminosos

Estado	LED	Buzzer
Apoyar	Parpadea en rojo	
Presione la tecla		Di
Leer tarjeta	Verde	Di.
Puerta 1 abierta	Verde	Di.
Puerta 2 abierta	El verde parpadea	Di.
Operación exitosa	Verde	Di.
Operación fallida		DiDiDi
Entrada de PIN	rojo	
Leer tarjeta y PIN	rojo	
Lectura de múltiples tarjetas	rojo	
Bajo el menú	rojo	
En configuración	naranja	
Ingresar tarjeta de administrador	naranja	DiDi
Salida de la tarjeta de administrador	Parpadea en rojo	Di.
Alarma	El rojo parpadea rápidamente	Alarma

Guía de programación rápida

1. Configuración de administrador

* Código master #	00	<i>Ingrese el nuevo maestro Código # Repita el nuevo maestro Código #</i>	Cambio Código master. <i>Nota: El maestro Código predeterminado es 999999. El maestro Código debe tener entre 6 y 8 dígitos.</i>
	01	<i>Leer la tarjeta</i>	Registro de tarjeta maestra para agregar tarjetas. <i>Nota: Predeterminado: zona 1.</i>
	02	<i>Leer la tarjeta</i>	Registro de tarjeta maestra eliminar tarjetas. <i>Nota: Predeterminado: zona 1</i>
	03	<i>Leer la tarjeta</i>	Registro de la tarjeta de alarma “duress” para la zona 1
	04	<i>Leer la tarjeta</i>	Registro de la tarjeta de alarma “duress” para la zona 2

* Código master #	05	<i>Ingrese el PIN de 8 dígitos</i>	Ingrese el código PIN de “duress” para zone1 Nota: El primer dígito del PIN debe ser 1 para la zona 1.
	06	<i>Ingrese el PIN de 8 dígitos</i>	Ingrese el código PIN de “duress” para zone2 Nota: El primer dígito del PIN debe ser 2 para la zona 2.
	07	<i>0000 #</i>	Eliminar todos los usuarios
	51	Administrador abre cerradura 1	
	52	Administrador abre cerradura 1	

Nota:

El PIN de “coacción” y la tarjeta de “coacción” se pueden utilizar cuando el usuario se ve obligado a abrir la puerta. Al escribir este código o leer esta tarjeta, la puerta se abrirá pero al mismo tiempo enviará una señal de alarma.

2. Configuración de usuario para Zona 1 y Zona 2

Agregar tarjeta de usuario

<i>* Código master #</i>	11 (para la Zona 1) 21 (para la Zona 2)	<i>Leer la tarjeta</i>
		<i>Introduzca el ID # Leer la tarjeta</i>
		<i>Introduzca el número de tarjeta#</i>
		<i>Introduzca el ID # Introduzca el número de tarjeta #</i>

Nota: Los usuarios se pueden agregar uno tras otro sin salir del modo de programación. El ID de usuario puede contener entre 1 y 4 dígitos, en el rango de 1 a 2000. 1, 01, 001 y 0001 todos significan 1.

Agregar PIN de usuario

<i>* Código master #</i>	11 (para la Zona 1) 21 (para la Zona 2)	<i>Introduzca el ID # Introduzca el PIN #</i>
--------------------------	--	---

Nota: El PIN puede tener de 4 a 6 dígitos. El primer dígito debe ser 1 para la Zona 1 y 2 para la Zona 2. “1234” está reservado, no se puede configurar como PIN.

Borrar usuario

<i>* Código master #</i>	12 (para la Zona 1)	<i>Leer la tarjeta</i>
	22 (para la Zona 2)	<i>Introduzca el ID #</i>
		<i>Introduzca el número de tarjeta #</i>

Nota: Los usuarios pueden eliminarse uno tras otro sin salir del modo de programación.

Eliminar todos los usuarios

<i>* Código master #</i>	07	0000 #
--------------------------	----	--------

Nota: este comando elimina a todos los usuarios en la Zona 1 y la Zona 2.

Modos de acceso

<i>* Código master #</i>	13 (para la Zona 1)	0 #	Por tarjeta
	23 (para la Zona 2)	1 #	Por tarjeta + PIN
		2 #	Por tarjeta o PIN (Predeterminado)

Retraso de puerta abierta

* <i>Codigo master</i> #	14 (para la Zona 1) 24 (para la Zona 2)	0 - 99 #	Predeterminado 5
-----------------------------	--	----------	------------------

Establecer modos de cierre de puertas

* <i>Codigo master</i> #	15 (para la Zona 1) 25 (para la Zona 2)	0 #	Modo pulso (Predeterminado). Cada vez que se ingresa un código o se lee una tarjeta válida, la puerta se abrirá y cerrará automáticamente después del intervalo de tiempo establecido (entre 0.05 seg. Y 99 seg.).
		1 #	Alternar modo. Cada vez que se ingresa un código o se lee una tarjeta válida, la puerta se abre pero no se cierra hasta que se ingresa nuevamente el código o se lee la tarjeta.

Abre la puerta con varias cartas.

* <i>Codigo master</i> #	16 (para la Zona 1) 26 (para la Zona 2)	1 - 10 #	Predeterminado 1
-----------------------------	--	----------	------------------

Nota: La puerta solo se abrirá después de que se hayan leído todas las tarjetas. Por ejemplo, por pedido * Codigo master # 16 3 #, tienes que leer 3 cartas seguidas para abrir la puerta. Esta configuración solo es útil si ha configurado el teclado en el modo de acceso de tarjeta.

Agregar tarjetas de usuario en serie

* <i>Codigo master</i> #	17 (para la Zona 1) 27 (para la Zona 2)	<i>Introduzca el ID #, Introduzca el número de tarjeta #, Introduzca la cantidad #</i>
-----------------------------	--	--

Nota: Los números de las tarjetas deben ser consecutivos (entre 8 y 10 caracteres). La cantidad de tarjetas está entre 1 y 2000.

3. Ajustes del sistema

<i>* Código master #</i>	30	0-15 #	Configuración del código de la unidad (Código de instalación). Predeterminado: 0
	31	0 #	Lector Wiegand
		1 #	Control de acceso autónomo de una puerta (Predeterminado)
		2 #	Control de acceso autónomo para dos puertas
		3 #	Con lector externo para dos puertas
		4 #	Dos unidades interconectadas para dos puertas (protección al abrir varias puertas)

* Código master #	31	5 #	Anti-passback para una puerta
		6 #	Anti-passback para dos puertas
	32	26-37 #	Configuración de formato Wiegand 26 34 37. Predeterminado 26
	33	0-2 #	Configuración del formato de transmisión del teclado: 0 1 2 Después de restablecer, esta configuración se mantiene sin cambios.

* Código master #	34	1-3 #	Establecer la duración de la alarma (Predeterminado 1 minuto) Después de restablecer, esta configuración se mantiene sin cambios.
			0 #
	35	1 #	Modo seguro 2. Si se ingresa el código incorrecto o se lee una tarjeta no válida 10 veces seguidas en 10 minutos, como medida de seguridad, el sistema se apaga.

* <i>Código master</i> #	35	2 #	<p>Modo de seguridad 3. Modo de alarma.</p> <p>Si se ingresa el código incorrecto o se lee una tarjeta inválida 10 veces seguidas en 10 minutos, como precaución, se activará la alarma externa (si está conectada) y el zumbador integrado en el teclado.</p>
-----------------------------	----	-----	--

4. Configuración de usuario opcional

* <i>Código master</i> #	41	0 #	<p>Zumbador apagado.</p> <p>El zumbador permanece activo solo cuando el dispositivo ingresa al modo de programación.</p>
		1 #	<p>Sonido de tecla activa (Predeterminado)</p>
	42	0 #	<p>Luz de fondo de tecla apagada</p>
		1 #	<p>Luz de fondo de tecla encendida</p>
		2 #	<p>Modo automático. Normalmente, la luz de la tecla está apagada pero se enciende cuando se detecta la presencia humana.</p>

* <i>Código master</i> #	43	0 #	LED apagado cuando el dispositivo está en espera.
		1 #	El LED parpadea cuando el dispositivo está en modo de espera. (Predeterminado)

Notas importantes

1. El maestro Código debe tener 6-8 dígitos.
2. El código “coacción” debe tener 8 dígitos. El primer dígito del código debe ser 1 para la Zona 1 y 2 para la Zona 2.
3. El PIN de usuario debe tener entre 4 y 6 dígitos. El primer dígito del PIN debe ser 1 para la Zona 1 y 2 para la Zona 2.
4. La identificación de usuario puede ser cualquier número entre 1 y 2000.
5. El número de la tarjeta debe tener entre 8 y 10 dígitos. Si el número de la tarjeta contiene menos de 8 dígitos, agregue 0 delante del código.
6. Tiempo de retardo de puerta abierta: entre 0 y 99 segundos. 0 = 50 mS
7. Cuando se registra una tarjeta de usuario en el dispositivo, el dispositivo generará automáticamente un PIN 1234 que no puede desbloquear la puerta.
8. Si se ingresa un PIN maestro no válido, el dispositivo entra en modo de espera después de 5 segundos. Si se ingresa un PIN maestro válido, el dispositivo ingresa al modo de espera después de 30 segundos.
9. Al usar el teclado, presionar la tecla # confirma el comando de teclado ejecutado previamente. Al agregar o eliminar tarjetas una

tras otra, presionar la tecla # indica el final del ciclo, y presionar la tecla * indica salir de esta operación.

10. Cuando agrega tarjetas en serie, el dispositivo asigna automáticamente un número de identificación y un número de tarjeta. El número de identificación y el número de tarjeta aumentan automáticamente con cada tarjeta agregada, hasta un máximo de 2000.

11. El modo de funcionamiento y el formato de transmisión del teclado vienen configurados de fábrica. El usuario puede cambiar esta configuración según sea necesario. Después de reiniciar el dispositivo, esta configuración permanece sin cambios.

12. Después de registrar correctamente a los usuarios en la Zona 1, el LED se ilumina en verde. Después de registrar con éxito a los usuarios en la Zona 2, el LED verde parpadea.

5. Operaciones con tarjeta maestra

Agregar usuario para la Zona 1

Lea la tarjeta de adición maestra, luego lea las tarjetas de usuario una tras otra y, finalmente, lea la tarjeta de adición maestra nuevamente.

Eliminar usuario para la Zona 1

Lea la tarjeta de eliminación maestra, luego lea las tarjetas de usuario una tras otra y, finalmente, lea la tarjeta de eliminación maestra nuevamente.

6. Operaciones de usuario

Por tarjeta

Leer la tarjeta. La cerradura se desbloqueará.

Si ha configurado varias tarjetas para la apertura de la puerta (entre 2 y 10), lea todas las tarjetas una tras otra en 5 segundos, después de lo cual se desbloqueará la cerradura.

Por tarjeta + PIN

Leer la tarjeta, ingrese el PIN (4 o 6 dígitos) + #. La cerradura se desbloqueará.

Por tarjeta o PIN

Leer la tarjeta. La cerradura se desbloqueará. ingrese el PIN + #. La cerradura se desbloqueará.

Cambiar PIN sin ingresar al modo de programación

** leer la tarjeta de usuario, ingresar el PIN antiguo #, ingresar el nuevo PIN # repetir el nuevo PIN*

o

** Ingrese el número de ID # ingrese el PIN antiguo #, ingrese el nuevo PIN # repita el nuevo PIN*

Nota: El PIN para la Zona 1 debe comenzar con 1 y el PIN para la Zona 2 debe comenzar con 2.

7. Función de alarma

Alarma de sabotaje

Si el dispositivo se desmonta por robo, sonarán el zumbador interno y la alarma externa (si está conectada).

Alarma de puerta abierta

Si ha conectado un sensor de puerta con cable al teclado de control de acceso y este sensor se activará, sonarán el zumbador interno y la alarma externa (si está conectada).

Para apagar la alarma:

Lea la tarjeta de usuario o la tarjeta maestra, o ingrese el PIN maestro.

Si no realiza ninguna operación, la alarma se apagará automáticamente después de 1 minuto.

Alarma “Duress“

Si se lee la tarjeta de “coacción” o se ingresa el código PIN de “coacción” en la Zona 1 o la Zona 2, la cerradura se abrirá y, al mismo tiempo, se activará la alarma externa (si está conectada). El zumbador interno no se activará.

8. Modos de funcionamiento

Lector de tarjetas Wiegand

En este modo, el teclado funciona como un lector de tarjetas conectado a un dispositivo de control de acceso.

Órdenes admitidas:

- Cambiar PIN maestro

- Establecer código de instalación
- Configuración del formato de transmisión de la tarjeta
- Configuración del formato de transmisión del teclado
- Configuraciones opcionales
- Alarma de sabotaje

Control de acceso autónomo para una sola puerta

En este modo, el teclado abre una sola puerta. La puerta se puede abrir Por tarjeta o PIN o tarjeta + PIN. El teclado admite la conexión de un lector de tarjetas externo o un botón de acceso para salir del edificio.

Control de acceso autónomo para dos puertas

En este modo, el teclado puede controlar dos puertas. Lea la tarjeta o ingrese el PIN para la Zona 1 y la puerta 1 se abrirá. Lea la tarjeta o ingrese el código PIN para la Zona 2 y la puerta 2 se abrirá.

Con lector de tarjetas externo para abrir dos puertas

En este modo, el teclado permite el acceso a la puerta 1 y el lector de tarjetas externo permite el acceso a la puerta 2.

Leer la tarjeta o ingresar el código para la Zona 1 en el teclado de control de acceso. La puerta 1 se abrirá. Leer la tarjeta o ingresar el código para la Zona 2 en el lector de tarjetas externo. La puerta 2 se abrirá.

Dos dispositivos interconectados para abrir dos puertas.

Este modo es más adecuado para ubicaciones como bancos, cárceles o para situaciones que requieren un nivel avanzado de seguridad.

Solo después de que la puerta 2 esté cerrada, lea la tarjeta o ingrese el código en el teclado para abrir la puerta 1. Y solo después de que la puerta 1 esté cerrada, lea la tarjeta o ingrese el código en el lector de tarjetas para abrir la puerta 2.

Anti-passback para una sola puerta

En este modo de funcionamiento, el teclado debe instalarse en el exterior para permitir el acceso al interior del edificio, y el lector de tarjetas externo debe montarse en el interior para permitir la salida del edificio.

Si no se ha registrado la entrada del usuario al edificio, el usuario no puede salir leyendo la tarjeta en el lector de tarjetas. Además, el usuario no puede entrar al edificio por segunda vez si su salida no ha sido registrada.

Nota: La puerta solo se puede abrir leyendo la tarjeta para la Zona 1. Todos los demás modos de acceso de la Zona 1 y la Zona 2 no son válidos.

Anti-passback para dos puertas

En este modo, el teclado en la puerta 1 es la unidad maestra anti-passback y el lector de tarjetas externo en la puerta 2 es la unidad anti-passback secundaria. Así, se crea un sistema anti-passback apto para su instalación en aparcamientos.

El usuario puede ingresar al edificio por la puerta 1 leyendo la tarjeta en el teclado de control de acceso y solo puede salir por la puerta 2 leyendo la tarjeta en el lector de tarjetas externo. Si la entrada del usuario no ha sido registrada en la puerta 1, no podrá salir por la puerta 2. Además, el usuario no puede entrar por segunda vez si su salida no ha sido registrada.

Nota: La puerta solo se puede abrir leyendo la tarjeta para la Zona

1. Todos los demás modos de acceso de la Zona 1 y la Zona 2 no son válidos.

Solución de problemas

Problema	Causa	Solución
Distancia de lectura de la tarjeta demasiado corta	Tarjeta de baja calidad	Usa tarjetas originales
Problemas de configuración de PIN	<ol style="list-style-type: none">1. El PIN no cumple con el estándar2. Está en modo de lectura de tarjetas, configure la contraseña	<ol style="list-style-type: none">1. El primer dígito del PIN debe ser 1 o 2, según la Zona.2. El PIN no debe ser 1234. El PIN debe tener 4 o 6 dígitos.
The PIN does not open the door	<ol style="list-style-type: none">1. Ha utilizado el PIN 12342. El modo de acceso configurado no permite el acceso con PIN	<ol style="list-style-type: none">1. Cambie su PIN.2. Cambiar el modo de acceso: tarjeta o PIN.
No answer after reading the card	El teclado no está en espera, puede estar en modo de programación	Presione la tecla *, el LED parpadea. El teclado ahora está en modo de espera.

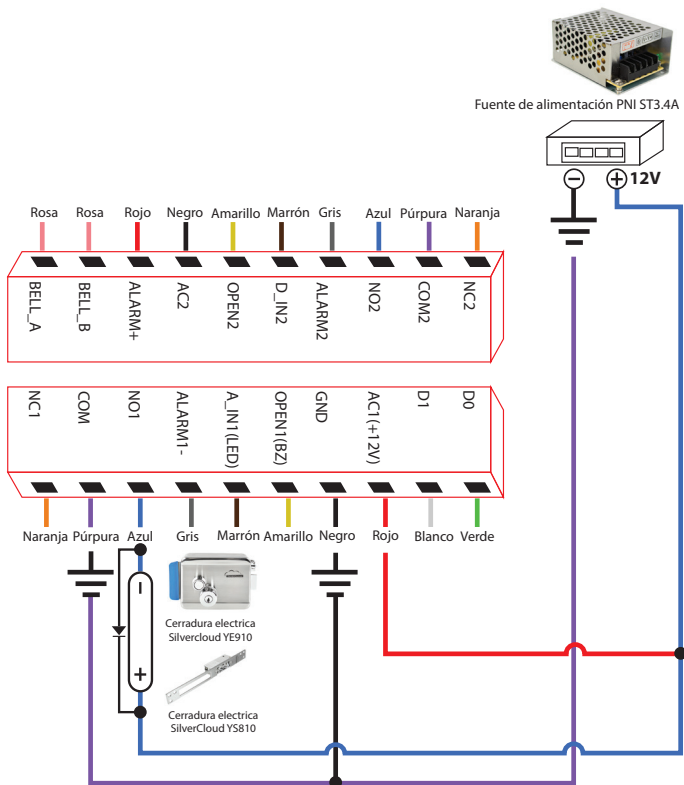
El teclado no se enciende	Configuración incorrecta del teclado	1. Encienda o encienda la luz de fondo de la tecla. En el modo automático, las teclas solo se iluminan después de presionarlas y permanecen encendidas durante 30 segundos.
Codigo master no válido	Te olvidaste del Codigo master	Reinicia el dispositivo. El maestro Codigo vuelve a 999999. Al reiniciar, los datos del usuario no se eliminan.

Restablecer el Codigo master

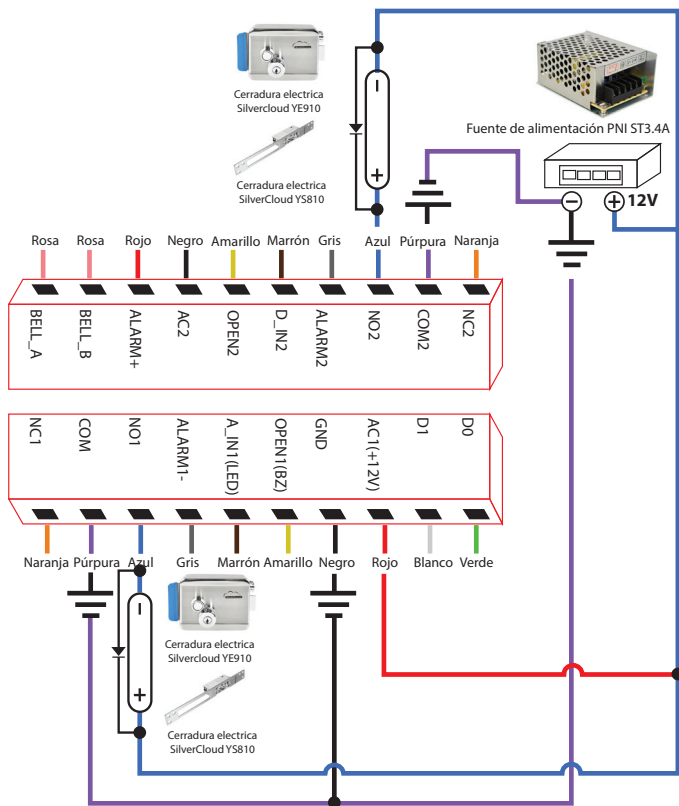
- Apague la alimentación del teclado de control de acceso.
- Mantenga presionada la tecla # mientras reinicia la energía.
- Después de escuchar dos sonidos Di ., suelte la tecla #.
- El teclado ha vuelto a la configuración de fábrica. La contraseña maestra vuelve a 999999. Los datos del usuario no se han eliminado.

Ejemplos de conexión para una y dos puertas

Control de acceso para una puerta con cerradura electromagnética Silvercloud YE910 o Silvercloud YS810 y fuente de alimentación PNI ST3.4A.



Control de acceso para dos puertas con cerradura electromagnética Silvercloud YE910 o Silvercloud YS810 y fuente de alimentación PNI ST3.4A.



Description

Le PNI DK220 est un dispositif de contrôle d'accès autonome et un lecteur de proximité. Il est équipé de deux relais pour le contrôle de deux portes et prend en charge un maximum de 2000 utilisateurs, chaque utilisateur peut disposer d'un code PIN et d'une carte d'accès. Le clavier peut être connecté à une clé électromagnétique, un système d'alarme, une sonnette, un bouton d'accès ou un capteur de porte.

L'appareil dispose de 7 modes de fonctionnement: lecteur de carte Wiegand, contrôle d'accès pour une porte, contrôle d'accès pour deux portes, contrôle d'accès avec lecteur de carte externe pour deux portes, deux unités interconnectées pour deux portes, anti-passback pour une porte et deux portes Anti-passback.

Caractéristiques principales

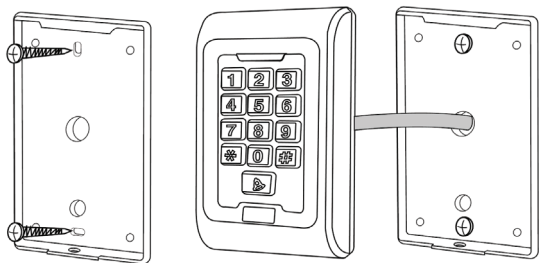
- Boîtier en alliage d'aluminium avec classe de résistance à l'eau IP65
- Lecteur de carte 125KHz intégré
- Touches numériques éclairées. L'éclairage de la touche peut être programmé comme suit: Normal ON, Normal OFF ou Human-Approach ON (s'allume lorsqu'il détecte un mouvement).
- Alarme de sabotage, alarme de déclenchement de capteur de porte, alarme de code de contrainte Ce code peut être utilisé lorsque l'utilisateur est forcé de menacer d'ouvrir la porte. En tapant ce code, la porte s'ouvrira mais activera une alarme silencieuse).
- Ajouter et supprimer des cartes avec la carte administrateur.
- Enregistrez et supprimez des utilisateurs par clés

Spécifications techniques

Tension d'alimentation	12V AC/DC
Consommation en veille	<25mA
Charge de sortie de serrure électrique	<1A
Charge de sortie d'alarme	<1A
Charge de sortie de sonnette	<1A
Distance de lecture de carte	maximum 40 mm
Capacité utilisateur	maximum 2000
Cartes compatibles	EM 125KHz/HID 125KHz
Format de transmission de la carte	26-37 bits Wiegand
Format de transmission du clavier	4 bits et 8 bits et numéro de carte virtuelle
Température de fonctionnement	-26°C ~ +80°C

Installation

Choisissez l'emplacement d'installation et faites des trous dans le mur qui correspondent aux trous du support de montage. Fixez le support mural avec les vis incluses dans l'emballage. Faites passer les câbles à travers la fente au milieu du support. Connectez les câbles. Isolez les câbles non utilisés pour éviter les courts-circuits.



Câblage

Zone 1		
BELL_A	Rose	Bouton de sonnette
BELL_B	Rose	Bouton de sonnette
ALARM+	Rouge	Connecteur d'alarme
AC2	Noir	AC
OPEN2	Jaune	Bouton d'accès
D_IN2	Brun	Contact de porte
ALARM2-	Gris	Alarme 2
NO2	Bleu	Relais 2 NO
COM2	Mauve	Relais 2 COM
NC2	Orange	Relais 2 NC

Zone 2

D0	Vert	Sortie Wiegand D0
D1	Blanc	Sortie Wiegand D1
AC1	Rouge	AC1 (+ 12V)
GND	Noir	GND
OPEN1(LED)	Jaune	Bouton d'accès (pour LED verte)
D_IN1(BZ)	Brun	Contact de porte (pour buzzer)
ALARM1-	Gris	Alarme 1
NO1	Bleu	Relais 1 NO
COM1	Mauve	Relais 1 COM
NC1	Orange	Relais 1 NC

Avertissements sonores et lumineux

Statut	LED	Buzzer
Etre prêt	Le rouge clignote	
appuyez sur la touche		Di
Lire la carte	Vert	Di.
Porte 1 ouverte	Vert	Di.
Porte 2 ouverte	Le vert clignote	Di.
Opération réussie	Vert	Di.
L'opération a échoué		DiDiDi
NIP	Rouge	
Lire la carte et le code PIN	Rouge	
Lecture de plusieurs cartes	Rouge	
Sous menu	Rouge	
Sous les paramètres	Orange	
Carte administrateur entrer	Orange	DiDi
Sortie carte administrateur	Le rouge clignote	Di.
Alarme	Le rouge clignote rapidement	Alarm

Guide de programmation rapide

1. Paramètres administrateur

* Code master #	00	<i>Saisissez le nouveau Code master # Répéter le nouveau Code master #</i>	Changer le code master. <i>Remarque: Le code maître par défaut est 999999. Le code maître doit avoir entre 6 et 8 chiffres.</i>
	01	<i>Lire la carte</i>	Enregistrement de la carte administrateur (master) pour l'ajout de cartes.
	02	<i>Lire la carte</i>	Enregistrement de la carte administrateur (master) pour la suppression des cartes.
	03	<i>Lire la carte</i>	Enregistrement de la carte d'alarme « duress » pour la zone 1
	04	<i>Lire la carte</i>	Enregistrement de la carte d'alarme « duress » pour la zone 2

* Code master #	05	Saisissez le code PIN à 8 chiffres	Saisissez le code PIN « duress » pour la zone1 Remarque: le premier chiffre du code PIN doit être 1 pour la zone 1.
	06	Saisissez le code PIN à 8 chiffres	Saisissez le code PIN « duress » pour la zone2 Remarque: le premier chiffre du code PIN doit être 2 pour la zone 2.
	07	0000 #	Supprimer tous les utilisateurs
	51	Master ouvert Serrure 1	
	52	Master ouvert Serrure 2	

Noter:

Le code PIN « contrainte » et la carte « contrainte » peuvent être utilisés lorsque l'utilisateur est contraint d'ouvrir la porte. En tapant ce code ou en lisant cette carte, la porte s'ouvrira mais en même temps elle enverra un signal d'alarme.

2. Paramètres utilisateur pour la zone 1 et la zone 2

Ajouter une carte d'utilisateur

<i>* Code master #</i>	11 (pour la zone 1)	<i>Lire la carte</i>
		<i>Saisissez ID # Lire la carte</i>
	21 (pour la zone 2)	<i>Saisissez numéro de carte #</i>
		<i>Saisissez ID # Saisissez numéro de carte #</i>

Remarque: les utilisateurs peuvent être ajoutés les uns après les autres sans quitter le mode de programmation. L'ID utilisateur peut contenir entre 1 et 4 chiffres, dans la plage 1 - 2000. 1, 01, 001 et 0001 signifient tous 1.

Ajouter un code PIN utilisateur

<i>* Code master #</i>	11 (pour la zone 1) 21 (pour la zone 2)	<i>Saisissez ID # Saisissez PIN #</i>
------------------------	--	---------------------------------------

Remarque: Le code PIN peut comporter de 4 à 6 chiffres. Le premier chiffre doit être 1 pour la zone 1 et 2 pour la zone 2. « 1234 » est réservé, ne peut pas être défini comme PIN.

Supprimer l'utilisateur

* Code master #	12 (pour la zone 1)	Lire la carte
	22 (pour la zone 2)	Saisissez ID #
		Saisissez numéro de carte #

Remarque: les utilisateurs peuvent être supprimés les uns après les autres sans quitter le mode de programmation.

Supprimer tous les utilisateurs

* Code master #	07	0000 #
-----------------	----	--------

Remarque: cette commande supprime tous les utilisateurs de la zone 1 et de la zone 2.

Modes d'accès

* Code master #	13 (pour la zone 1) 23 (pour la zone 2)	0 #	Par carte
		1 #	Par carte + PIN
		2 #	Par carte ou PIN (default setting)

Délai de porte ouverte

* Code master #	14 (pour la zone 1) 24 (pour la zone 2)	0 - 99 #	Par défaut 5
-----------------	--	----------	--------------

Définir les modes de fermeture de la porte

* Code master #	15 (pour la zone 1)	0 #	Mode impulsion (réglage par défaut). Chaque fois qu'un code est entré ou qu'une carte valide a été lue, la porte s'ouvrira et se fermera automatiquement après l'intervalle de temps défini (entre 0,05 s et 99 s).
	25 (pour la zone 2)	1 #	Basculer en mode. Chaque fois qu'un code est entré ou qu'une carte valide a été lue, la porte s'ouvrira mais ne se fermera pas jusqu'à ce que le code soit à nouveau entré ou que la carte soit lue.

Ouvrez la porte avec plusieurs cartes

* Code master #	16 (pour la zone 1) 26 (pour la zone 2)	1 - 10 #	Par défaut 1
-----------------	--	----------	--------------

Remarque: la porte ne s'ouvrira qu'une fois toutes les cartes lues.

Par exemple, par commande *Code master#16 3#, vous devez lire 3 cartes d'affilée pour ouvrir la porte. Ce paramètre n'est utile que si vous avez configuré le clavier en mode d'accès par carte.

Ajouter des cartes d'utilisateur en série

<i>* Code master #</i>	<i>17</i> (pour la zone 1) <i>27</i> (pour la zone 2)	<i>Saisissez ID #, Saisissez numéro de carte #, Saisissez quantité #</i>
------------------------	--	--

Remarque: les numéros de cartes doivent être consécutifs (entre 8 et 10 caractères). La quantité de carte est comprise entre 1 et 2000.

3. Les paramètres du système

* Code master #	30	0-15 #	Réglage du code de l'unité (Facility Code). Par défaut: 0
	31	0 #	Lecteur Wiegand
		1 #	Contrôle d'accès autonome à une porte (paramètre par défaut)
		2 #	Contrôle d'accès autonome pour deux portes
		3 #	Avec lecteur externe pour deux portes
		4 #	Deux unités interconnectées pour deux portes (protection lors de l'ouverture de plusieurs portes)
* Code master #	31	5 #	Anti-passback pour une porte
		6 #	Anti-passback pour deux portes
	32	26-37 #	Réglage du format Wiegand 26 34 37. Par défaut 26.
	33	0-2 #	Paramétrage du format de transmission du clavier: 0 1 2 Après réinitialisation, ce paramètre reste inchangé.

<i>* Code master #</i>	34	1-3 #	Définir la durée de l'alarme (réglage par défaut 1 minute) Après réinitialisation, ce paramètre reste inchangé.
	35	0 #	Mode sans échec 1. Mode normal. (Paramètres par défaut)
		1 #	Mode sans échec 2. Si un mauvais code est entré ou qu'une carte invalide est lue 10 fois de suite dans les 10 minutes, par mesure de sécurité, le système s'arrête.

<i>* Code master #</i>	35	2 #	Mode sécurité 3. Mode alarme. En cas de saisie d'un mauvais code ou de lecture d'une carte invalide 10 fois de suite en 10 minutes, par précaution, l'alarme externe (si connectée) et le buzzer intégré au clavier se déclencheront.
------------------------	----	-----	--

4. Paramètres utilisateur facultatifs

* Code master #	41	0 #	Buzzer désactivé. Le buzzer ne reste actif que lorsque l'appareil entre en mode programmation.
		1 #	Son des touches actives (Paramètres par défaut)
	42	0 #	Rétroéclairage des touches désactivé
		1 #	Rétroéclairage des touches activé
		2 #	Mode automatique. Normalement, le voyant de la touche est éteint mais s'allume lorsque la présence humaine est détectée.

* Code master #	43	0 #	LED éteinte lorsque l'appareil est en veille.
		1 #	La LED clignote lorsque l'appareil est en mode veille. (Paramètres par défaut)

Notes importantes

1. The Code master must have 6-8 digits.
2. The code "duress" must have 8 digits. The first digit of the code must be 1 pour la zone 1 and 2 pour la zone 2.

3. Le code PIN de l'utilisateur doit comporter de 4 à 6 chiffres. Le premier chiffre du code PIN doit être 1 pour la zone 1 et 2 pour la zone 2.
4. L'ID utilisateur peut être n'importe quel nombre entre 1 et 2000.
5. Le numéro de carte doit comporter entre 8 et 10 chiffres. Si le numéro de carte contient moins de 8 chiffres, ajoutez 0 devant le code.
6. Temporisation porte ouverte: entre 0 et 99 secondes. 0 = 50mS
7. Lorsqu'une carte d'utilisateur est enregistrée dans l'appareil, l'appareil génère automatiquement un code PIN 1234 qui ne peut pas déverrouiller la porte.
8. Si un code PIN principal non valide est saisi, l'appareil passe en veille au bout de 5 secondes. Si un code PIN maître valide est saisi, l'appareil passe en mode veille au bout de 30 secondes.
9. Lors de l'utilisation du clavier, l'appui sur la touche # confirme le raccourci clavier exécuté précédemment. Lors de l'ajout ou de la suppression de cartes les unes après les autres, l'appui sur la touche # indique la fin du cycle, et l'appui sur la touche * indique la sortie de cette opération.
10. Lorsque vous ajoutez des cartes en série, l'appareil attribue automatiquement un numéro d'identification et un numéro de carte. Le numéro d'identification et le numéro de carte augmentent automatiquement à chaque carte ajoutée, jusqu'à un maximum de 2000.
11. Le mode de fonctionnement et le format de transmission du clavier sont réglés en usine. L'utilisateur peut modifier ces paramètres selon ses besoins. Après la réinitialisation de l'appareil, ce paramètre reste inchangé.
12. Après avoir enregistré avec succès les utilisateurs dans la zone 1, le voyant devient vert. Après avoir enregistré avec succès les

utilisateurs dans la zone 2, la LED verte clignote.

5. Opérations de carte maîtresse

Ajouter un utilisateur pour la zone 1

Lisez la carte d'ajout principale, puis lisez les cartes d'utilisateur l'une après l'autre, et enfin lisez à nouveau la carte d'ajout principale.

Supprimer l'utilisateur pour la zone 1

Lire la carte de suppression principale, puis lire les cartes d'utilisateur l'une après l'autre, et enfin relire la carte de suppression principale.

6. Opérations utilisateur

Par carte

Lire à la carte. La serrure se déverrouillera.

Si vous avez défini plusieurs cartes pour l'ouverture de la porte (entre 2 et 10), lisez toutes les cartes l'une après l'autre dans les 5 secondes, après quoi la serrure se déverrouillera.

Par carte + PIN

Lire la carte délimitée, le NIP (4 ou 6 chiffres) +#. La serrure se déverrouillera.

Par carte ou PIN

Lire à la carte. La serrure se déverrouillera. Ou le PIN +#. La serrure se déverrouillera.

Changer le code PIN sans entrer en mode programmation

** lire la carte de l'utilisateur, Saisissez l'ancien PIN #, Saisissez le nouveau PIN # répéter le nouveau PIN*

ou

** Saisissez le numéro d'identification ID, Saisissez l'ancien PIN #, Saisissez le nouveau PIN # répéter le nouveau PIN*

Remarque: Le PIN pour la zone 1 doit commencer par 1 et le PIN pour la zone 2 doit commencer par 2.

7. Fonction d'alarme

Alarme de sabotage

Si l'appareil est démonté par effraction, le buzzer interne et l'alarme externe (si connecté) sonneront.

Alarme porte ouverte

Si vous avez connecté un capteur de porte filaire au clavier de contrôle d'accès et que ce capteur se déclenche, le buzzer interne et l'alarme externe (si connecté) sonneront.

Pour désactiver l'alarme:

Read the user card or master card, or Saisissez le PIN administrateur (master).

Si vous n'effectuez aucune opération, l'alarme s'éteindra automatiquement après 1 minute.

Alarme “Duress”

Si la carte « duress » est lue ou le code PIN « duress » est entré sur la zone 1 ou la zone 2, la serrure s’ouvrira et, en même temps, l’alarme externe sera déclenchée (si connectée). Le buzzer interne ne se déclenchera pas.

8. Modes de fonctionnement

Lecteur de carte Wiegand

Dans ce mode, le clavier fonctionne comme un lecteur de carte connecté à un dispositif de contrôle d’accès.

Commandes prises en charge:

- Changer le code PIN principal
- Définir le code de l’établissement
- Paramétrage du format de transmission de la carte
- Paramétrage du format de transmission du clavier
- Paramètres facultatifs
- Alarme de sabotage

Contrôle d’accès autonome pour une seule porte

Dans ce mode, le clavier ouvre une seule porte. La porte peut être ouverte Par carte ou PIN ou carte + PIN. Le clavier prend en charge la connexion d’un lecteur de carte externe ou d’un bouton d’accès pour sortir du bâtiment.

Contrôle d’accès autonome pour deux portes

Dans ce mode, le clavier peut contrôler deux portes. Lire la carte ou le PIN pour la zone 1 et la porte 1 s’ouvriront. Lire la carte ou le code

PIN pour la zone 2 et la porte 2 s'ouvriront.

Avec lecteur de carte externe pour ouvrir deux portes

Dans ce mode, le clavier permet l'accès pour la porte 1 et le lecteur de carte externe permet l'accès pour la porte 2.

Lire la carte ou le code pour la zone 1 sur le clavier du contrôle d'accès. La porte 1 s'ouvrira. Lire la carte ou le code pour la zone 2 sur le lecteur de carte externe. La porte 2 s'ouvrira.

Deux appareils interconnectés pour ouvrir deux portes

Ce mode est plus adapté aux emplacements tels que les banques, les prisons ou pour les situations qui nécessitent un niveau de sécurité avancé.

Seulement après la fermeture de la porte 2, Lire la carte ou le code sur le clavier pour ouvrir la porte 1. Et seulement après que la porte 1 est fermée, Lire la carte ou le code sur le lecteur de carte pour ouvrir la porte 2.

Anti-passback pour une seule porte

Dans ce mode de fonctionnement, le clavier doit être installé à l'extérieur pour permettre l'accès à l'intérieur du bâtiment, et le lecteur de carte externe doit être monté à l'intérieur pour permettre la sortie hors du bâtiment.

Si l'entrée de l'utilisateur dans le bâtiment n'a pas été enregistrée, l'utilisateur ne peut pas sortir en lisant la carte sur le lecteur de carte. Aussi, l'usager ne peut pas entrer une seconde fois dans le bâtiment si sa sortie n'a pas été enregistrée.

Remarque: La porte ne peut être ouverte qu'en lisant la carte pour la zone 1. Tous les autres modes d'accès à la zone 1 et à la zone 2 sont

invalides.

Anti-passback pour deux portes

Dans ce mode, le clavier de la porte 1 est l'unité principale d'anti-passback et le lecteur de carte externe de la porte 2 est l'unité d'anti-passback secondaire. Ainsi, un système anti-passback adapté à une installation dans les parkings est créé.

L'utilisateur peut entrer dans le bâtiment par la porte 1 en lisant la carte sur le clavier du contrôle d'accès et ne peut sortir que par la porte 2 en lisant la carte sur le lecteur de carte externe. Si l'entrée de l'utilisateur n'a pas été enregistrée sur la porte 1, il ne pourra pas sortir par la porte 2. De plus, l'utilisateur ne pourra pas entrer une deuxième fois si sa sortie n'a pas été enregistrée.

Remarque: La porte ne peut être ouverte qu'en lisant la carte pour la zone 1. Tous les autres modes d'accès Zone 1 et Zone 2 sont invalides.

Dépannage

Problème	Cause	Solution
Distance de lecture de carte trop courte	Carte de faible qualité	Utiliser des cartes originales
Problèmes de configuration du code PIN	1. Le code PIN n'est pas conforme à la norme 2. Vous êtes en mode lecture de carte, définissez le mot de passe	1. Le premier chiffre du PIN doit être 1 ou 2, selon la Zone. 2. Le code PIN ne doit pas être 1234. Le code PIN doit comporter 4 ou 6 chiffres.

<p>Le code PIN n'ouvre pas la porte</p>	<p>1. Vous avez utilisé le code PIN 1234 2. Le mode d'accès défini ne permet pas l'accès PIN</p>	<p>1. Modifiez votre NIP. 2. Changer le mode d'accès: carte ou PIN.</p>
<p>Pas de réponse après lecture de la carte</p>	<p>Le clavier n'est pas en veille, il peut être en mode programmation</p>	<p>Appuyez sur la touche *, la LED clignote. Le clavier est maintenant en mode veille.</p>
<p>Le clavier ne s'allume pas</p>	<p>Mauvais réglages du clavier</p>	<p>1. Activez ou activez le rétroéclairage des touches. En mode auto, les touches ne s'allument qu'après appui et restent allumées 30 secondes.</p>
<p>Code maître invalide</p>	<p>Vous avez oublié le code maître</p>	<p>Réinitialisez l'appareil. Le code maître revient à 999999. Lors de la réinitialisation, les données utilisateur ne sont pas supprimées.</p>

Réinitialiser le Code master

Coupez l'alimentation du clavier de contrôle d'accès.

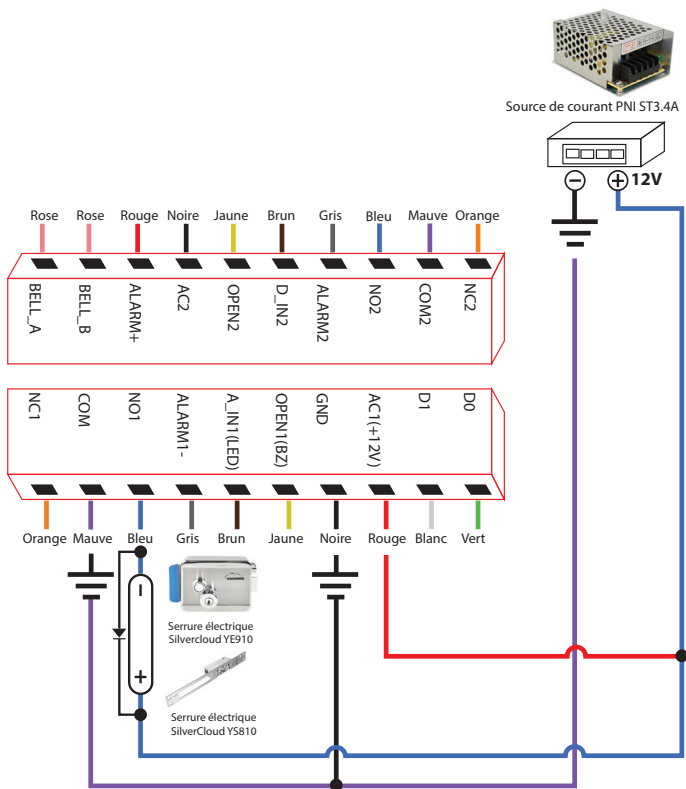
Maintenez la touche # enfoncée tout en redémarrant l'alimentation.

Après avoir entendu deux sons Di ., relâchez la touche #.

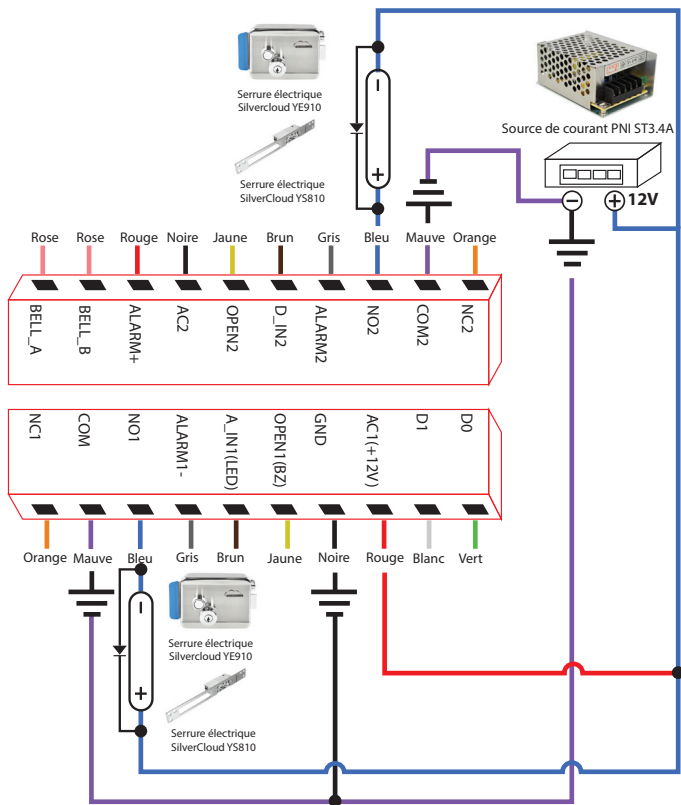
Le clavier est revenu aux réglages d'usine. Le mot de passe maître revient à 999999. Les données utilisateur n'ont pas été supprimées

Exemples de connexion pour une et deux portes

Contrôle d'accès pour une porte avec serrure électromagnétique Silvercloud YE910 ou Silvercloud YS810 et alimentation PNI ST3.4A.



Contrôle d'accès pour deux portes avec serrure électromagnétique Silvercloud YE910 ou Silvercloud YS810 et alimentation PNI ST3.4A.



Leírás

A PNI DK220 egy önálló beléptetőeszköz és proximity olvasó. Két relével van felszerelve a kétajtós vezérléshez és maximum 2000 felhasználót támogat, minden felhasználó rendelkezhet PIN kóddal és belépőkártyával.

A billentyűzet csatlakoztatható elektromágneses kulcshoz, riasztórendszerhez, csengőhöz, beléptetőgombhoz vagy ajtóérzékelőhöz.

A készülék 7 üzemmóddal rendelkezik: Wiegand kártyaolvasó, beléptető egy ajtóhoz, beléptető két ajtóhoz, beléptető külső kártyaolvasóval két ajtóhoz, két összekapcsolt egység két ajtóhoz, visszalépés gátló egy ajtóhoz és két ajtóhoz anti-passback.

Főbb jellemzői

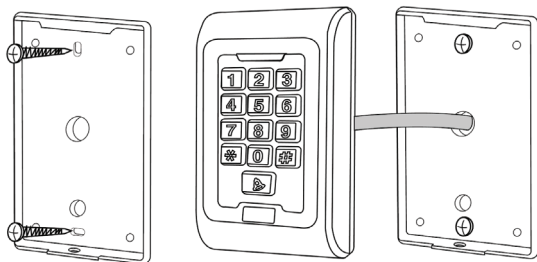
- Alumíniumötvözet ház IP65 vízállósági osztályú
- Beépített 125KHz-es kártyaolvasó
- Megvilágított számbillentyűk. A gomb lámpája a következőképpen programozható: Normál BE, Normál KI vagy Human-Approach ON (világít, ha mozgást észlel).
- Szabotázsriasztó, ajtóérzékelő kioldó riasztás, kényszerkódos riasztás Ez a kód akkor használható, ha a felhasználót az ajtó kinyitásával kényszerítik. Amikor beírja ezt a kódot, az ajtó kinyílik, de bekapcsol egy néma riasztás.
- Kártyák hozzáadása és törlése a rendszergazdai kártyával.
- Felhasználók regisztrálása és törlése kulcsokkal

Műszaki adatok

Tápfeszültség	12V AC/DC
Készenléti fogyasztás	<25mA
Elektromos zár kimeneti terhelése	<1A
Riasztás kimeneti terhelés	<1A
Az ajtócsengő kimeneti terhelése	<1A
Kártyaolvasási távolság	maximum 40 mm
Felhasználói kapacitás	maximum 2000
Kompatibilis kártyák	EM 125Khz/HID 125KHz
Kártyás átviteli formátum	26-37 bites Wiegand
Billentyűzet átviteli formátum	4 bites és 8 bites, valamint virtuális kártyaszám
Üzemhőmérséklet	-26°C ~ +80°C

Telepítés

Válassza ki a telepítési helyet, és készítsen lyukakat a falon, amelyek megegyeznek a tartókonzolon lévő lyukakkal. Rögzítse a fali tartót a csomagban található csavarokkal. Vezesse át a kábeleket a tartó közepén lévő nyíláson. Csatlakoztassa a kábeleket. A rövidzárlat elkerülése érdekében szigetelje le a nem használt kábeleket.



Vezeték

Zóna 1		
BELL_A	Rózsaszín	Ajtócsengő gomb
BELL_B	Rózsaszín	Ajtócsengő gomb
ALARM+	Piros	Riasztó csatlakozó
AC2	Fekete	AC bemenet
OPEN2	Sárga	Kilépés gomb
D_IN2	Barna	Ajtóérintkező
ALARM2-	Szürke	2. riasztás
NO2	Kék	Relé 2 NO
COM2	Lila	Relé 2 COM
NC2	Narancs	Relé 2 NC

Zóna 2

D0	Zöld	Wiegand kimenet D0
D1	Fehér	Wiegand kimenet D1
AC1	Piros	AC1 (+ 12V)
GND	Fekete	GND
OPEN1(LED)	Sárga	Kilépés gomb (zöld LED-hez)
D_IN1(BZ)	Barna	Ajtóérintkező (csengőhöz)
ALARM1-	Szürke	1. riasztás
NO1	Kék	Relé 1 NO
COM1	Lila	Relé 1 Com
NC1	Narancs	Relé 1 NC

Hangos és fényes figyelmeztetések

Állapot	LED	Buzzer
Készenlétben lévő	Piros villog	
Nyomja meg a gombot		Di
Olvassa el a kártyát	Zöld	Di.
1. ajtó nyitva	Zöld	Di.
2. ajtó nyitva	Zöld villog	Di.
Sikeres művelet	Zöld	Di.
A művelet nem sikerült		DiDiDi
PIN bevétel	Piros	
Olvassa el a kártyát és a PIN-kódot	Piros	
Több kártya olvasása	Piros	
A menü alatt	Piros	
A beállítások alatt	narancs	
Adminisztrátori kártya beírása	narancs	DiDi
Adminisztrátori kártya kilépése	Piros villog	Di.
Riasztás	A piros gyorsan villog	Riasztás

Gyors programozási útmutató

1. Rendszergazdai beállítások

* Rendszergazda kód #	00	Írja be az új Rendszergazda kódot # Ismételje meg az új Rendszergazda kódot #	Változás Rendszergazda kód. Megjegyzés: Az alapértelmezett mesterkód a 999999. A mesterkódnak 6-8 számjegyből kell állnia.
	01	Olvassa el a kártyát	Rendszergazdai kártya regisztráció a kártyák hozzáadásához.
	02	Olvassa el a kártyát	Rendszergazdai kártya regisztráció a kártyák törléséhez.
	03	Olvassa el a kártyát	„Duess” riasztókártya regisztráció az 1. zónához
	04	Olvassa el a kártyát	„Duess” riasztókártya regisztráció az 2. zónához

* Rendszergazda kód #	05	Írja be a 8 számjegyű PIN-kódot	Írja be az 1. zóna „kényszer” PIN kódját Megjegyzés: A PIN-kód első számjegyének 1-nek kell lennie az 1-es zónához.
	06	Írja be a 8 számjegyű PIN-kódot	Írja be az 2. zóna „kényszer” PIN kódját Megjegyzés: A PIN-kód első számjegyének 2-nek kell lennie az 2-es zónához.
	07	0000 #	Az összes felhasználó törlése
	51	A rendszergazda nyissa meg a zárat 1	
	52	A rendszergazda nyissa meg a zárat 2	

Jegyzet:

A „kényszer” PIN kód és a „kényszer” kártya akkor használható, ha a felhasználó kénytelen kinyitni az ajtót. A kód begépelésekor vagy a kártya kiolvasásakor az ajtó kinyílik, ugyanakkor riasztást küld.

2. Felhasználói beállítások az 1. és 2. zónához

Felhasználói kártya hozzáadása

<i>* Rendszergazda kód #</i>	11 (az 1. zónához)	<i>Olvassa el a kártyát</i>
		<i>Írja be az azonosítót # Olvassa el a kártyát</i>
	21 (az 2. zónához)	<i>Írja be a kártya számát #</i>
		<i>Írja be az azonosítót # Írja be a kártya számát #</i>

Megjegyzés: A felhasználók egymás után adhatók hozzá a programozási mód elhagyása nélkül. A felhasználói azonosító 1 és 4 számjegyből állhat, 1 és 2000 közötti tartományban. Az 1, 01, 001 és 0001 mindegyike 1.

Felhasználói PIN hozzáadása

<i>* Rendszergazda kód #</i>	11 (az 1. zónához)	<i>Írja be az azonosítót # Írja be a PIN-kódot #</i>
	21 (az 2. zónához)	

Megjegyzés: A PIN-kód 4-6 számjegyből állhat. Az első számjegynek 1 az 1. zónához és 2 az 2. zónához kell lennie. Az „1234” le van foglalva, nem állítható be PIN-kódként.

Felhasználó törlése

* Rendszergazda kód #	12 (az 1. zónához)	Olvassa el a kártyát
	22 (az 2. zónához)	Írja be az azonosítót #
		Írja be a kártya számát #

Megjegyzés: A felhasználók egymás után törölhetők a programozási mód elhagyása nélkül.

Az összes felhasználó törlése

* Rendszergazda kód #	07	0000 #
-----------------------	----	--------

Megjegyzés: Ez a parancs törli az 1. és 2. zónában lévő összes felhasználót.

Hozzáférési módok

* Rendszergazda kód #	13 (az 1. zónához)	0 #	Kártyával
		1 #	Kártyával + PIN
	23 (az 2. zónához)	2 #	Kártyával vagy PIN (alapértelmezett beállítás)

Nyitott ajtó késleltetés

* Rendszergazda kód #	14 (az 1. zónához) 24 (az 2. zónához)	0 - 99 #	Alapbeállítás 5
-----------------------	--	----------	-----------------

Állítsa be az ajtózárási módokat

* Rendszergazda kód #	15 (az 1. zónához) 25 (az 2. zónához)	0 #	Impulzus üzemmód (alapbeállítás). Minden alkalommal, amikor beírnak egy kódot vagy egy érvényes kártyát olvasnak, az ajtó automatikusan kinyílik és bezárul a beállított időintervallum elteltével (0,05 mp és 99 mp között).
		1 #	Mód váltása. Minden alkalommal, amikor beírnak egy kódot vagy egy érvényes kártyát leolvasnak, az ajtó kinyílik, de nem záródik be, amíg a kódot újra be nem írják, vagy a kártya leolvasásra nem kerül.

Nyissa ki az ajtót több kártyával

<i>* Rendszergazda kód #</i>	16 (az 1. zónához) 26 (az 2. zónához)	1 - 10 #	Alapértelmezett beállítás 1
------------------------------	--	----------	-----------------------------

Megjegyzés: Az ajtó csak az összes kártya beolvasása után nyílik ki. Például a * Rendszergazda kód # 16 3 # parancsra egymás után 3 kártyát kell elolvasni az ajtó kinyitásához. Ez a beállítás csak akkor hasznos, ha a billentyűzetet kártya hozzáférési módba állította.

Felhasználói kártyák hozzáadása sorozatban

<i>* Rendszergazda kód #</i>	17 (az 1. zónához) 27 (az 2. zónához)	<i>Írja be az azonosítót #, Írja be a kártya számát #, Adja meg a mennyiséget #</i>
------------------------------	--	---

Megjegyzés: A kártyaszámoknak egymást követőnek kell lenniük (8 és 10 karakter között). A kártya mennyisége 1 és 2000 között van.

3. Rendszerbeállítások

* Rendszergazda kód #	30	0-15 #	Az egységkód (Facility Code) beállítása. Alapértelmezett: 0
	31	0 #	Wiegand olvasó
		1 #	Egyajtós, önálló beléptető-vezérlés (alapbeállítás)
		2 #	Önálló beléptető rendszer két ajtóhoz
		3 #	Külső olvasóval két ajtóhoz
		4 #	Két összekapcsolt egység két ajtóhoz (védelem több ajtó nyitásakor)
* Rendszergazda kód #	31	5 #	Anti-passback ajtóhoz
		6 #	Anti-passback két ajtóhoz
	32	26-37 #	Wiegand formátumbeállítás 26 34 37. Alapértelmezett 26
	33	0-2 #	Billentyűzet átviteli formátum beállítása: 0 1 2 A visszaállítás után ez a beállítás változatlan marad.

<i>* Rendszergazda kód #</i>	34	1-3 #	Állítsa be a riasztás időtartamát (alapbeállítás 1 perc) A visszaállítás után ez a beállítás változatlan marad.
	35	0 #	Csökkentett mód 1. Normál mód. (alapértelmezett beállítás)
		1 #	Biztonságos mód 2. Ha rossz kódot ír be, vagy 10 percen belül egymás után 10-szer érvénytelen kártyát olvas ki, biztonsági okokból a rendszer leáll.

<i>* Rendszergazda kód #</i>	35	2 #	Biztonsági mód 3. Riasztási mód. Ha rossz kódot ír be, vagy 10 percen belül 10-szer egymás után érvénytelen kártyát olvas ki, elővigyázatosságból a külső riasztó (ha csatlakoztatva van) és a billentyűzetbe épített hangjelző bekapcsol.
------------------------------	----	-----	---

4. Választható felhasználói beállítások

<i>* Rendszergazda kód #</i>	41	0 #	Hangjelzés kikapcsolva. A hangjelző csak akkor marad aktív, ha a készülék programozási módba lép.
		1 #	Aktív billentyűhang (alapértelmezett beállítás)
	42	0 #	Billentyű háttérvilágítás kikapcsolva
		1 #	Billentyű háttérvilágítás bekapcsolva
		2 #	Automata üzemmód. Normál esetben a gomb jelzőfénye nem világít, de felgyullad, ha emberi jelenlétet észlel.

<i>* Rendszergazda kód #</i>	43	0 #	A LED nem világít, ha a készülék készenléti állapotban van.
		1 #	A LED villog, ha a készülék készenléti üzemmódban van. (alapértelmezett beállítás)

Fontos jegyzetek

1. A mesterkódnak 6-8 számjegyűnek kell lennie.
2. A „duress” kódnak 8 számjegyűből kell állnia. A kód első számjegye 1 az 1. zónához és 2 az 2. zónához.

3. A felhasználói PIN-kódnak 4-6 számjegyből kell állnia. A PIN kód első számjegyének 1 az 1. zónához és 2 az 2. zónához kell lennie.
4. A felhasználói azonosító bármilyen szám lehet 1 és 2000 között.
5. A kártyaszámnak 8 és 10 közötti számjegyből kell állnia. Ha a kártyaszám 8 számjegynél kevesebbet tartalmaz, adjon hozzá 0-t a kód elé.
6. Nyitott ajtó késleltetési ideje: 0 és 99 másodperc között. 0 = 50 ms
7. Amikor felhasználói kártyát regisztrálnak a készülékben, a készülék automatikusan generál egy PIN 1234 kódot, amely nem tudja kinyitni az ajtót.
8. Érvénytelen mester PIN megadása esetén a készülék 5 másodperc múlva készenléti állapotba lép. Érvényes mester PIN kód megadása esetén a készülék 30 másodperc elteltével készenléti módba lép.
9. A billentyűzet használatakor a # gomb megnyomásával megerősíti az előzőleg végrehajtott billentyűparancsot. A kártyák egymás utáni hozzáadásakor vagy törlésekor a # gomb megnyomása a ciklus végét, a * gomb megnyomása pedig a műveletből való kilépést jelzi.
10. Amikor sorba helyezi a kártyákat, a készülék automatikusan hozzárendel egy azonosítószámot és egy kártyaszámot. Az azonosítószám és a kártyaszám minden egyes kártya hozzáadásával automatikusan növekszik, maximum 2000-ig.
11. A billentyűzet működési módja és átviteli formátuma gyárilag be van állítva. A felhasználó szükség szerint módosíthatja ezeket a beállításokat. Az eszköz visszaállítása után ez a beállítás változatlan marad.
12. Miután sikeresen regisztrálta a felhasználókat az 1. zónában, a LED zöldre vált. A felhasználók sikeres regisztrációja után a 2. zónában a zöld LED villog.

5. Rendszergazdai kártya műveletek

Felhasználó hozzáadása az 1. zónához

Olvassa el a fő hozzáadó kártyát, majd olvassa el egymás után a felhasználói kártyákat, végül olvassa el újra a fő hozzáadó kártyát.

Felhasználó törlése az 1. zónához

Olvassa el a főtörlési kártyát, majd olvassa el egymás után a felhasználói kártyákat, végül olvassa el újra a főtörlési kártyát.

6. Felhasználói műveletek

Kártyával

Olvassa el a kártyát. A zár feloldódik.

Ha több kártyát állított be az ajtónyitáshoz (2 és 10 között), olvassa el az összes kártyát egymás után 5 másodpercen belül, ami után a zár kiold.

Kártyával + PIN

Olvassa el a kártyát, írja be a PIN-kódot (4 vagy 6 számjegy) +#. A zár feloldódik.

Kártyával vagy PIN

Olvassa el a kártyát. A zár feloldódik. Vagy írja be a PIN +# kódot. A zár feloldódik.

Változtassa meg a PIN kódot anélkül, hogy programozási módba lépne

** Olvassa el a felhasználói kártyát, írja be a régi PIN # kódot, írja be az új PIN kódot # ismétlje meg az új PIN kódot*

vagy

** írja be az azonosítószámot # írja be a régi PIN-kódot #, írja be az új PIN-kódot # ismétlje meg az új PIN-kódot*

Megjegyzés: A PIN az 1. zónához 1-gyel, a PIN az 2. zónához 2-vel kell kezdődnie.

7. Riasztás funkció

Szabotázs riasztás

Ha a készüléket betörés miatt szétszedték, megszólal a belső hangjelző és a külső riasztó (ha csatlakoztatva van).

Nyitott ajtó riasztó

Ha vezetékes ajtóérzékelőt csatlakoztatott a beléptető billentyűzethez, és ez az érzékelő aktiválódik, megszólal a belső berregő és a külső riasztó (ha van).

Az ébresztő kikapcsolása:

Olvassa el a felhasználói kártyát vagy a rendszergazdai kártyát, vagy írja be a rendszergazdai PIN-kódot.

Ha nem végez semmilyen műveletet, az ébresztő 1 perc múlva automatikusan kikapcsol.

“Duress” riasztás

Ha a „duress” kártya beolvasásra kerül, vagy a „duress” PIN kódot beírják az 1. vagy 2. zónába, a zár kinyílik, és ezzel egyidejűleg a külső riasztás is aktiválódik (ha csatlakoztatva van). A belső hangjelzés nem szólal meg.

8. Üzem módok

Wiegand kártyaolvasó

Ebben az üzemmódban a billentyűzet kártyaolvasóként működik beléptető eszközhöz csatlakoztatva.

Támogatott megrendelések:

- Rendszergazdai PIN módosítása
- Állítsa be a létesítmény kódját
- Kártya átviteli formátum beállítása
- Billentyűzet átviteli formátum beállítása
- Választható beállítások
- Szabotázs riasztás

Önálló beléptető egy ajtóhoz

Ebben az üzemmódban a billentyűzet egyetlen ajtót nyit ki. Az ajtó kártyával vagy PIN-kóddal vagy kártya + PIN-kóddal nyitható. A billentyűzet támogatja egy külső kártyaolvasó vagy egy beléptető gomb csatlakoztatását az épületből való kilépéshez.

Önálló beléptető rendszer két ajtóhoz

Ebben az üzemmódban a billentyűzet két ajtót tud vezérelni. Olvassa el a kártyát vagy írja be a PIN kódot az 1. zónához és az 1-es ajtó

kinyílik. Olvassa el a kártyát vagy írja be a PIN kódot az 2. zónához és kinyílik a 2. ajtó.

Külső kártyaolvasóval két ajtó nyitására

Ebben az üzemmódban a billentyűzet lehetővé teszi a hozzáférést az 1-es ajtóhoz, a külső kártyaolvasó pedig a 2-es ajtóhoz.

Olvassa el a kártyát vagy írja be az 1. zónához kódot a beléptető billentyűzeten. Az 1-es ajtó kinyílik. Olvassa el a kártyát vagy írja be az 2. zónához kódot a külső kártyaolvasóba. A 2-es ajtó kinyílik.

Két összekapcsolt eszköz két ajtó kinyitására

Ez a mód alkalmasabb olyan helyekre, mint például bankok, börtönök vagy olyan helyzetek, amelyek magasabb szintű biztonságot igényelnek.

Csak a 2. ajtó bezárása után olvassa el a kártyát, vagy írja be a kódot a billentyűzeten az 1. ajtó kinyitására. És csak az 1. ajtó bezárása után olvassa el a kártyát, vagy írja be a kódot a kártyaolvasón a 2. ajtó kinyitására.

Anti-passback egyetlen ajtóhoz

Ebben az üzemmódban a billentyűzetet a szabadban kell elhelyezni, hogy lehetővé tegye az épületen belüli hozzáférést, és a külső kártyaolvasót beltérben kell felszerelni, hogy lehetővé tegye az épületből való kilépést.

Ha a felhasználó belépését az épületbe nem regisztrálták, a felhasználó a kártyaolvasón lévő kártya leolvasásával nem tud kilépni. Ezenkívül a felhasználó nem léphet be másodszor az épületbe, ha a kilépését nem regisztrálták.

Megjegyzés: Az ajtó csak a kártya leolvasásával nyitható az 1. zónához.

Az összes többi 1. és 2. zóna hozzáférési mód érvénytelen.

Anti-passback két ajtóhoz

Ebben a módban az 1. ajtón lévő billentyűzet a visszalépést gátló adminisztrátor, a 2. ajtó külső kártyaolvasója pedig a másodlagos visszalépést gátló egység. Így jön létre a parkolóba való beépítésre alkalmas anti-passback rendszer.

A felhasználó az épületbe az 1-es ajtón a beléptető billentyűzet kártyájának leolvasásával léphet be, a 2-es ajtón pedig csak a külső kártyaolvasó kártyájának leolvasásával léphet ki. Ha a felhasználó belépését nem regisztrálták az 1-es ajtón, akkor nem tud kilépni a 2-es ajtón. Másodszor sem léphet be a felhasználó, ha a kilépését nem regisztrálták.

Megjegyzés: Az ajtó csak a kártya leolvasásával nyitható az 1. zónához. Az összes többi 1. és 2. zóna hozzáférési mód érvénytelen.

Hibaelhárítás

Probléma	Ok	Megoldás
A kártyaolvasási távolság túl rövid	Alacsony kártyaminőség	Használjon eredeti kártyákat
PIN beállítási problémák	1. A PIN kód nem felel meg a szabványnak 2. Kártyaolvasási módban van, állítsa be a jelszót	1. A PIN kód első számjegye 1 vagy 2 lehet, a zónától függően. 2. A PIN-kód nem lehet 1234. A PIN-kódnak 4 vagy 6 számjegyből kell állnia.

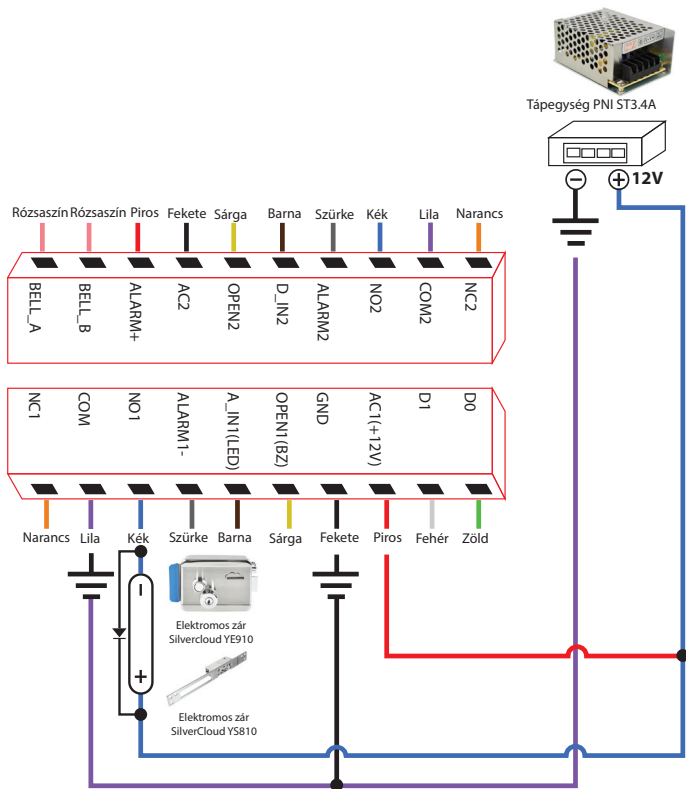
<p>A PIN kód nem nyitja ki az ajtót</p>	<p>1. 1234-es PIN kódot használt 2. A beállított hozzáférési mód nem teszi lehetővé a PIN hozzáférést</p>	<p>1. Módosítsa a PIN-kódot. 2. Változtassa meg a hozzáférési módot: kártya vagy PIN.</p>
<p>A kártya elolvasása után nincs válasz</p>	<p>A billentyűzet nincs készenléti állapotban, lehet programozási módban</p>	<p>Nyomja meg a * gombot, a LED villog. A billentyűzet készenléti üzemmódban van.</p>
<p>A billentyűzet nem világít</p>	<p>Hibás billentyűzet beállítások</p>	<p>1. Kapcsolja be vagy be a gomb háttérvilágítását. Automatikus módban a gombok csak lenyomásuk után világítanak, és 30 másodpercig világítanak.</p>
<p>Érvénytelen rendszergazdai kód</p>	<p>Elfelejtette a rendszergazdai kódot</p>	<p>Állítsa vissza a készüléket. Az adminisztrátori kód visszatér a 999999-re. A visszaállítással a felhasználói adatok nem törlődnek.</p>

Állítsa vissza a rendszergazdai kódot

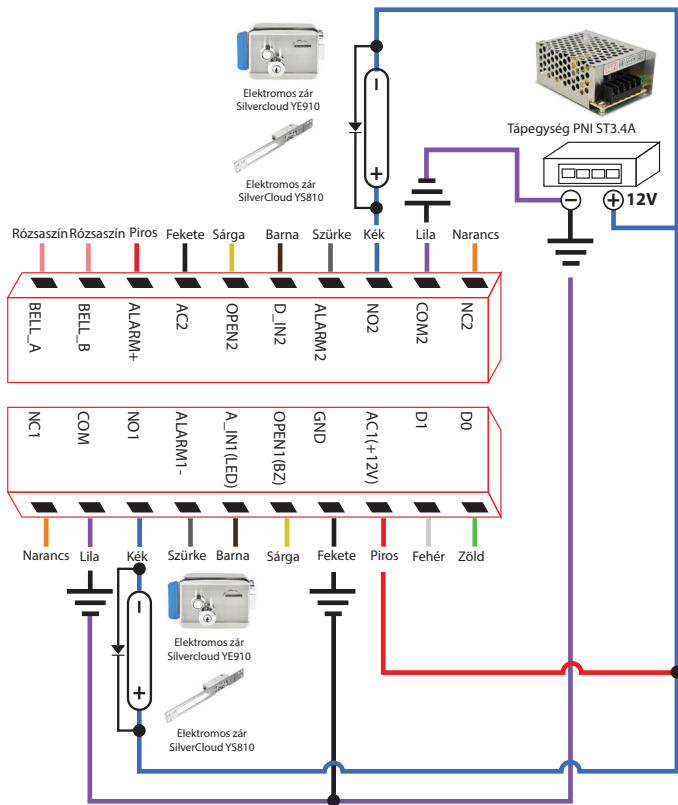
1. Kapcsolja ki a beléptető billentyűzet tápellátását.
2. Tartsa lenyomva a # gombot, miközben újraindítja a tápellátást.
3. Miután meghallotta két Di . hangot, engedje fel a # gombot.
4. A billentyűzet visszaállt a gyári beállításokra. A rendszergazdai jelszó visszatér a 999999-re. A felhasználói adatok nem törlődnek.

Csatlakozási példák egy és két ajtóhoz

Beléptető egy ajtóhoz Silvercloud YE910 vagy Silvercloud YS810 elektromágneses zárral és PNI ST3.4A tápegységgel.



Beléptető két ajtóhoz Silvercloud YE910 vagy Silvercloud YS810 elektromágneses zárral és PNI ST3.4A tápegységgel.



Descrizione

PNI DK220 è un dispositivo di controllo accessi autonomo e lettore di prossimità. È dotato di due relè per il comando di due porte e supporta un massimo di 2000 utenti, ogni utente può avere un codice PIN e una carta di accesso. La tastiera può essere collegata a una chiave elettromagnetica, un sistema di allarme, un campanello, un pulsante di accesso o un sensore porta. Il dispositivo dispone di 7 modalità di funzionamento: lettore di carte Wiegand, controllo accessi per una porta, controllo accessi per due porte, controllo accessi con lettore di carte esterno per due porte, due unità interconnesse per due porte, anti-passback per una porta e due porte anti-passback.

Caratteristiche principali

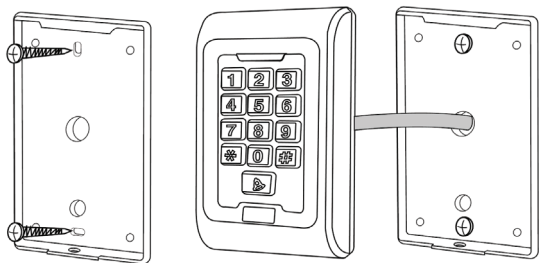
- Custodia in lega di alluminio con classe di resistenza all'acqua IP65
- Lettore di carte 125KHz integrato
- Tasti numerici illuminati. La luce dei tasti può essere programmata come segue: Normale ON, Normale OFF o Human-Approach ON (si accende quando rileva un movimento).
- Allarme manomissione, allarme attivazione sensore porta, allarme codice coercizione. Questo codice può essere utilizzato quando l'utente è costretto a minacciare di aprire la porta. Digitando questo codice la porta si aprirà ma attiverà un allarme silenzioso).
- Aggiungi ed elimina le carte con la carta amministratore.
- Registra ed elimina utenti tramite la tastiera.

Specifiche tecniche

Tensione di alimentazione	12V AC/DC
Consumo in standby	<25mA
Carico uscita elettroserratura	<1A
Carico uscita allarme	<1A
Carico uscita suoneria	<1A
Distanza di lettura della carta	massimo 40 mm
Capacità utente	massimo 2000
Carte compatibili	EM 125Khz/NASCO 125KHz
Formato di trasmissione della carta	26-37 bit Wiegand
Formato di trasmissione della tastiera	4 bit e 8 bit e numero di carta virtuale
Temperatura di lavoro	-26°C ~ +80°C

Installazione

Scegliere la posizione di installazione e praticare dei fori nel muro che corrispondano ai fori della staffa di montaggio. Fissare la staffa a parete con le viti incluse nella confezione. Passare i cavi attraverso la fessura al centro del supporto. Collegare i cavi. Isolare i cavi inutilizzati per evitare cortocircuiti.



Cablaggio

Zona 1		
BELL_A	Rosa	Pulsante campanello
BELL_B	Rosa	Pulsante campanello
ALARM+	Rosso	Connettore di allarme
AC2	Nero	INGRESSO CA
OPEN2	Giallo	Pulsante accesso
D_IN2	Marrone	Contatto porta
ALARM2-	Grigio	Allarme 2
NO2	Blu	Relè 2 NO
COM2	Viola	Relè 2 COM
NC2	Arancione	Relè 2 NC

Zona 2

D0	Verde	Uscita Wiegand D0
D1	Bianco	Uscita Wiegand D1
AC1	Rosso	AC1 (+ 12V)
GND	Nero	GND
OPEN1(LED)	Giallo	Pulsante di uscita (per LED verde)
D_IN1(BZ)	Marrone	Contatto porta (per cicalino)
ALARM1-	Grigio	Allarme 1
NO1	Blu	Relè 1 NO
COM1	Viola	Relè 1 Com
NC1	Arancione	Relè 1 NC

Avvisi sonori e luminosi

Status	LED	Buzzer
Pausa	Lampeggia rosso	
Tasto premuto		Di
Lettura della carta	Verde	Di.
Porta 1 aperta	Verde	Di.
Porta 2 aperta	Lampeggia verde	Di.
Operazione riuscita	Verde	Di.
Operazione fallita		DiDiDi
Inserimento PIN	Rosso	
Lettura carta e PIN	Rosso	
Lettura di più carte	Rosso	
Nel menu	Rosso	
Nelle impostazioni	Arancione	
Accesso con carta amministratore	Arancione	DiDi
Uscita con carta amministratore	Lampeggia rosso	Di.
Allarme	Il rosso lampeggia velocemente	Allarme

Guida rapida alla programmazione

1. Impostazioni amministratore

* Codice master #	00	<i>Inserisci il nuovo Codice master # Rpeti il nuovo Codice master #</i>	Cambia codice master. <i>Nota: il codice master predefinito è 999999. Il codice master deve avere tra 6 e 8 cifre.</i>
	01	<i>Leggi la carta</i>	Registrazione carta master per aggiungere carte. <i>Nota: Predefinito: zona 1.</i>
	02	<i>Leggi la carta</i>	Registrazione carta master per eliminare carte. <i>Nota: Predefinito: zona 1</i>
	03	<i>Leggi la carta</i>	Registrazione carta allarme “Duress” per la zona 1
	04	<i>Leggi la carta</i>	Registrazione carta allarme “Duress” per la zona 2

* Codice master #	05	<i>Inserisci il PIN di 8 cifre</i>	Inserisci il codice PIN “duress” per la zona1 Nota: La prima cifra del PIN deve essere 1 per la zona 1.
	06	<i>Inserisci il PIN di 8 cifre</i>	Inserisci il codice PIN “duress” per la zona2 Nota: La prima cifra del PIN deve essere 2 per la zona 2.
	07	0000 #	Elimina tutti gli utenti
	51	Master apre Serratura 1	
	52	Master apre Serratura 2	

Nota:

Il PIN “duress” e la carta “duress” possono essere utilizzati quando l’utente è costretto ad aprire la porta. Digitando questo codice o leggendo questa carta, la porta si aprirà ma allo stesso tempo invierà un segnale di allarme.

2. Impostazioni utente per Zona 1 e Zona 2

Aggiungi la carta utente

<i>* Codice master #</i>	<i>11</i> (per la Zona 1) <i>21</i> (per la Zona 2)	<i>Leggi la carta</i>
		<i>Inserisci l'ID # Leggi la carta</i>
		<i>Inserisci il numero della carta #</i>
		<i>Inserisci l'ID # Inserisci il numero della carta #</i>

Nota: Gli utenti possono essere aggiunti uno dopo l'altro senza uscire dalla modalità di programmazione. L'ID utente può contenere da 1 a 4 cifre, nell'intervallo 1 - 2000. 1, 01, 001 e 0001 tutti significano 1.

Aggiungi PIN utente

<i>* Codice master #</i>	<i>11</i> (per la Zona 1) <i>21</i> (per la Zona 2)	<i>Inserisci l'ID # Inserisci PIN #</i>
--------------------------	--	---

Nota: il PIN può avere da 4 a 6 cifre. La prima cifra deve essere 1 per la Zona 1 e 2 per la Zona 2. "1234" è riservato, non può essere impostato come PIN.

Elimina utente

<i>* Codice master #</i>	12 (per la Zona 1)	<i>Leggi la carta</i>
	22 (per la Zona 2)	<i>Inserisci l'ID #</i>
		<i>Inserisci il numero della carta #</i>

Nota: Gli utenti possono essere cancellati uno dopo l'altro senza uscire dalla modalità di programmazione.

Elimina tutti gli utenti

<i>* Codice master #</i>	07	0000 #
--------------------------	----	--------

Nota: questo comando elimina tutti gli utenti in Zona 1 e Zona 2.

Modalità di accesso

<i>* Codice master #</i>	13 (per la Zona 1)	0 #	Con carta
	23 (per la Zona 2)	1 #	Con carta + PIN
		2 #	Con carta or PIN (impostazione predefinita)

Ritardo porta aperta

<i>* Codice master #</i>	14 (per la Zona 1) 24 (per la Zona 2)	0 - 99 #	Impostazione predefinita 5
--------------------------	--	----------	----------------------------

Imposta le modalità di chiusura della porta

<i>* Codice master #</i>	15 (per la Zona 1)	0 #	Modalità a impulsi (predefinito). Ad ogni inserimento di un codice o lettura di una carta valida, la porta si aprirà e si chiuderà automaticamente dopo l'intervallo di tempo impostato (tra 0,05 sec. e 99 sec).
	25 (per la Zona 2)	1 #	Modalità di commutazione. Ad ogni inserimento di un codice o lettura di una carta valida, la porta si aprirà ma non si chiuderà fino a quando non verrà inserito nuovamente il codice o non verrà letta la carta.

Apri la porta con diverse carte

<i>* Codice master #</i>	16 (per la Zona 1) 26 (per la Zona 2)	1 - 10 #	Impostazione predefinita 1
--------------------------	--	----------	----------------------------

Nota: La porta si aprirà solo dopo che tutte le carte sono state lette. Ad esempio, per ordine * Codice master # 16 3 #, devi leggere 3 carte di fila per aprire la porta. Questa impostazione è utile solo se la tastiera è stata impostata sulla modalità di accesso alla carta.

Aggiungi carte utente in serie

<i>* Codice master #</i>	<i>17</i> (per la Zona 1) <i>27</i> (per la Zona 2)	<i>Inserisci l'ID #, Inserisci il numero della carta #, Inserisci quantità #</i>
--------------------------	--	--

Nota: i numeri delle carte devono essere consecutivi (tra 8 e 10 caratteri). La quantità della carta è compresa tra 1 e 2000.

3. Impostazioni di sistema

<i>* Codice master #</i>	30	0-15 #	Impostazione del codice dell'unità (Codice impianto). Predefinito: 0
	31	0 #	Letto re Wiegand
		1 #	Controllo accessi stand-alone a una porta (impostazione predefinita)
		2 #	Controllo accessi autonomo per due porte
		3 #	Con lettore esterno per due porte
		4 #	Due unità interconnesse per due porte (protezione in caso di apertura di più porte)
<i>* Codice master #</i>	31	5 #	Anti-passback per una porta
		6 #	Anti-passback per due porte
	32	26-37 #	Impostazione formato Wiegand 26 34 37. Predefinito 26
	33	0-2 #	Impostazione formato di trasmissione da tastiera: 0 1 2 Dopo il ripristino, questa impostazione rimane invariata.

* Codice master #	34	1-3 #	Imposta la durata della sveglia (impostazione predefinita 1 minuto) Dopo il ripristino, questa impostazione rimane invariata.
	35	0 #	Modalità di sicurezza 1. Modalità normale. (impostazione predefinita)
		1 #	Modalità di sicurezza 2. Se viene inserito il codice sbagliato o viene letta una carta non valida per 10 volte di seguito entro 10 minuti, come precauzione di sicurezza, il sistema si spegne.

* Codice master #	35	2 #	Modalità di sicurezza 3. Modalità di allarme. In caso di digitazione del codice errato o lettura di una carta non valida per 10 volte consecutive entro 10 minuti, a scopo precauzionale, verrà attivato l'allarme esterno (se collegato) e il buzzer integrato nella tastiera.
----------------------	----	-----	--

4. Impostazioni utente opzionali

* Codice master #	41	0 #	Buzzer disattivato. Il buzzer rimane attivo solo quando il dispositivo entra in modalità programmazione.
		1 #	Suono tasti attivo (impostazione predefinita)
	42	0 #	Retroilluminazione tasti disattivata
		1 #	Retroilluminazione tasti accesa
		2 #	Modalità automatica. Normalmente, la luce del tasto è spenta ma si accende quando viene rilevata la presenza umana.

* Codice master #	43	0 #	LED spento quando il dispositivo è in standby.
		1 #	Il LED lampeggia quando il dispositivo è in modalità standby. (impostazione predefinita)

Note importanti

1. Il codice master deve avere 6-8 cifre.
2. Il codice “coercizione” deve avere 8 cifre. La prima cifra del codice deve essere 1 per la Zona 1 e 2 per la Zona 2.
3. Il PIN utente deve avere 4-6 cifre. La prima cifra del PIN deve essere 1 per la Zona 1 e 2 per la Zona 2.
4. L’ID utente può essere qualsiasi numero compreso tra 1 e 2000.

5. Il numero della carta deve avere da 8 a 10 cifre. Se il numero della carta contiene meno di 8 cifre, aggiungere 0 davanti al codice.
6. Tempo di ritardo porta aperta: tra 0 e 99 secondi. 0 = 50 ms
7. Quando una carta utente è registrata nel dispositivo, il dispositivo genererà automaticamente un PIN 1234 che non può sbloccare la porta.
8. Se viene immesso un PIN principale non valido, il dispositivo entra in standby dopo 5 secondi. Se viene immesso un PIN principale valido, il dispositivo entra in modalità standby dopo 30 secondi.
9. Quando si utilizza la tastiera, premendo il tasto # si conferma il comando da tastiera eseguito in precedenza. Quando si aggiungono o si eliminano carte una dopo l'altra, la pressione del tasto # indica la fine del ciclo, mentre la pressione del tasto * indica l'uscita da questa operazione.
10. Quando si aggiungono carte in serie, il dispositivo assegna automaticamente un numero ID e un numero carta. Il numero identificativo e il numero della carta aumentano automaticamente con ogni carta aggiunta, fino ad un massimo di 2000.
11. La modalità di funzionamento e il formato di trasmissione della tastiera sono impostati in fabbrica. L'utente può modificare queste impostazioni secondo necessità. Dopo aver ripristinato il dispositivo, questa impostazione rimane invariata.
12. Dopo aver registrato con successo gli utenti nella Zona 1, il LED diventa verde. Dopo aver registrato con successo gli utenti nella Zona 2, il LED verde lampeggia.

5. Operazioni con le carte master

Aggiungi utente per la Zona 1

Leggi la carta master per aggiungere carte, quindi Leggi le carte utente una dopo l'altra e infine Leggi di nuovo la carta master.

Elimina utente per la Zona 1

Leggi la carta master per eliminare carte, quindi Leggi le carte utente una dopo l'altra e infine Leggi di nuovo la carta master.

6. Operazioni dell'utente

Modalità di accesso

Con carta

Leggi la carta. La serratura si sbloccherà.

Se hai impostato più carte per l'apertura della porta (tra 2 e 10), leggi tutte le carte una dopo l'altra entro 5 secondi, dopodiché la serratura si sbloccherà.

Con carta + PIN

Leggi la carta, Immettere il PIN (4 o 6 cifre) +#. La serratura si sbloccherà.

Con carta o PIN

Leggi la carta. Immettere il PIN (4 o 6 cifre) +#. La serratura si sbloccherà il PIN (4 o 6 cifre) +#. La serratura si sbloccherà.

Modificare il PIN senza entrare in modalità di programmazione

** leggi la carta utente, inserisci il vecchio PIN #, inserisci il nuovo PIN #
ripeti il nuovo PIN*

o

** Inserisci l'ID # Digita il vecchio PIN #, Digita il nuovo PIN # ripeti il
nuovo PIN*

Nota: Il PIN per la Zona 1 deve iniziare con 1 e il PIN per la Zona 2 deve iniziare con 2.

7. Funzione di allarme

Allarme manomissione

Se il dispositivo viene disassemblato da furto con scasso, suoneranno il buzzer interno e l'allarme esterno (se collegato).

Allarme porta aperta

Se è stato collegato un sensore porta cablato alla tastiera di controllo accessi e questo sensore si attiverà, suoneranno il cicalino interno e l'allarme esterno (se collegato).

Per disattivare l'allarme:

Leggi la carta utente o la carta principale, oppure inserisci il PIN principale.

Se non si esegue alcuna operazione, l'allarme si spegne automaticamente dopo 1 minuto.

Allarme “Duress”

Se si legge la carta “duress” o si digita il codice PIN “duress” su Zona 1 o Zona 2, la serratura si aprirà e, contemporaneamente, scatterà l’allarme esterno (se connesso). Il cicalino interno non verrà attivato.

8. Modalità operative

Letto di carte Wiegand

In questa modalità la tastiera funziona come un lettore di carte collegato a un dispositivo di controllo accessi.

Ordini supportati:

- Cambia PIN principale
- Imposta codice struttura
- Impostazione del formato di trasmissione della carta
- Impostazione del formato di trasmissione da tastiera
- Impostazioni opzionali
- Allarme manomissione

Controllo accessi autonomo per una singola porta

In questa modalità, la tastiera apre una singola porta. La porta può essere aperta Con carta o PIN o carta + PIN. La tastiera supporta il collegamento di un lettore di carte esterno o di un pulsante di accesso per uscire dall’edificio.

Controllo accessi autonomo per due porte

In questa modalità, la tastiera può controllare due porte. Leggi la carta oppure Inserisci il PIN per la Zona 1 e si aprirà la porta 1. Leggi la carta oppure Inserisci il codice PIN per la Zona 2 e la porta 2 si aprirà.

Con lettore di carte esterno per aprire due porte

In questa modalità, la tastiera consente l'accesso alla porta 1 e il lettore di carte esterno consente l'accesso alla porta 2.

Leggi la carta oppure Digita il codice per la Zona 1 sulla tastiera controllo accessi. La porta 1 si aprirà. Leggi la carta oppure Inserisci il codice per la Zona 2 sul lettore di carte esterno. La porta 2 si aprirà.

Due dispositivi interconnessi per aprire due porte

Questa modalità è più adatta per luoghi come banche, carceri o per situazioni che richiedono un livello di sicurezza avanzato.

Solo dopo la chiusura della porta 2 Leggi la carta o Digita il codice sulla tastiera per aprire la porta 1. E solo dopo la chiusura della porta 1 Leggi la carta o Digita il codice sul lettore di carte per aprire la porta 2.

Anti-passback per una singola porta

In questa modalità di funzionamento, la tastiera deve essere installata all'esterno per consentire l'accesso all'interno dell'edificio, e il lettore di carte esterno deve essere installato all'interno per consentire l'uscita dall'edificio.

Se l'ingresso dell'utente nell'edificio non è stato registrato, l'utente non può uscire leggendo la carta sul lettore di carte. Inoltre, l'utente non può entrare una seconda volta nell'edificio se la sua uscita non è stata registrata.

Nota: La porta può essere aperta solo leggendo la carta per la Zona 1. Tutte le altre modalità di accesso Zona 1 e Zona 2 non sono valide.

Anti-passback per due porte

In questa modalità, la tastiera sulla porta 1 è l'unità principale anti-passback e il lettore di carte esterno sulla porta 2 è l'unità secondaria anti-passback. Si crea così un sistema anti-passback adatto all'installazione nei parcheggi.

L'utente può entrare nell'edificio dalla porta 1 leggendo la carta sulla tastiera di controllo accessi e può uscire solo dalla porta 2 leggendo la carta sul lettore di carte esterno. Se l'ingresso dell'utente non è stato registrato sulla porta 1, non potrà uscire sulla porta 2. Inoltre, l'utente non può entrare una seconda volta se la sua uscita non è stata registrata.

Nota: La porta può essere aperta solo leggendo la carta per la Zona 1. Tutte le altre modalità di accesso Zona 1 e Zona 2 non sono valide.

Risoluzione dei problemi

Problema	Causa	Soluzione
Distanza di lettura della carta troppo corta	Bassa qualità della carta	Usa le carte originali
Problemi di impostazione del PIN	1. Il PIN non è conforme allo standard 2. Sei in modalità di lettura della carta, imposta la password	1. La prima cifra del PIN deve essere 1 o 2, a seconda della Zona. 2. Il PIN non deve essere 1234. Il PIN deve essere lungo 4 o 6 cifre.

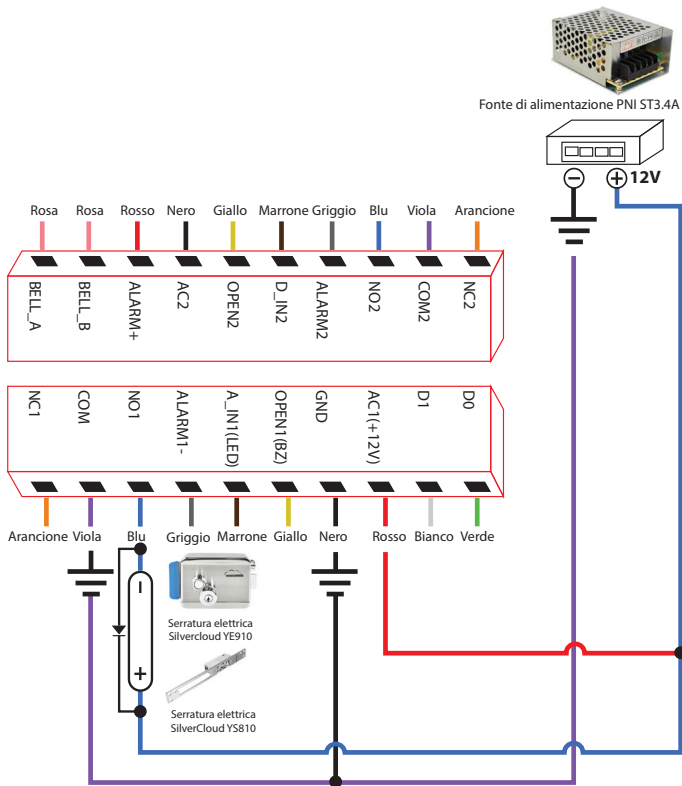
<p>Il PIN non apre la porta</p>	<ol style="list-style-type: none"> 1. Hai utilizzato il PIN 1234 2. La modalità di accesso impostata non consente l'accesso tramite PIN 	<ol style="list-style-type: none"> 1. Modifica il tuo PIN. 2. Modificare la modalità di accesso: carta o PIN.
<p>Nessuna risposta dopo aver letto la carta</p>	<p>La tastiera non è in standby, può essere in modalità programmazione</p>	<p>Premere il tasto *, il LED lampeggia. La tastiera è ora in modalità standby.</p>
<p>La tastiera non si accende</p>	<p>Impostazioni tastiera errate</p>	<ol style="list-style-type: none"> 1. Attivare o attivare la retroilluminazione dei tasti. In modalità automatica, i tasti si accendono solo dopo essere stati premuti e rimangono accesi per 30 secondi.
<p>Codice master non valido</p>	<p>Hai dimenticato il codice master</p>	<p>Ripristina il dispositivo. Il codice master torna a 999999. Con il reset i dati dell'utente non vengono cancellati.</p>

Ripristino del codice master

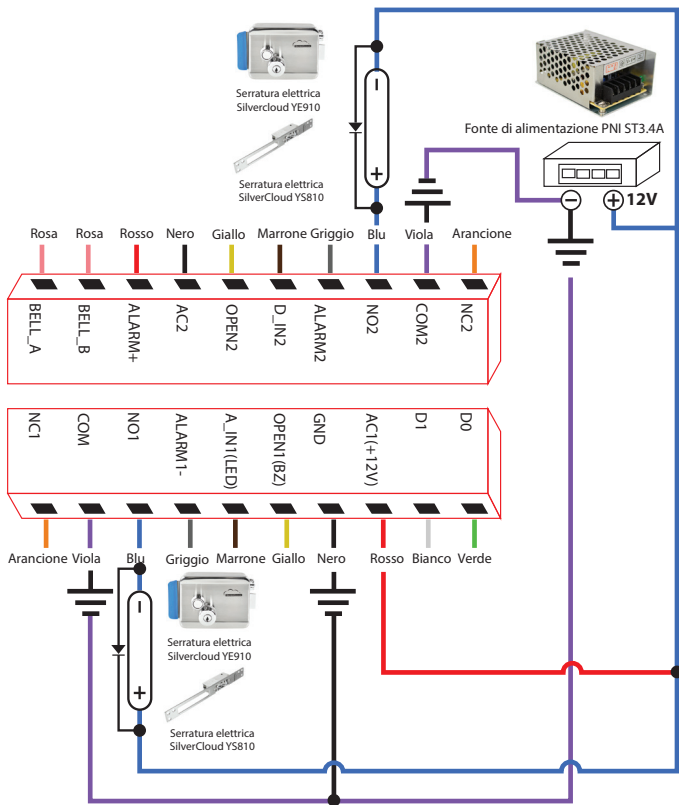
1. Spegner l'alimentazione alla tastiera di controllo accessi.
2. Tenere premuto il tasto # durante il riavvio dell'alimentazione.
3. Dopo aver ascoltato due suoni Di ., rilasciare il tasto #.
4. La tastiera è tornata alle impostazioni di fabbrica. La password principale torna a 999999. I dati dell'utente non sono stati cancellati.

Esempi di collegamento per una e due porte

Controllo accessi per una porta con serratura elettromagnetica Silvercloud YE910 o Silvercloud YS810 e alimentatore PNI ST3.4A.



Controllo accessi per due porte con serratura elettromagnetica Silvercloud YE910 o Silvercloud YS810 e alimentatore PNI ST3.4A.



Beschrijving

PNI DK220 is een stand-alone toegangscontrole-apparaat en proximity-lezer. Het is uitgerust met twee relais voor tweedeursbesturing en ondersteunt maximaal 2000 gebruikers, elke gebruiker kan beschikken over een pincode en een toegangskaart. Het toetsenbord kan worden aangesloten op een elektromagnetische sleutel, een alarmsysteem, een deurbel, een toegangsknop of een deursensor.

Het apparaat heeft 7 bedrijfsmodi: Wiegand-kaartlezer, toegangscontrole voor één deur, toegangscontrole voor twee deuren, toegangscontrole met externe kaartlezer voor twee deuren, twee onderling verbonden units voor twee deuren, anti-passback voor één deur en tweedeurs anti-passback.

Belangrijkste kenmerken

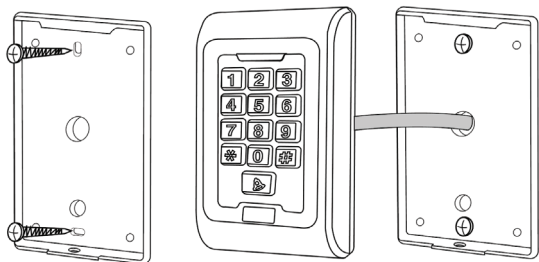
- Behuizing van aluminiumlegering met IP65 waterbestendigheidsklasse
- Ingebouwde 125KHz kaartlezer
- Verlichte numerieke toetsen. Het toetslampje kan als volgt worden geprogrammeerd: Normaal AAN, Normaal UIT of Menselijk naderen AAN (licht op wanneer het beweging detecteert).
- Sabotage alarm, deursensor trigger alarm, duresscode alarm (Deze code kan worden gebruikt wanneer de gebruiker wordt gedwongen om te dreigen de deur te openen. Wanneer u deze code typt, gaat de deur open maar activeert een stil alarm).
- Kaarten toevoegen en verwijderen met de beheerderskaart.
- Registreer en verwijder gebruikers met sleutels.

Technische specificaties

Voedingsspanning:	12V AC/DC
Stand-by verbruik	<25mA
Uitgangsbelasting elektrisch slot	<1A
Belasting alarmuitgang	<1A
Uitgangsbelasting deurbel	<1A
Kaartleesafstand	maximaal 40 mm
Gebruikerscapaciteit	maximaal 2000
Compatibele kaarten	EM 125KHz/HID 125KHz
Indeling kaartoverdracht:	26-37 bit Wiegand
Verzendformaat toetsenbord	4 bit en 8 bit en virtueel kaartnummer
Werktemperatuur	-26°C ~ +80°C

Installatie

Kies de installatielocatie en maak gaten in de muur die overeenkomen met de gaten in de montagebeugel. Zet de muurbeugel vast met de meegeleverde schroeven. Leid de kabels door de gleuf in het midden van de houder. Sluit de kabels aan. Isoleer ongebruikte kabels om kortsluiting te voorkomen.



Bedrading

Zone 1		
BELL_A	Roze	Deurbel knop
BELL_B	Roze	Deurbel knop
ALARM+	Rood	Alarmconnector
AC2	Zwart	AC-INGANG
OPEN2	Geel	Toegangsknop
D_IN2	Bruin	Deurcontact
ALARM2-	Grijs	Alarm 2
NO2	Blauw	Relais 2 NO
COM2	Purper	Relais 2 COM
NC2	Oranje	Relais 2 NC

Zone 2

D0	Groente	Wiegand-uitgang D0
D1	Wit	Wiegand-uitgang D1
AC1	Rood	AC1 (+ 12V)
GND	Zwart	GND
OPEN1(LED)	Geel	Toegangsknop (voor groene LED)
D_IN1(BZ)	Bruin	Deurcontact (voor zoemer)
ALARM1-	Grijs	Alarm 1
NO1	Blauw	Relais 1 NO
COM1	Purper	Relais 1 Com
NC1	Oranje	Relais 1 NC

Hoorbare en lichtgevende waarschuwingen

Toestand	LED	Buzzer
Stand-by	Rood knippert	
Druk op toets		Di
Kaart lezen	Groente	Di.
Deur 1 open	Groente	Di.
Deur 2 open	Groen knippert	Di.
Succesvolle operatie	Groente	Di.
Operatie mislukt		DiDiDi
Pin-invoer	Rood	
Kaart & PIN lezen	Rood	
Meerdere kaarten lezen	Rood	
Onder menu	Rood	
Onder instellingen	Oranje	
Beheerderskaart invoeren	Oranje	DiDi
Beheerderskaart afsluiten	Rood knippert	Di.
Alarm	Rood knippert snel	Alarm

Snelle programmeergids

1. Beheerdersinstellingen

<i>* Master code #</i>	00	<i>Voer de nieuwe Mastercode in # Herhaal de nieuwe Mastercode #</i>	Mastercode wijzigen. <i>Opmerking: de standaard mastercode is 999999. De mastercode moet tussen 6 en 8 cijfers hebben.</i>
	01	<i>Lees de kaart</i>	Mastercard- registratie voor het toevoegen van kaarten.
	02	<i>Lees de kaart</i>	Mastercard- registratie voor het verwijderen van kaarten.
	03	<i>Lees de kaart</i>	“Duress” alarmkaart registratie voor zone 1
	04	<i>Lees de kaart</i>	“Duress” alarmkaart registratie voor zone 2

* Master code #	05	<i>Voer de 8-cijferige pincode in</i>	Voer de “duress”-pincode in voor zone1 Opmerking: het eerste cijfer van de pincode moet 1 zijn voor zone 1.
	06	<i>Voer de 8-cijferige pincode in</i>	Voer de “duress”-pincode in voor zone2 Opmerking: het eerste cijfer van de pincode moet 2 zijn voor zone 2.
	07	0000 #	Alle gebruikers verwijderen
	51	Meester open slot 1	
	52	Meester open slot 2	

Opmerking:

De “duress”-pincode en de “duress”-kaart kunnen worden gebruikt wanneer de gebruiker wordt gedwongen om de deur te openen. Bij het typen van deze code of het lezen van deze kaart gaat de deur open maar geeft tegelijkertijd een alarmsignaal af.

2. Gebruikersinstellingen voor Zone 1 en Zone 2

Gebruikerskaart toevoegen

<i>* Master code #</i>	11 (voor zone 1)	<i>Lees de kaart</i>
		<i>Voer ID in # Lees de kaart</i>
	21 (voor zone 2)	<i>Voer kaartnummer in #</i>
		<i>Voer ID in # Voer kaartnummer in #</i>

Opmerking: Gebruikers kunnen de een na de ander worden toegevoegd zonder de programmeermodus te verlaten. Gebruikers-ID kan 1 tot 4 cijfers bevatten, in het bereik 1 - 2000. 1, 01, 001 en 0001 betekent allemaal 1.

Gebruikerspincode toevoegen

<i>* Master code #</i>	11 (voor zone 1) 21 (voor zone 2)	<i>Voer ID in # Voer Pin-code in #</i>
------------------------	--	--

Opmerking: de pincode kan 4 tot 6 cijfers hebben. Het eerste cijfer moet 1 zijn voor zone 1 en 2 voor zone 2. "1234" is gereserveerd, kan niet worden ingesteld als PIN.

Verwijder gebruiker

<i>* Master code #</i>	12 (voor zone 1)	Lees de kaart
	22 (voor zone 2)	Voer ID in #
		Voer kaartnummer in #

Opmerking: gebruikers kunnen na elkaar worden verwijderd zonder de programmeermodus te verlaten.

Alle gebruikers verwijderen

<i>* Master code #</i>	07	0000 #
------------------------	----	--------

Opmerking: met deze opdracht kunnen alle gebruikers in Zone 1 en Zone 2 verwijderd.

Toegangsmodi

<i>* Master code #</i>	13 (voor zone 1)	0 #	Per kaart
	23 (voor zone 2)	1 #	Per kaart + PIN
		2 #	Per kaart or PIN (standaardinstelling)

Open door delay

<i>* Master code #</i>	14 (voor zone 1) 24 (voor zone 2)	0 - 99 #	Standaardinstelling 5
------------------------	--	----------	--------------------------

Modi voor het sluiten van deuren instellen

<i>* Master code #</i>	15 (voor zone 1) 25 (voor zone 2)	0 #	Pulsmodus (standaardinstelling). Elke keer dat een code wordt ingevoerd of een geldige kaart wordt gelezen, zal de deur automatisch openen en sluiten na het ingestelde tijdsinterval (tussen 0,05 sec. en 99 sec).
		1 #	Schakel modus. Elke keer dat een code wordt ingevoerd of een geldige kaart is gelezen, zal de deur openen maar niet sluiten totdat de code opnieuw wordt ingevoerd of de kaart wordt gelezen.

Open de deur met meerdere kaarten

<i>* Master code #</i>	16 (voor zone 1) 26 (voor zone 2)	1 - 10 #	Standaardinstelling 1
------------------------	--	----------	--------------------------

Let op: De deur gaat pas open nadat alle kaarten zijn gelezen.

Bijvoorbeeld bij bestelling * Mastercode # 16 3 #, moet je 3 kaarten achter elkaar lezen om de deur te openen. Deze instelling is alleen nuttig als u het toetsenbord in de kaarttoegangsmodus hebt gezet.

Gebruikerskaarten in serie toevoegen

<i>* Master code #</i>	<i>17</i> (voor zone 1) <i>27</i> (voor zone 2)	<i>Voer ID in #, Voer kaartnummer in #, Voer aantal in #</i>
------------------------	--	--

Opmerking: kaartnummers moeten opeenvolgend zijn (tussen 8 en 10 tekens). Het aantal kaarten ligt tussen 1 en 2000.

3. Systeem instellingen

<i>* Master code #</i>	30	0-15 #	De unitcode instellen (Faciliteitscode). Standaard: 0
	31	0 #	Lezer Wiegand
		1 #	Eendeurs stand-alone toegangscontrole (standaardinstelling)
		2 #	Stand-alone toegangscontrole voor twee deuren
		3 #	Met externe lezer voor twee deuren
		4 #	Twee onderling verbonden units voor twee deuren (bescherming bij het openen van meerdere deuren)
<i>* Master code #</i>	31	5 #	Anti-passback voor een deur
		6 #	Anti-passback voor twee deuren
	32	26-37 #	Instelling Wiegand-formaat 26 34 37. Standaard 26
	33	0-2 #	Instelling transmissieformaat toetsenbord: 0 1 2 Na het resetten blijft deze instelling ongewijzigd

<i>* Master code #</i>	34	1-3 #	Alarmduur instellen (standaardinstelling 1 minuut) Na het resetten blijft deze instelling ongewijzigd .
	35	0 #	Veilige modus 1. Normale modus. (standaardinstelling)
		1 #	Veilige modus 2. Als de verkeerde code wordt ingevoerd of een ongeldige kaart binnen 10 minuten 10 keer achter elkaar wordt gelezen, wordt het systeem uit veiligheidsoverwegingen uitgeschakeld.

<i>* Master code #</i>	35	2 #	Veiligheidsmodus 3. Alarmmodus. Als de verkeerde code wordt ingevoerd of een ongeldige kaart binnen 10 minuten 10 keer achter elkaar wordt gelezen, wordt uit voorzorg het externe alarm (indien aangesloten) en de in het toetsenbord ingebouwde zoemer geactiveerd.
------------------------	----	-----	--

4. Optional user settings

<i>* Master code #</i>	41	0 #	Zoemer uit. De zoemer blijft alleen actief wanneer het apparaat naar de programmeermodus gaat.
		1 #	Actief toetsgeluid (standaardinstelling)
	42	0 #	Achtergrondverlichting toets uit
		1 #	Achtergrondverlichting toets aan
		2 #	Automatische modus. Normaal gesproken is het toetslampje uit, maar gaat het branden wanneer menselijke aanwezigheid wordt gedetecteerd.

<i>* Master code #</i>	43	0 #	LED uit wanneer het apparaat in stand-by staat.
		1 #	De LED knippert wanneer het apparaat in de standby-modus staat. (standaardinstelling)

Belangrijke aantekeningen

1. De mastercode moet uit 6-8 cijfers bestaan.
2. De code “duress” moet uit 8 cijfers bestaan. Het eerste cijfer van de code moet 1 zijn voor zone 1 en 2 voor zone 2.
3. De gebruikerspincode moet 4-6 cijfers hebben. Het eerste cijfer

- van de pincode moet 1 zijn voor zone 1 en 2 voor zone 2.
4. Gebruikers-ID kan elk getal tussen 1 en 2000 zijn.
 5. Het kaartnummer moet tussen de 8 en 10 cijfers hebben. Als het kaartnummer minder dan 8 cijfers bevat, voeg dan 0 toe voor de code.
 6. Vertragingstijd deur: tussen 0 en 99 seconden. 0 = 50mS
 7. Wanneer een gebruikerskaart in het apparaat is geregistreerd, genereert het apparaat automatisch een pincode 1234 die de deur niet kan ontgrendelen.
 8. Als een ongeldige master-PIN wordt ingevoerd, gaat het apparaat na 5 seconden in stand-by. Als een geldige master-PIN wordt ingevoerd, gaat het apparaat na 30 seconden naar de stand-bymodus.
 9. Bij gebruik van het toetsenbord bevestigt het indrukken van de #-toets het eerder uitgevoerde toetscommando. Als u de ene na de andere kaart toevoegt of verwijdert, geeft het indrukken van de #-toets het einde van de cyclus aan en door op de *-toets te drukken, wordt het verlaten van deze handeling aangegeven.
 10. Wanneer u kaarten in serie toevoegt, wijst het apparaat automatisch een ID-nummer en een kaartnummer toe. Het ID-nummer en het kaartnummer worden automatisch verhoogd met elke toegevoegde kaart, tot een maximum van 2000.
 11. De bedrijfsmodus en het transmissieformaat van het toetsenbord zijn in de fabriek ingesteld. De gebruiker kan deze instellingen naar behoefte wijzigen. Na het resetten van het apparaat blijft deze instelling ongewijzigd.
 12. Na het succesvol registreren van gebruikers in Zone 1, wordt de LED groen. Na het succesvol registreren van gebruikers in Zone 2, knippert de groene LED.

5. Masterkaartbewerkingen

Gebruiker toevoegen voor zone 1

Lees de master-add-kaart, lees vervolgens de gebruikerskaarten een voor de andere, en lees ten slotte de master-add-kaart opnieuw.

Gebruiker verwijderen voor zone 1

Lees de master delete-kaart, lees dan de gebruikerskaarten een voor de andere, en lees ten slotte de master delete-kaart opnieuw.

6. Gebruikersbewerkingen

Per kaart

Lees de kaart. Het slot wordt ontgrendeld.

Als je meerdere kaarten voor de deuropening hebt ingesteld (tussen 2 en 10), lees dan binnen 5 seconden alle kaarten achter elkaar uit, waarna het slot ontgrendelt.

Per kaart + PIN

Lees de kaart, Voer de pincode in (4 of 6 cijfers) +#. Het slot wordt ontgrendeld.

Per kaart of PIN

Lees de kaart. Het slot wordt ontgrendeld. Of voer de pincode +# in. Het slot wordt ontgrendeld.

Pincode wijzigen zonder de programmeermodus te openen

** lees gebruikerskaart, voer oude pincode in # in, voer nieuwe pincode in # herhaal nieuwe pincode*

of

** Voer ID in nummer # Voer oude pincode in #, Voer nieuwe pincode in # herhaal nieuwe pincode*

Let op: De pincode voor zone 1 moet beginnen met 1, en de pincode voor zone 2 moet beginnen met 2.

7. Alarmfunctie:

Sabotage alarm

Als het apparaat door inbraak wordt gedemonteerd, gaan de interne zoemer en het externe alarm (indien aangesloten) af.

Open deur alarm

Als u een bedrade deursensor hebt aangesloten op het toegangscontroletoetsenbord en deze sensor wordt geactiveerd, zullen de interne zoemer en het externe alarm (indien aangesloten) afgaan.

Het alarm uitschakelen:

Lees de gebruikerskaart of masterkaart, of voer de masterpincode in.

Als u geen handeling uitvoert, wordt het alarm na 1 minuut automatisch uitgeschakeld.

“Duress” alarm

Als de “duress”-kaart wordt gelezen of de “duress”-pincode wordt ingevoerd in Zone 1 of Zone 2, gaat het slot open en wordt tegelijkertijd het externe alarm geactiveerd (indien aangesloten). De interne zoemer wordt niet geactiveerd.

8. Bedrijfsmodi

Wiegand-kaartlezer

In deze modus functioneert het toetsenbord als een kaartlezer die is aangesloten op een toegangscontroleapparaat.

Ondersteunde bestellingen:

- Hoofdpincode wijzigen
- Faciliteitscode instellen
- Instelling kaartverzendingsformaat
- Instelling transmissieformaat toetsenbord
- Optionele instellingen
- Sabotage alarm

Stand-alone toegangscontrole voor een enkele deur

In deze modus opent het toetsenbord een enkele deur. De deur kan worden geopend Per kaart of PIN of kaart + PIN. Het toetsenbord ondersteunt het aansluiten van een externe kaartlezer of een toegangsknop om het gebouw te verlaten.

Stand-alone toegangscontrole voor twee deuren

In deze modus kan het toetsenbord twee deuren bedienen. Lees de kaart of Voer de pincode in voor zone 1 en deur 1 gaat open. Lees de

kaart of Voer de pincode in voor zone 2 en deur 2 gaat open.

Met externe kaartlezer om twee deuren te openen

In deze modus geeft het toetsenbord toegang voor deur 1 en de externe kaartlezer geeft toegang voor deur 2.

Lees de kaart of Voer de code voor zone 1 in op het toegangscontrole toetsenbord. Deur 1 gaat open. Lees de kaart of Voer de code voor zone 2 in op de externe kaartlezer. Deur 2 gaat open.

Twee onderling verbonden apparaten om twee deuren te openen

Deze modus is meer geschikt voor locaties zoals banken, gevangenissen of voor situaties die een geavanceerd beveiligingsniveau vereisen.

Pas nadat deur 2 is gesloten, Lees de kaart of Voer de code in op het toetsenbord om deur 1 te openen. En pas nadat deur 1 is gesloten, Lees de kaart of Voer de code in op de kaartlezer om deur 2 te openen.

Anti-passback voor een enkele deur

In deze bedrijfsmodus moet het toetsenbord buiten worden geïnstalleerd om toegang tot het gebouw mogelijk te maken, en de externe kaartlezer moet binnenshuis worden gemonteerd om de uitgang uit het gebouw mogelijk te maken.

Als de toegang van de gebruiker tot het gebouw niet is geregistreerd, kan de gebruiker het gebouw niet verlaten door de kaart op de kaartlezer te lezen. Ook kan de gebruiker het gebouw niet een tweede keer betreden als zijn uitgang niet is geregistreerd.

Opmerking: De deur kan alleen worden geopend door de kaart voor zone 1 te lezen. Alle andere toegangsmodi voor Zone 1 en Zone 2 zijn ongeldig.

Anti-passback voor twee deuren

In deze modus is het toetsenbord op deur 1 de anti-passback-mastereenheid en is de externe kaartlezer op deur 2 de secundaire anti-passback-eenheid. Zo ontstaat een anti-passbacksysteem dat geschikt is voor installatie op parkeerplaatsen.

De gebruiker kan het gebouw op deur 1 betreden door de kaart op het toetsenbord van de toegangscontrole te lezen en kan alleen verlaten op deur 2 door de kaart op de externe kaartlezer te lezen. Als de toegang van de gebruiker niet is geregistreerd bij deur 1, kan hij niet naar deur 2 gaan. Ook kan de gebruiker niet een tweede keer naar binnen als zijn uitgang niet is geregistreerd.

Opmerking: De deur kan alleen worden geopend door de kaart voor zone 1 te lezen. Alle andere toegangsmodi voor Zone 1 en Zone 2 zijn ongeldig.

Probleemoplossen

Probleem	Oorzaak	Oplossing
Kaartleesafstand te kort	Lage kaartkwaliteit	Gebruik originele kaarten
Problemen met pincode instellen	1. De pincode voldoet niet aan de norm 2. U bevindt zich in de kaartleesmodus, stel het wachtwoord in!	1. Het eerste cijfer van de pincode moet 1 of 2 zijn, afhankelijk van de Zone. 2. De pincode mag niet 1234 zijn. De pincode moet 4 of 6 cijfers lang zijn.

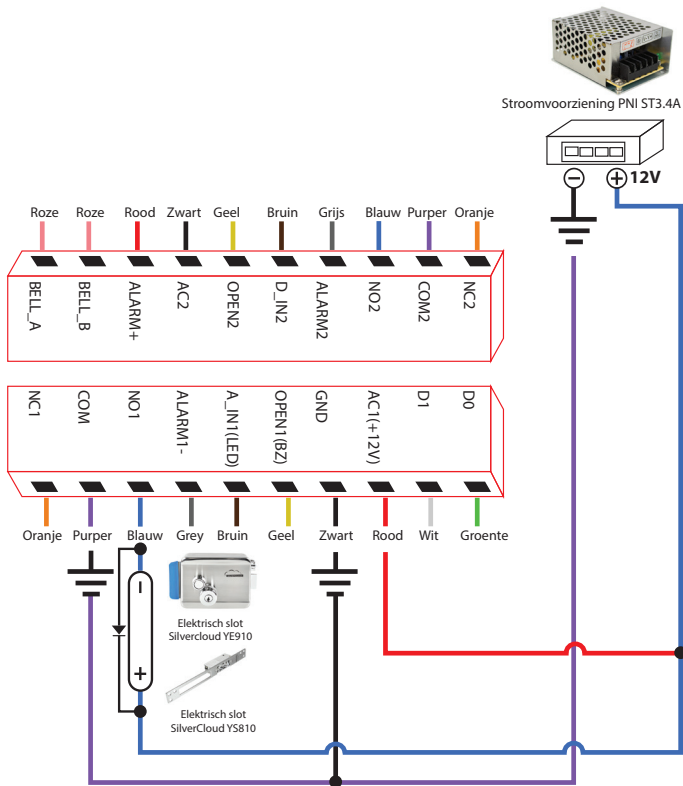
De pincode opent de deur niet	<ol style="list-style-type: none"> 1. U heeft pincode 1234 gebruikt 2. De ingestelde toegangsmodus staat geen PIN-toegang toe 	<ol style="list-style-type: none"> 1. Wijzig uw pincode. 2. Wijzig de toegangsmodus: kaart of pincode.
Geen antwoord na het lezen van de kaart	Het toetsenbord staat niet in standby, het kan in de programmeermodus staan	Druk op de * toets, de LED knippert. Het toetsenbord staat nu in de standby-modus.
Het toetsenbord licht niet op	Verkeerde toetsenbord instellingen	1. Zet de toetsverlichting op aan of aan. In de automatische modus lichten de toetsen pas op nadat ze zijn ingedrukt en blijven ze 30 seconden branden.
Ongeldige mastercode	Je bent de hoofdcode vergeten	Stel het apparaat opnieuw in. De mastercode keert terug naar 999999. Bij reset worden de gebruikersgegevens niet verwijderd.

Reset de mastercode

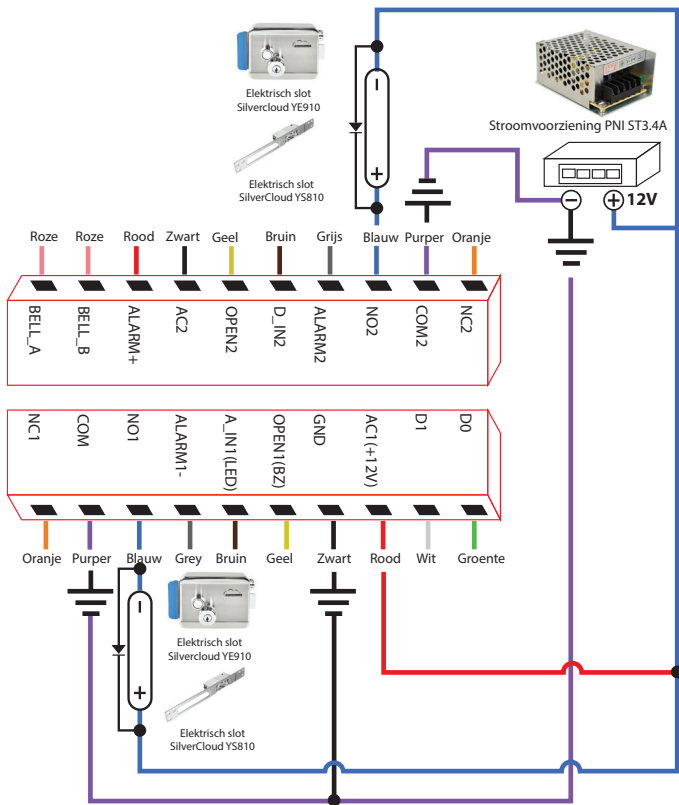
1. Schakel de stroom naar het toetsenbord voor toegangscontrole uit.
2. Houd de #-toets ingedrukt terwijl u de stroom opnieuw start.
3. Nadat u twee Di.-geluiden hebt gehoord, laat u de #-toets los.
4. Het toetsenbord is teruggekeerd naar de fabrieksinstellingen. Het hoofdwachtwoord keert terug naar 999999. De gebruikersgegevens zijn niet verwijderd.

Aansluitvoorbeelden voor één en twee deuren

Toegangscontrole voor één deur met Silvercloud YE910 of Silvercloud YS810 elektromagnetisch slot en PNI ST3.4A voeding.



Toegangscontrole voor twee deuren met Silvercloud YE910 of Silvercloud YS810 elektromagnetisch slot en PNI ST3.4A voeding.



Opis

PNI DK220 to samodzielne urządzenie kontroli dostępu i czytnik zbliżeniowy. Jest wyposażony w dwa przekaźniki do kontroli dwóch przejść i obsługuje maksymalnie 2000 użytkowników, każdy użytkownik może posiadać kod PIN i kartę dostępu.

Do klawiatury można podłączyć klucz elektromagnetyczny, system alarmowy, dzwonek, przycisk dostępu lub czujnik drzwi.

Urządzenie posiada 7 trybów pracy: czytnik kart Wiegand, kontrola dostępu dla jednych przejść, kontrola dostępu dla dwójga przejść, kontrola dostępu z zewnętrznym czytnikiem kart dla dwójga przejść, dwie połączone jednostki dla dwójga przejść, anti-passback dla jednych i dwójga przejść anti-passback.

Główne cechy

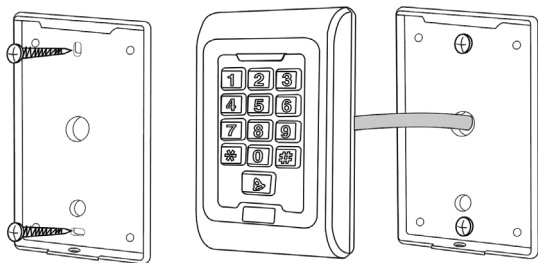
- Obudowa ze stopu aluminium o klasie wodoodporności IP65
- Wbudowany czytnik kart 125 KHz
- Podświetlane klawisze numeryczne. Światło klawisza można zaprogramować w następujący sposób: Normal ON, Normal OFF lub Human Approach ON (zapala się, gdy wykryje ruch).
- Alarm sabotażowy, alarm wywołania czujnika drzwi, alarm kodem pod duressem Ten kod może być użyty, gdy użytkownik jest zmuszony grozić otwarciem drzwi. Po wpisaniu tego kodu drzwi otworzą się, ale uruchomią cichy alarm).
- Dodawaj i usuwaj karty za pomocą karty administratora.
- Rejestruj i usuwaj użytkowników za pomocą kluczy.

Specyfikacja techniczna

Napięcie zasilania	12V AC/DC
Zużycie w trybie czuwania	<25mA
Obciążenie wyjściowe zamka elektrycznego	<1A
Obciążenie wyjścia alarmowego	<1A
Obciążenie wyjścia dzwonka	<1A
Odległość odczytu karty	maksymalnie 40 mm
Pojemność użytkownika	maksymalnie 2000
Kompatybilne karty	EM 125KHz/HID 125KHz
Format transmisji karty	26-37 bitów Wieganda
Format transmisji klawiatury	4-bitowy i 8-bitowy numer karty wirtualnej
Temperatura pracy	-26°C ~ +80°C

Instalacja

Wybierz miejsce instalacji i wykonaj otwory w ścianie, które pasują do otworów we wsporniku montażowym. Zamocuj wspornik ścienny za pomocą śrub dołączonych do opakowania. Przetnij kable przez szczelinę pośrodku uchwytu. Podłącz kable. Izoluj nieużywane kable, aby uniknąć zwarcia.



Okablowanie

Strefa 1		
BELL_A	Różowy	Przycisk dzwonka
BELL_B	Różowy	Przycisk dzwonka
ALARM+	Czerwony	Złącze alarmowe
AC2	Czarny	WEJŚCIE AC
OPEN2	Żółty	Przycisk dostępu
D_IN2	Brązowy	Kontakt drzwiowy
ALARM2-	Szary	Alarm 2
NO2	Niebieski	Przełącznik 2 NO
COM2	Fioletowy	Przełącznik 2 COM
NC2	Pomarańczowy	Przełącznik 2 NC

Strefa 2

D0	Zielony	Wyjście Wieganda D0
D1	Biały	Wyjście Wieganda D1
AC1	Czerwony	AC1 (+12V)
GND	Czarny	GND
OPEN1(LED)	Żółty	Przycisk dostępu (dla zielonej diody LED)
D_IN1(BZ)	Brązowy	Kontakt drzwiowy (dla brzęczyka)
ALARM1-	Szary	Alarm 1
NO1	Niebieski	Przełącznik 1 NO
COM1	Fioletowy	Przełącznik 1 Com
NC1	Pomarańczowy	Przełącznik 1 NC

Ostrzeżenia dźwiękowe i świetlne

Status	LED	Buzzer
Czekaj	Czerwony miga	
naciśnij klawisz		Di
Przeczytaj kartę	Zielony	Di.
Drzwi 1 otwarte	Zielony	Di.
Drzwi 2 otwarte	Zielony miga	Di.
Udana operacja	Zielony	Di.
Operacja nie powiodła się		DiDiDi
Wprowadzanie kodu PIN	Czerwony	
Przeczytaj kartę i kod PIN	Czerwony	
Odczyt wielu kart	Czerwony	
W menu	Czerwony	
W ustawieniach	Pomarańczowy	
Wprowadź kartę administratora	Pomarańczowy	DiDi
Wyjście z karty administratora	Czerwony miga	Di.
Alarm	Czerwony miga szybko	Alarm

Szybki przewodnik po programowaniu

1. Ustawienia administratora

* Kod główny #	00	<i>Wpisz nowy Kod główny # Powtórz nowy Kod główny #</i>	Zmień Kod główny. Uwaga: Wartość domyślna Kod główny to 999999. Kod główny musi mieć od 6 do 8 cyfr.
	01	<i>Przeczytaj kartę</i>	Rejestracja karty głównej do dodawania kart.
	02	<i>Przeczytaj kartę</i>	Rejestracja karty głównej do usuwania kart.
	03	<i>Przeczytaj kartę</i>	Rejestracja karty alarmowej „duress” dla strefy 1
	04	<i>Przeczytaj kartę</i>	Rejestracja karty alarmowej „duress” dla strefy 2

* Kod główny #	05	Wprowadź 8-cyfrowy kod PIN	Wprowadź kod PIN „duressu” dla strefy1 Uwaga: Pierwsza cyfra kodu PIN musi wynosić 1 dla strefy 1.
	06	Wprowadź 8-cyfrowy kod PIN	Wprowadź kod PIN „duressu” dla strefy 2 Uwaga: Pierwsza cyfra kodu PIN musi wynosić 2 dla strefy 2.
	07	0000 #	Usuń wszystkich użytkowników
	51	Otwórz zamek główny 1	
	52	Otwórz zamek główny 2	

Notatka:

PIN „duress” i karta „duress” mogą być użyte, gdy użytkownik zostanie zmuszony do otwarcia drzwi. Podczas wpisywania tego kodu lub odczytywania tej karty drzwi otworzą się, ale jednocześnie wyśle sygnał alarmowy.

2. Ustawienia użytkownika dla Strefy 1 i Strefy 2

Add user card

<i>* Kod główny #</i>	11	<i>Przeczytaj kartę</i>
	(dla strefy 1)	<i>Wpisz ID # Przeczytaj kartę</i>
	21	<i>Wpisz numer karty #</i>
	(dla strefy 2)	<i>Wpisz ID # Wpisz numer karty #</i>

Uwaga: Użytkowników można dodawać po kolei bez wychodzenia z trybu programowania. Identyfikator użytkownika może zawierać od 1 do 4 cyfr, w zakresie 1 - 2000. 1, 01, 001 i 0001 oznacza 1.

Dodaj kod PIN użytkownika

<i>* Kod główny #</i>	11 (dla strefy 1) 21 (dla strefy 2)	<i>Wpisz ID # Wpisz PIN #</i>
-----------------------	--	-------------------------------

Uwaga: PIN może mieć od 4 do 6 cyfr. Pierwsza cyfra musi być 1 dla strefy 1 i 2 dla strefy 2. „1234” jest zastrzeżona, nie może być ustawiana jako PIN.

Usuń użytkownika

<i>* Kod główny #</i>	12 (dla strefy 1)	Przeczytaj kartę
	22 (dla strefy 2)	Wpisz ID #
		Wpisz numer karty #

Uwaga: Użytkowników można usuwać jeden po drugim bez wychodzenia z trybu programowania.

Usuń wszystkich użytkowników

<i>* Kod główny #</i>	07	0000 #
-----------------------	----	--------

Uwaga: To polecenie usuwa wszystkich użytkowników w Strefie 1 i Strefie 2.

Tryby dostępu

<i>* Kod główny #</i>	13 (dla strefy 1)	0 #	Kartą
	23 (dla strefy 2)	1 #	Kartą + PIN
		2 #	Kartą lub PIN (ustawienia domyślne)

Opóźnienie otwarcia drzwi

<i>* Kod główny #</i>	14 (dla strefy 1) 24 (dla strefy 2)	0 - 99 #	Ustawienia domyślne 5
-----------------------	--	----------	-----------------------

Ustaw tryby zamykania drzwi

<i>* Kod główny #</i>	15 (dla strefy 1) 25 (dla strefy 2)	0 #	Tryb impulsowy (ustawienia). Za każdym razem, gdy zostanie wprowadzony kod lub odczytana ważna karta, drzwi otworzą się i zamkną automatycznie po upływie ustawionego czasu (od 0,05 s do 99 s).
		1 #	Przełącz tryb. Za każdym razem, gdy zostanie wprowadzony kod lub odczytana ważna karta, drzwi otworzą się, ale nie zamkną się, dopóki kod nie zostanie ponownie wprowadzony lub karta zostanie odczytana

Otwórz drzwi kilkoma kartami

<i>* Kod główny #</i>	16 (dla strefy 1) 26 (dla strefy 2)	1 - 10 #	Ustawienia domyślne 1
-----------------------	--	----------	-----------------------

Uwaga: Drzwi otworzą się dopiero po odczytaniu wszystkich kart.

Np. zamówieniem * Kod główny # 16 3 #, aby otworzyć drzwi trzeba przeczytać 3 kartki pod rząd. To ustawienie jest przydatne tylko wtedy, gdy klawiatura jest ustawiona na tryb dostępu do karty.

Dodaj karty użytkownika szeregowo

<i>* Kod główny #</i>	<i>17</i> (dla strefy 1) <i>27</i> (dla strefy 2)	<i>Wpisz ID #, Wpisz numer karty #, Wprowadź ilość #</i>
-----------------------	--	--

Uwaga: Numery kart muszą być następujące po sobie (od 8 do 10 znaków). Ilość kart wynosi od 1 do 2000.

3. Ustawienia systemowe

* Kod główny #	30	0-15 #	Ustawianie kodu jednostki (Facility Code). Domyślnie: 0
	31	0 #	Czytnik Wiegand
		1 #	Jednodrzwiowa samodzielna kontrola dostępu (ustawienia)
		2 #	Samodzielna kontrola dostępu dla dwojga drzwi
		3 #	Z czytnikiem zewnętrznym na dwoje drzwi
		4 #	Dwie połączone jednostki dla dwojga drzwi (ochrona podczas otwierania wielu drzwi)
* Kod główny #	31	5 #	Anti-passback dla drzwi
		6 #	Anti-passback dla dwojga drzwi
	32	26-37 #	Ustawienie formatu Wiegand 26 34 37. Domyślnie 26.
	33	0-2 #	Ustawienie formatu transmisji z klawiatury: 0 1 2 Po zresetowaniu to ustawienie pozostaje niezmienione.

* Kod główny #	34	1-3 #	Ustaw czas trwania alarmu (ustawienia przedstawienia 1 minuta) Po zresetowaniu to ustawienie pozostaje niezmienione.
	35	0 #	Tryb awaryjny 1. Tryb normalny. (ustawienia domyślne)
		1 #	Tryb awaryjny 2. Jeśli zostanie wprowadzony błędny kod lub nieważna karta zostanie odczytana 10 razy z rzędu w ciągu 10 minut, ze względów bezpieczeństwa system zostanie wyłączony.

* Kod główny #	35	2 #	Tryb awaryjny 3. Tryb alarmu. Jeżeli zostanie wprowadzony błędny kod lub 10 razy z rzędu odczytana zostanie nieważna karta w ciągu 10 minut, zapobiegawczo zostanie uruchomiony alarm zewnętrzny (jeśli jest podłączony) oraz brzęczyk wbudowany w klawiaturę.
----------------	----	-----	---

4. Opcjonalne ustawienia użytkownika

<i>* Kod główny #</i>	41	0 #	Wyłącz brzęczyk. Brzęczyk pozostaje aktywny tylko wtedy, gdy urządzenie wejdzie w tryb programowania.
		1 #	Aktywny dźwięk klawiszy (ustawienia domyślne)
	42	0 #	Podświetlenie klawiszy wyłączone
		1 #	Podświetlenie klawiszy włączone
		2 #	Tryb automatyczny. Zwykle podświetlenie klawisza jest wyłączone, ale włącza się po wykryciu obecności człowieka.

<i>* Kod główny #</i>	43	0 #	Dioda nie świeci, gdy urządzenie jest w trybie czuwania.
		1 #	Dioda LED miga, gdy urządzenie jest w trybie czuwania. (ustawienia)

Ważne notatki

1. Kod główny musi mieć 6-8 cyfr.
2. Kod „duress” musi mieć 8 cyfr. Pierwsza cyfra kodu musi oznaczać 1 dla strefy 1 i 2 dla strefy 2.
3. PIN użytkownika musi mieć 4-6 cyfr. Pierwsza cyfra kodu PIN musi być 1 dla strefy 1 i 2 dla strefy 2.

4. Identyfikatorem użytkownika może być dowolna liczba z zakresu od 1 do 2000.
5. Numer karty musi mieć od 8 do 10 cyfr. Jeśli numer karty zawiera mniej niż 8 cyfr, dodaj 0 przed kodem.
6. Czas opóźnienia otwarcia drzwi: od 0 do 99 sekund. 0 = 50mS
7. Gdy w urządzeniu zarejestrowana jest karta użytkownika, urządzenie automatycznie wygeneruje kod PIN 1234, który nie może otworzyć drzwi.
8. W przypadku wprowadzenia nieprawidłowego głównego kodu PIN urządzenie przechodzi w stan czuwania po 5 sekundach. Po wprowadzeniu prawidłowego głównego kodu PIN urządzenie przechodzi w tryb czuwania po 30 sekundach.
9. W przypadku korzystania z manipulatora naciśnięcie klawisza # potwierdza poprzednio wykonane polecenie klawisza. Przy dodawaniu lub usuwaniu kart jedna po drugiej naciśnięcie klawisza # oznacza zakończenie cyklu, a naciśnięcie klawisza * wyjście z tej operacji.
10. Przy dodawaniu kart szeregowo urządzenie automatycznie przypisuje numer ID oraz numer karty. Numer identyfikacyjny i numer karty zwiększają się automatycznie z każdą dodaną kartą, maksymalnie do 2000.
11. Fabrycznie ustawiony jest tryb pracy i format transmisji manipulatora. Użytkownik może w razie potrzeby zmienić te ustawienia. Po zresetowaniu urządzenia to ustawienie pozostaje niezmienione.
12. Po pomyślnym zarejestrowaniu użytkowników w Strefie 1 dioda LED zmienia kolor na zielony. Po pomyślnym zarejestrowaniu użytkowników w strefie 2 zielona dioda LED miga.

5. Operacje na karcie głównej

Dodaj użytkownika dla strefy 1

Przeczytaj główną kartę dodawania, następnie odczytaj karty użytkowników jedna po drugiej, a na koniec ponownie przeczytaj główną kartę dodawania.

Usuń użytkownika dla strefy 1

Przeczytaj główną kartę usuwania, następnie odczytaj karty użytkowników jedna po drugiej, a na koniec ponownie przeczytaj główną kartę usuwania.

6. Operacje użytkownika

Kartą

Przeczytaj kartę. Zamek zostanie odblokowany.

Jeśli ustawisz wiele kart do otwierania drzwi (od 2 do 10), przeczytaj wszystkie karty jedna po drugiej w ciągu 5 sekund, po czym zamek zostanie odblokowany.

Kartą + PIN

Przeczytaj kartę, wprowadź PIN (4 lub 6 cyfr) +#. Zamek odblokuje się.

Kartą lub PIN

Przeczytaj kartę. Zamek zostanie odblokowany. Lub wprowadź kod PIN +#. Zamek odblokuje się.

Zmień PIN bez wchodzenia w tryb programowania

** odczytaj kartę użytkownika, wprowadź stary PIN #, wprowadź nowy PIN # powtórz nowy PIN*

lub

** Wpisz numer ID # Wpisz stary PIN #, Wpisz nowy PIN # powtórz nowy PIN*

Uwaga: PIN dla strefy 1 musi zaczynać się od 1, a PIN dla strefy 2 musi zaczynać się od 2.

7. Funkcja alarmu

Alarm sabotażowy

Jeśli urządzenie zostanie zdemontowane przez włamanie, zabrzmi wewnętrzny brzęczyk i zewnętrzny alarm (jeśli jest podłączony).

Alarm otwartych drzwi

Jeśli podłączyłeś przewodowy czujnik drzwi do klawiatury kontroli dostępu i ten czujnik zostanie wyzwolony, zabrzmi wewnętrzny brzęczyk i zewnętrzny alarm (jeśli jest podłączony).

Aby wyłączyć alarm:

Odczytaj kartę użytkownika lub kartę master albo wprowadź kod PIN master.

Jeśli nie wykonasz żadnej operacji, alarm wyłączy się automatycznie po 1 minucie.

“Duress” alarm

W przypadku odczytania karty „duress” lub wprowadzenia kodu PIN „duressu” w Strefie 1 lub Strefie 2, zamek otworzy się i jednocześnie zostanie uruchomiony alarm zewnętrzny (jeśli jest podłączony). Wewnętrzny brzęczyk nie zostanie uruchomiony.

8. Tryby pracy

Czytnik kart Wiegand

W tym trybie manipulator pełni rolę czytnika kart podłączonego do urządzenia kontroli dostępu.

Obsługiwane zamówienia:

- Zmień nadrzędny kod PIN
- Ustaw kod obiektu
- Ustawienie formatu transmisji karty
- Ustawienie formatu transmisji z klawiatury
- Ustawienia opcjonalne
- Alarm sabotażowy

Samodzielna kontrola dostępu dla pojedynczych drzwi

W tym trybie manipulator otwiera pojedyncze drzwi. Drzwi można otworzyć Kartą lub PINem lub kartą + PIN. Klawiatura obsługuje podłączenie zewnętrznego czytnika kart lub przycisku dostępu do wyjścia z budynku.

Samodzielna kontrola dostępu dla dwojga drzwi

W tym trybie manipulator może sterować dwojgiem przejść. Przeczytaj kartę lub wprowadź PIN dla strefy 1 i otworzą się drzwi

1. Przeczytaj kartę lub wprowadź kod PIN dla strefy 2 i otworzą się drzwi 2.

Z zewnętrznym czytnikiem kart do otwierania dwojga drzwi

W tym trybie klawiatura umożliwia dostęp do drzwi 1, a zewnętrzny czytnik kart umożliwia dostęp do drzwi 2.

Przeczytaj kartę lub Wprowadź kod dla strefy 1 na klawiaturze kontroli dostępu. Drzwi 1 otworzą się. Przeczytaj kartę lub Wprowadź kod dla strefy 2 na zewnętrznym czytniku kart. Drzwi 2 otworzą się.

Dwa połączone urządzenia do otwierania dwojga drzwi

Ten tryb jest bardziej odpowiedni w takich lokalizacjach, jak banki, więzienia lub w sytuacjach wymagających zaawansowanego poziomu bezpieczeństwa.

Dopiero po zamknięciu drzwi 2, przeczytaj kartę lub Wprowadź kod na klawiaturze, aby otworzyć drzwi 1. A dopiero po zamknięciu drzwi 1, przeczytaj kartę lub Wprowadź kod na czytniku kart, aby otworzyć drzwi 2.

Anti-passback dla pojedynczych drzwi

W tym trybie pracy klawiatura musi być zainstalowana na zewnątrz, aby umożliwić dostęp do wnętrza budynku, a zewnętrzny czytnik kart musi być zamontowany wewnątrz, aby umożliwić wyjście z budynku. Jeżeli wejście użytkownika do budynku nie zostało zarejestrowane, użytkownik nie może wyjść poprzez odczytanie karty na czytniku kart. Ponadto użytkownik nie może wejść do budynku po raz drugi, jeśli jego wyjście nie zostało zarejestrowane.

Uwaga: Przejście można otworzyć tylko poprzez odczytanie karty dla strefy 1. Wszystkie pozostałe tryby dostępu do Strefy 1 i Strefy 2 są

nieważne.

Anti-passback dla dwojga drzwi

W tym trybie klawiatura na drzwiach 1 jest jednostką nadrzędną zapobiegającą passbackowi, a zewnętrzny czytnik kart na drzwiach 2 jest dodatkową jednostką anti-passback. W ten sposób powstaje system anti-passback odpowiedni do montażu na parkingach.

Użytkownik może wejść do budynku drzwiami 1, odczytując kartę na klawiaturze kontroli dostępu i może wyjść tylko drzwiami 2, odczytując kartę na zewnętrznym czytniku kart. Jeśli wejście użytkownika nie zostało zarejestrowane przez drzwi 1, nie będzie on mógł wyjść drzwiami 2. Ponadto użytkownik nie może wejść po raz drugi, jeśli jego wyjście nie zostało zarejestrowane.

Uwaga: przejście można otworzyć tylko poprzez odczytanie karty dla strefy 1. Wszystkie pozostałe tryby dostępu do Strefy 1 i Strefy 2 są nieważne.

Rozwiązywanie problemów

Problem	Przyczyna	Rozwiązanie
Za mała odległość odczytu karty	Niska jakość karty	Użyj oryginalnych kart
Problemy z ustawieniem PIN	1. PIN nie jest zgodny ze standardem 2. Jesteś w trybie odczytu karty, ustaw hasło	1. Pierwsza cyfra kodu PIN musi wynosić 1 lub 2, w zależności od Strefy. 2. PIN nie może mieć 1234. PIN musi mieć 4 lub 6 cyfr.

Kod PIN nie otwiera drzwi	<ol style="list-style-type: none"> 1. Użyłeś kodu PIN 1234 2. Ustawiony tryb dostępu nie pozwala na dostęp do kodu PIN 	<ol style="list-style-type: none"> 1. Zmień kod PIN. 2. Zmień tryb dostępu: karta lub PIN.
Brak odpowiedzi po przeczytaniu karty	Klawiatura nie jest w stanie czuwania, może być w trybie programowania	Naciśnij klawisz *, dioda LED zacznie migać. Klawiatura jest teraz w trybie czuwania.
Klawiatura nie świeci	Złe ustawienia klawiatury	1. Włącz lub wyłącz podświetlenie klawiszy. W trybie automatycznym klawisze zapalają się dopiero po ich naciśnięciu i pozostają podświetlone przez 30 sekund.
Nieprawidłowy Kod główny	Zapomniałeś o kodzie głównym	Zresetuj urządzenie. Kod główny wraca do 999999. Po zresetowaniu dane użytkownika nie są kasowane.

Zresetuj Kod główny

Wyłączyć zasilanie klawiatury kontroli dostępu.

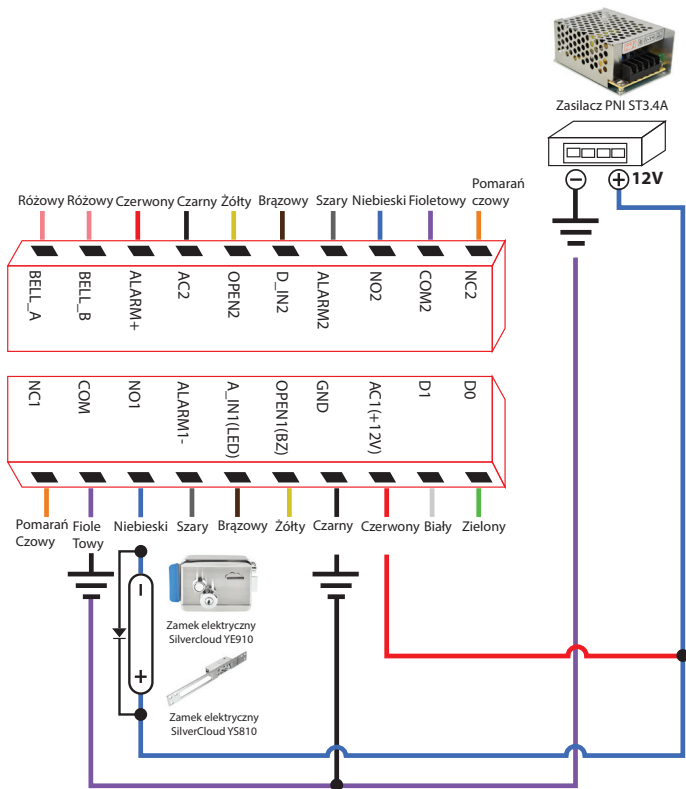
Przytrzymaj klawisz # podczas ponownego uruchamiania zasilania.

Po usłyszeniu dwóch dźwięków Di.. zwolnij klawisz #.

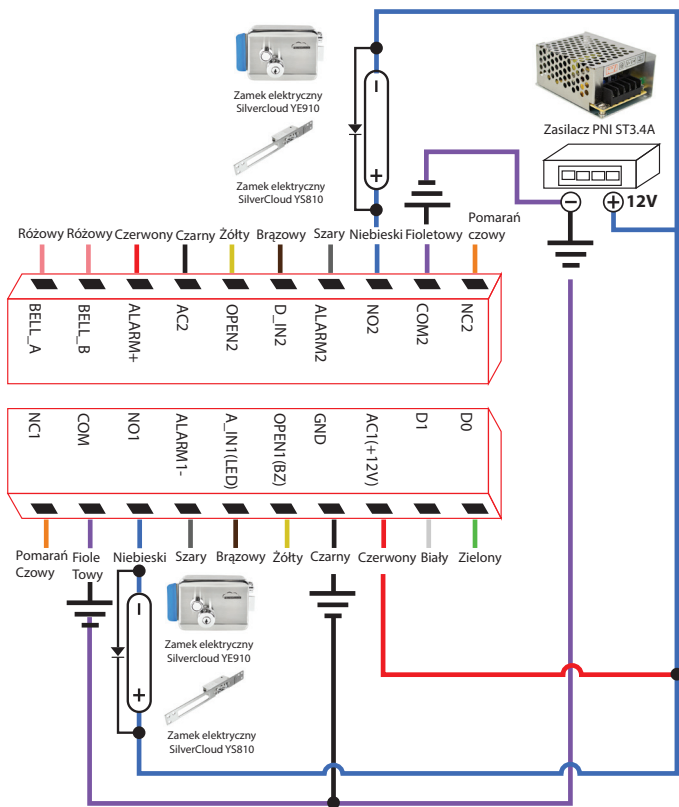
Klawiatura wróciła do ustawień fabrycznych. Hasło główne powraca do 999999. Dane użytkownika nie zostały usunięte.

Przykłady połączeń dla jednych i dwojga drzwi

Kontrola dostępu dla jednych drzwi z zamkiem elektromagnetycznym Silvercloud YE910 lub Silvercloud YS810 i zasilaczem PNI ST3.4A.



Kontrola dostępu dla dwójga drzwi z zamkiem elektromagnetycznym Silvercloud YE910 lub Silvercloud YS810 i zasilaczem PNI ST3.4A.



Descriere

PNI DK220 este un dispozitiv de control acces independent (stand alone) si cititor de proximitate. Este echipat cu doua relee pentru controlul a doua usi si suporta maxim 2000 de utilizatori, fiecare utilizator poate avea un cod PIN si un card de acces.

Tastatura poate fi conectata la o yala electromagnetica, la un sistem de alarma, o sonerie, buton de acces sau senzor usa.

Dispozitivul are 7 moduri de functionare: cititor de card Wiegand, control acces pentru o singura usa, control acces pentru doua usi, control acces cu cititor de card extern pentru doua usi, doua unitati interconectate pentru doua usi, anti-passback pentru o singura usa si anti-passback pentru doua usi.

Caracteristici de baza

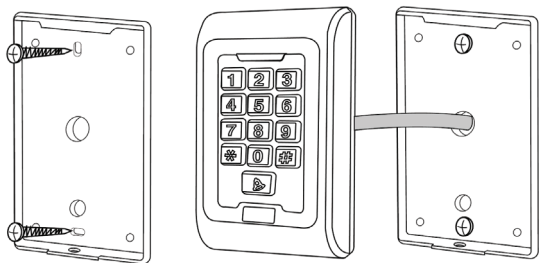
- Carcasa din aliaj de aluminiu cu clasa de rezistenta la apa IP65
- Cititor de carduri incorporat 125KHz
- Taste numerice iluminate. Lumina tastelor poate fi programata astfel: Normal ON, Normal OFF sau Human-Approach ON (se aprinde cand detecteaza miscare).
- Alarma anti-sabotaj (tamper), alarma declansare senzor usa, alarma "cod duress" (acest cod poate fi folosit atunci cand utilizatorul este fortat sub amenintare sa deschida usa. La tastarea acestui cod, usa se va deschide dar va activa o alarma silentioasa).
- Adaugare si stergere carduri prin cardul administrator.
- Inregistrare si stergere utilizatori prin taste.

Specificatii tehnice

Tensiune de alimentare	12V AC/DC
Consum in standby	<25mA
Sarcina iesire yala	<1A
Sarcina iesire alarma	<1A
Sarcina iesire sonerie	<1A
Distanta citire card	maxim 40 mm
Capacitate utilizatori	maxim 2000
Card compatibil	EM 125Khz/HID 125KHz
Format transmisie card	26-37 bit Wiegand
Format transmisie tastatura	4 bit si 8 bit si numar card virtual
Temperatura de lucru	-26°C ~ +80°C

Instalare

Alegeti locul de instalare si faceti gauri in perete care sa corespunda cu gaurile din suportul de montaj. Fixati suportul de perete cu ajutorul suruburilor incluse in pachet. Treceti cablurile prin fanta din mijlocul suportului. Conectati cablurile. Izolati cablurile nefolosite pentru a evita producerea unui scurtcircuit.



Cabluri

Zona 1		
BELL_A	roz	Sonerie
BELL_B	roz	Sonerie
ALARM+	rosu	Conector alarma
AC2	negru	Intrare AC
OPEN2	galben	Buton de iesire
D_IN2	maro	Contact usa
ALARM2-	gri	Alarma 2
NO2	albastru	Releu 2 NO
COM2	violet	Releu 2 Com
NC2	orange	Releu 2 NC

Zona 2

D0	verde	Iesire Wiegand D0
D1	alb	Iesire Wiegand D1
AC1	rosu	AC1 (+12V)
GND	negru	GND
OPEN1(LED)	galben	Buton de iesire (LED verde)
D_IN1(BZ)	maro	Contact usa (pentru buzzer)
ALARM1-	gri	Alarma 1
NO1	albastru	Releu 1 NO
COM1	violet	Releu 1 Com
NC1	orange	Releu 1 NC

Avertizari sonore si luminoase

Status	LED	Sunet
Standby	Rosu clipeste	
Apasare tasta		Di
Citire card	Verde	Di.
Usa 1 deschisa	Verde	Di.
Usa 2 deschisa	Verde clipeste	Di.
Operatiune reusita	Verde	Di.
Eroare operatiune		DiDiDi
Introducere PIN	Rosu	
Citire card&PIN	Rosu	
Citire carduri multiple	Rosu	
In meniu	Rosu	
In setari	Orange	
Acces card administrator	Orange	DiDi
Iesire card administrator	Rosu clipeste	Di.
Alarma	Rosu clipeste des	Alarma

Ghid programare rapida

1. Setari administrator

* Cod master #	00	<i>Introdu noul cod master # Repeta noul cod master #</i>	Schimbare cod master. <i>Nota: Codul master implicit este 999999. Codul master trebuie sa contina intre 6 si 8 cifre.</i>
	01	<i>Citeste cardul</i>	Inregistrare card administrator pentru adaugare carduri. <i>Nota: Implicit: zona 1.</i>
	02	<i>Citeste cardul</i>	Inregistrare card administrator pentru stergere carduri.
	03	<i>Citeste cardul</i>	Inregistrare card alarma "duress" pentru zona 1
	04	<i>Citeste cardul</i>	Inregistrare card alarma "duress" pentru zona 2

* Cod master #	05	<i>Introdu PIN-ul din 8 cifre</i>	Inregistrare cod PIN “duress” pentru zona 1 Nota: Prima cifra a PIN-ului trebuie sa fie 1 pentru zona 1.
	06	<i>Introdu PIN-ul din 8 cifre</i>	Inregistrare cod PIN “duress” pentru zona 2 Nota: Prima cifra a PIN-ului trebuie sa fie 1 pentru zona 2.
	07	<i>0000 #</i>	Sterge toti utilizatorii
	51	Set administrator open Lock 1	
	52	Set administrator open Lock 2	

Nota:

Codul PIN “duress” si cardul “duress” pot fi folosite atunci cand utilizatorul este fortat sub amenintare sa deschida usa. La tastarea acestui cod sau la citirea acestui card, usa se va deschide dar va trimite in acelasi timp un semnal de alarma.

2. Setari utilizator pentru Zona 1 si Zona 2

Adauga card utilizator

<i>* Cod master #</i>	11 (pentru Zona 1)	<i>Citeste cardul</i>
		<i>Introdu ID # Citeste cardul</i>
	21 (pentru Zona 2)	<i>Introdu numar card #</i>
		<i>Introdu ID # Introdu numar card #</i>

Nota: Utilizatorii pot fi adaugati unul dupa altul fara a iesi din programare. ID utilizator poate contine intre 1 si 4 cifre, in intervalul 1 - 2000. 1, 01, 001 si 0001 inseamna 1.

Adauga PIN utilizator

<i>* Cod master #</i>	11 (pentru Zona 1) 21 (pentru Zona 2)	<i>Introdu ID # Introdu PIN #</i>
-----------------------	--	-----------------------------------

Nota: PIN-ul poate contine 4 - 6 cifre. Prima cifra trebuie sa fie 1 pentru Zona 1 si 2 pentru Zona 2. "1234" este rezervat, nu poate fi setat ca PIN.

Sterge utilizator

<i>* Cod master #</i>	12 (pentru Zona 1)	<i>Citeste cardul</i>
	22 (pentru Zona 2)	<i>Introdu ID #</i>
		<i>Introdu numar card #</i>

Nota: Utilizatorii pot fi stersi unul dupa altul fara a iesi din programare.

Sterge toti utilizatorii

<i>* Cod master #</i>	07	0000 #
-----------------------	----	--------

Nota: Aceasta comanda sterge toti utilizatorii de pe Zona 1 si Zona 2.

Moduri de acces

<i>* Cod master #</i>	13 (pentru Zona 1)	0 #	Prin card
	23 (pentru Zona 2)	1 #	Prin card + PIN
		2 #	Prin card sau PIN (setare implicita)

Setare intarziere usa deschisa

<i>* Cod master #</i>	14 (pentru Zona 1) 24 (pentru Zona 2)	0 - 99 #	Setare implicita 5
-----------------------	--	----------	--------------------

Setare moduri inchidere usa

* Cod master #	15 (pentru Zona 1) 25 (pentru Zona 2)	0 #	Setare releu pe mod impuls (setare implicita). De fiecare data cand va fi introdus un cod sa va fi citit un card valid, usa se va deschide si se va inchide automat dupa intervalul de timp setat (intre 0.05 sec. si 99 sec).
		1 #	Setare releu pe mod comutare. De fiecare data cand va fi introdus un cod sa va fi citit un card valid, usa se va deschide dar nu se va inchide pana cand nu va fi tastat din nou codul sau va fi citit cardul.

Deschidere usa cu mai multe carduri

* Cod master #	16 (pentru Zona 1) 26 (pentru Zona 2)	1 - 10 #	Setare implicita 1
----------------	--	----------	--------------------

Nota: Usa se va deschide doar dupa ce vor fi citite toate cardurile. De exemplu, prin comanda * **cod master # 16 3 #**, trebuie sa cititi consecutiv 3 carduri ca sa deschideti usa. Aceasta setare este utila doar daca ati setat tastatura pe modul de acces cu card.

Adaugare carduri utilizator in serie

<i>* Cod master #</i>	<i>17</i> (pentru Zona 1) <i>27</i> (pentru Zona 2)	<i>Introdu ID #, Introdu numar card #, Introdu cantitate card #</i>
-----------------------	--	---

Nota: Numerele cardurilor trebuie sa fie consecutive (intre 8 si 10 caractere). Cantitate card este intre 1 si 2000.

3. Setari sistem

* Cod master #	30	0-15 #	Setare cod unitate (Facility Code). Implicit: 0
	31	0 #	Cititor Wiegand
		1 #	Control acces stand-alone pentru o singura usa (setare implicita)
		2 #	Control acces stand-alone pentru doua usu
		3 #	Cu cititor extern pentru doua usu
		4 #	Doua unitati interconectate pentru doua usu (protectie la deschidere usu multiple)
		5 #	Anti-passback pentru o usa (protectie la transmitere cartela)
		6 #	Anti-passback pentru doua usu (protectie la transmitere cartela)
	32	26-37 #	Setare format Wiegand 26 34 37. Implicit 26.
	33	0-2 #	Setare format transmisie tastatura: 0 1 2 Dupa reset, aceasta setare ramane neschimbata.

* Cod master #	34	1-3 #	Setare durata alarma (setare implicita 1 minut) Dupa reset, aceasta setare ramane neschimbata.
	35	0 #	Mod siguranta 1. Mod normal. (setare implicita)
		1 #	Mod siguranta 2. Daca se introduce codul gresit sau se citeste un card invalid de 10 ori la rand in intervalul de 10 minute, ca masura de siguranta, sistemul se opreste.
		2 #	Mod siguranta 3. Mod alarma. Daca se introduce codul gresit sau se citeste un card invalid de 10 ori la rand in intervalul de 10 minute, ca masura de siguranta, se va declansa alarma externa (daca este conectata) si buzzer-ul incorporat in tastatura.

4. Setari optionale utilizator

* Cod master #	41	0 #	Buzzer dezactivat. Buzzer-ul ramane activ doar cand dispozitivul intra in mod programare.
		1 #	Sunet taste activ (setare implicita)
	42	0 #	Lumina taste dezactivata
		1 #	Lumina taste activata
		2 #	Mod automat. In mod normal, lumina taste este stinsa dar se aprinde cand se detecteaza miscare.
	43	0 #	LED dezactivat cand dispozitivul se afla in standby.
		1 #	LED-ul clipeste cand dispozitivul se afla in standby. (setare implicita)

Note importante

1. Codul master trebuie sa contina 6-8 cifre.
2. Codul "duress" trebuie sa contina 8 cifre. Prima cifra a codului trebuie sa fie 1 pentru zona 1 si 2 pentru zona 2.
3. PIN utilizator trebuie sa contina 4-6 cifre. Prima cifra a PIN-ului trebuie sa fie 1 pentru zona 1 si 2 pentru zona 2.
4. ID utilizator poate fi orice numar intre 1 si 2000.

5. Numarul cardului trebuie sa contina intre 8 si 10 cifre. Daca numarul cardului contine mai putin de 8 cifre, adaugati 0 in fata codului.
6. Timp de intarziere usa deschisa: intre 0 si 99 secunde.
0 = 50mS
7. Cand se inregistreaza un card utilizator in dispozitiv, dispozitivul va genera automat un PIN 1234 care nu poate debloca usa.
8. Daca se introduce un cod PIN master invalid, dispozitivul intra in standby dupa 5 secunde. Daca se introduce un cod PIN master valid, dispozitivul intra in standby dupa 30 secunde.
9. Cand se foloseste tastatura, prin apasarea tastei # se confirma comanda din taste executata anterior. Cand se adauga sau se sterg carduri unul dupa altul, apasarea tastei # indica sfarsit ciclu, iar apasarea tastei * indica iesirea din aceasta operatiune.
10. Cand adaugati carduri in serie, dispozitivul aloca automat un numar ID si un numar de card. Numarul ID si numarul de card cresc automat cu fiecare card adaugat, pana la un maxim de 2000.
11. Modul de operare si formatul de transmisie al tastaturii sunt setate din fabrica. Utilizatorul poate schimba aceste setari in functie de necesitate. Dupa resetarea dispozitivului, aceasta setare ramane neschimbata.
12. Dupa inregistrarea cu succes a utilizatorilor in Zona 1, LED-ul devine verde. Dupa inregistrarea cu succes a utilizatorilor in Zona 2, LED-ul verde clipeste.

5. Operatiuni prin card administrator

Adauga utilizator pentru Zona 1

Citeste cardul administrator pentru adaugare carduri, apoi Citeste cardurile de utilizator unul dupa altul, la final Citeste din nou cardul administrator pentru adaugare carduri.

Sterge utilizator pentru Zona 1

Citeste cardul administrator pentru stergere carduri, apoi Citeste cardurile de utilizator unul dupa altul, la final Citeste din nou cardul administrator pentru stergere carduri.

6. Operatiuni utilizator

Acces prin card

Apropiati cardul de tastatura. Yala se va debloca.

Daca ati setat mai multe carduri pentru deschidere usa (intre 2 si 10), cititi succesiv toate cardurile in intervalul de timp de 5 secunde., dupa care yala se va debloca.

Acces prin card + PIN

Apropiati cardul de tastatura, tastati imediat codul PIN din 4 sau 6 cifre +#. Yala se va debloca.

Acces prin card sau PIN

Apropiati cardul de tastatura. Yala se va debloca. Sau tastati codul PIN din 4 sau 6 cifre +#. Yala se va debloca.

Modifica PIN fara a intra in mod programare

** citeste card user, tasteaza PIN-ul vechi #, tasteaza noul PIN # repeta noul PIN*

sau

** tasteaza numar ID # tasteaza PIN-ul vechi #, tasteaza noul PIN # repeta noul PIN*

Nota: PIN-ul pentru Zona 1 trebuie sa inceapa cu 1, iar PIN-ul pentru Zona 2 trebuie sa inceapa cu 2.

7. Functia alarma

Alarma anti-sabotaj (tamper)

Daca dispozitivul este demontat prin efracție, buzzer-ul intern si alarma externa (daca este conectata) vor suna.

Alarma usa deschisa

Daca ati conectat la tastatura de control acces un senzor de usa cu fir si acest senzor se va declansa, buzzer-ul intern si alarma externa (daca este conectata) vor suna.

Pentru a opri alarma:

Cititi cardul de utilizator sau cardul administrator sau introduceti PIN-ul de administrator.

Daca nu efectuati nici o operatiune, alarma se va opri automat dupa 1 minut.

Alarma “duress“

Daca se citeste cardul “duress“ sau se introduce codul PIN “duress“

pe Zona 1 sau Zona 2, yala se va deschide si, in acelasi timp, se va declansa alarma externa (daca este conectata). Buzzerul intern nu va suna.

8. Moduri de functionare

Cititor Wiegand

In acest mod tastatura functioneaza ca un cititor de card conectat la un dispozitiv de control acces.

Comenzi suportate:

- Modificare cod PIN administrator
- Setare cod unitate (facility code)
- Setare format transmisie card
- Setare format transmisie tastatura
- Setari optionale
- Alarma anti-sabotaj (tamper)

Control acces stand-alone pentru o singura usa

In acest mod, tastatura deschide o singura usa pentru accesul in cladire. Usa poate fi deschisa prin card sau PIN sau card+PIN. Tastatura suporta conectarea unui cititor de card extern sau a unui buton de acces pentru iesirea din cladire.

Control acces stand-alone pentru doua usi

In acest mod, pot controla doua usi. Cititi cardul sau tastati codul PIN pentru Zona 1 si usa 1 se va deschide. Cititi cardul sau tastati codul PIN pentru Zona 2 si usa 2 se va deschide.

Cu cititor de card extern pentru a deschide doua usi

In acest mod, tastatura de acces permite accesul pentru usa 1, iar cititorul de card extern permite accesul pentru usa 2.

Cititi cardul sau introduceti codul pentru Zona 1 pe tastatura de control acces. Usa 1 se va deschide. Cititi cardul sau introduceti codul pentru Zona 2 pe cititorul de card extern. Usa 2 se va deschide.

Doa dispozitive interconectate pentru a deschide doua usi

Acest mod este mai potrivit pentru locatii precum banci, inchisori sau pentru situatii care necesita un nivel de securitate avansat.

Doar dupa ce usa 2 s-a inchis, cititi cardul sau tastati codul pe tastatura pentru a deschide usa 1. Si doar dupa ce usa 1 s-a inchis, cititi cardul sau tastati codul pe cititorul de card pentru a deschide usa 2.

Anti-passback pentru o singura usa

In acest mod de functionare, tastatura trebuie montata la exterior pentru a permite accesul in interior, iar cititorul de card extern trebuie montat la interior pentru a permite iesirea din cladire.

Daca nu s-a inregistrat intrarea utilizatorului in cladire, utilizatorul nu poate iesi citind cardul pe cititorul de card de la interior. De asemenea, utilizatorul nu poate intra a doua oara in cladire daca nu s-a inregistrat iesirea lui.

Nota: Usa se poate deschide doar prin citirea cardului pentru Zona 1. Toate celelalte moduri de acces pentru Zona 1 si Zona 2 nu sunt valide.

Anti-passback pentru doua usi

In acest mod de functionare, tastatura de la usa 1 este unitatea master anti-passback, iar cititorul de card extern de la usa 2 este unitate secundara anti-passback. Astfel, se creeaza un sistem anti-passback potrivit pentru instalarea in parcuri.

Utilizatorul poate intra in cladire pe usa 1 citind cardul pe tastatura de control acces si poate iesi doar pe usa 2 citind cardul pe cititorul de card extern. Daca nu s-a inregistrat intrarea utilizatorului pe usa 1, nu va putea iesi pe usa 2. De asemenea, utilizatorul nu poate intra a doua oara daca nu s-a inregistrat iesirea lui.

Nota: Usa se poate deschide doar prin citirea cardului pentru Zona 1. Toate celelalte moduri de acces pentru Zona 1 si Zona 2 nu sunt valide.

Probleme si solutii

Problema	Cauza	Solutie
Distanta de citire card prea mica	Calitatea scazuta a cardului	Folositi carduri originale
Probleme de setare PIN	<ol style="list-style-type: none">1. PIN-ul nu respecta forma standard2. Sunteti pe modul cititor, setati parola	<ol style="list-style-type: none">1. Prima cifra din PIN trebuie sa fie 1 sau 2, in functie de Zona.2. PIN-ul nu trebuie sa fie de forma 1234. PIN-ul trebuie sa contina 4 sau 6 cifre.3. Nu incercati sa setati PIN pe modul cititor.
PIN-ul nu deschide usa	<ol style="list-style-type: none">1. Ati folosit PIN 12342. Modul de acces setat nu permite accesul cu PIN	<ol style="list-style-type: none">1. Schimbati PIN-ul.2. Schimbati modul de acces: card sau PIN.
Nici un raspuns dupa citire card	Tastatura nu este in standby, poate fi in modul de programare	Apasati tasta *, LED-ul clipeste. Acum tastatura este in modul standby.

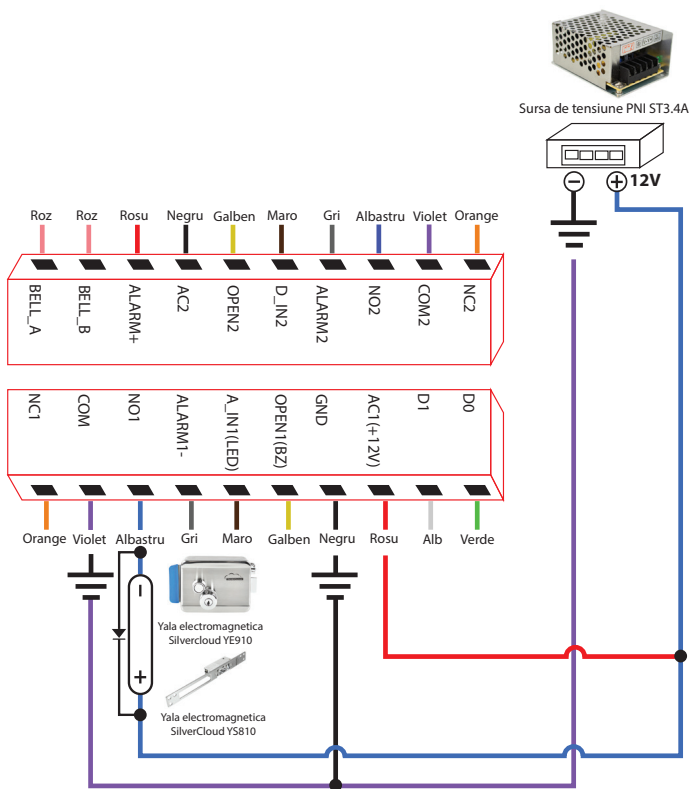
Tastatura nu se aprinde	Setari tastatura gresite	1. Setati lumina de fundal a tastelor pe aprins sau auto. In modul auto, tastele se aprind doar dupa ce sunt apasate si raman aprinde timp de 30 secunde.
Master code invalid	Ati uitat codul master	Resetati dispozitivul. Codul master redevine 999999. Prin reset datele de utilizator nu se sterg.

Resetare dispozitiv

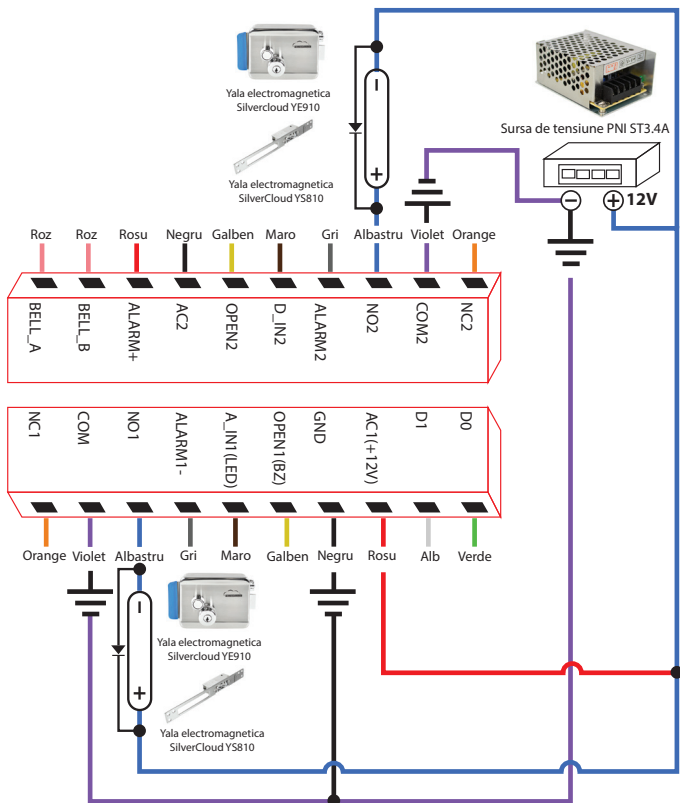
1. Intrerupeti alimentarea tastaturii de control acces.
2. Tineti apasat tasta # in timp ce reporniti alimentarea.
3. Dupa ce auziti doua sunete Di., eliberati tasta #.
4. Tastatura a revenit la setarile din fabrica. Parola master redevine 999999. Datele utilizatorilor nu s-au sters.

Exemple conexiune

Control acces pentru o singura usa cu yala electromagnetica Silvercloud YE910 sau Silvercloud YS810 si sursa de tensiune PNI ST3.4A.



Control acces pentru doua usi cu yala electromagnetica Silvercloud YE910 sau Silvercloud YS810 si sursa de tensiune PNI ST3.4A.

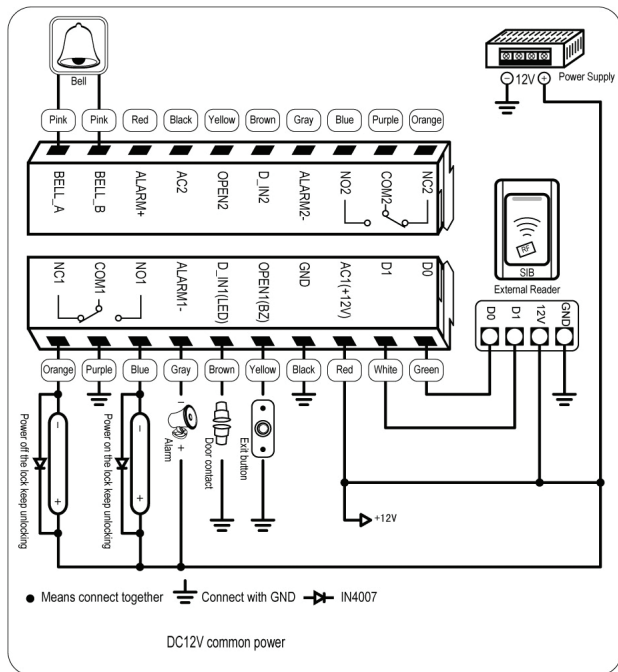


Connection diagrams for the 7 operating modes

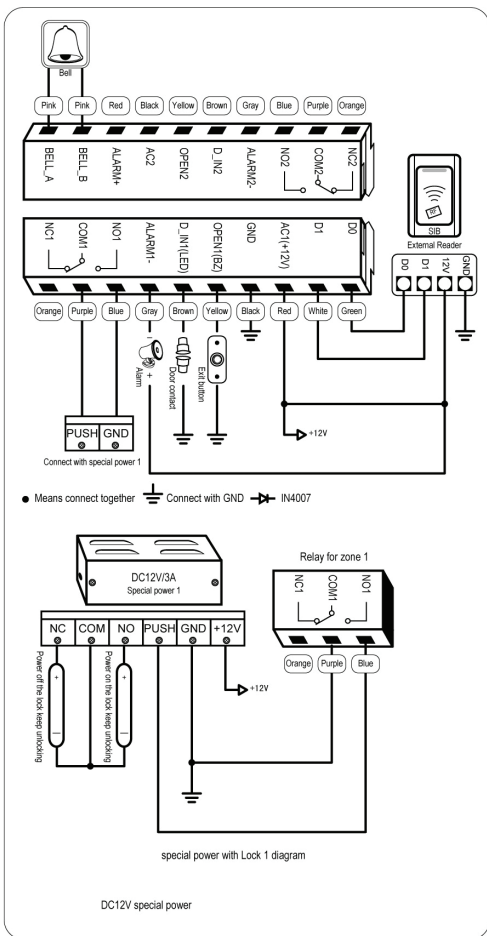
A. Stand-alone access control for a single door

Anti-passback for a single door

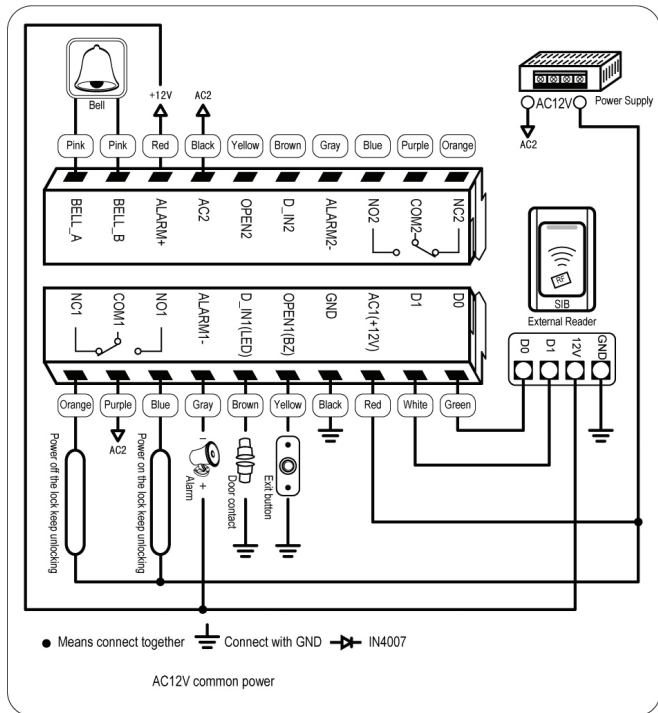
A1. With common 12V DC (direct current) power supply



A2. With special 12V DC (direct current) power supply

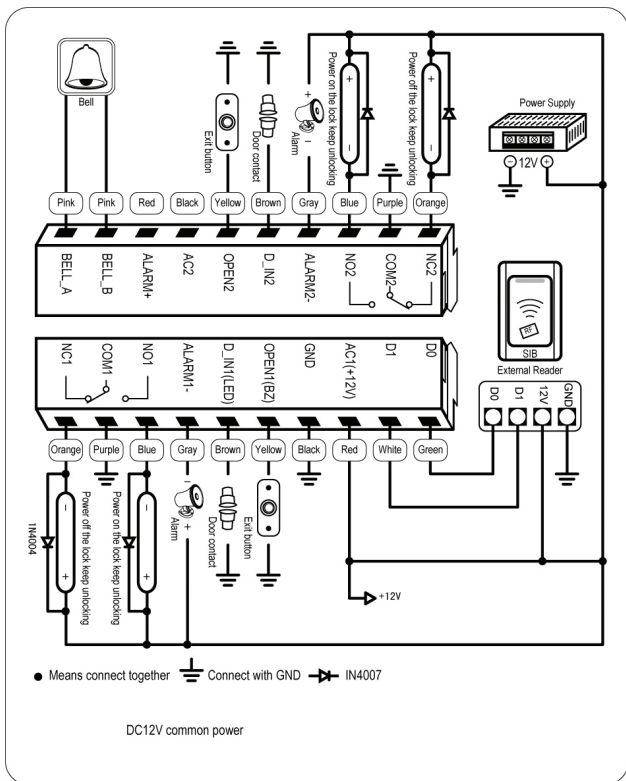


A3. With common 12V AC (alternating current) power supply

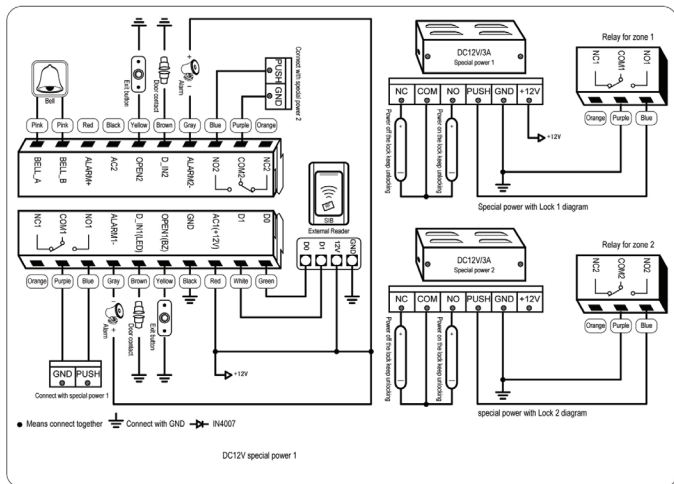


- B. With external card reader for two doors
- Stand-alone for two doors
- Two interconnected units for two doors
- Anti-passback for two doors

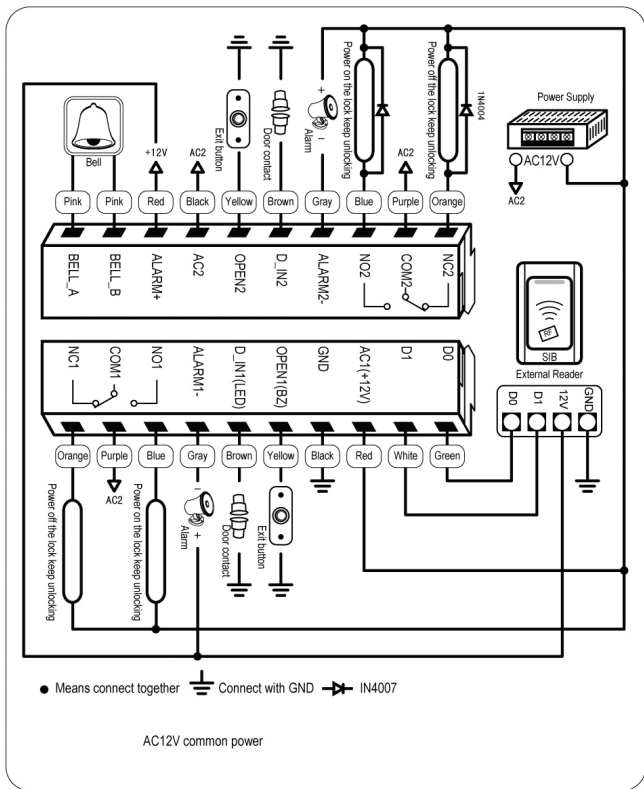
B1. With common 12V DC (direct current) power supply



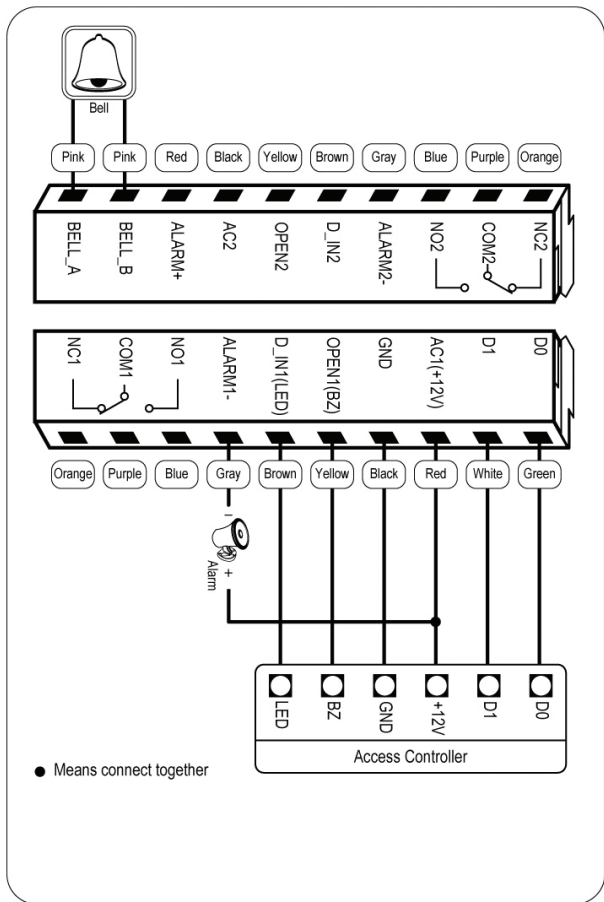
B2. With special 12V DC (direct current) power supply



B3. With common 12V AC (alternating current) power supply



C. Wiegand card reader



EN:

EU Simplified Declaration of Conformity

SC ONLINESHOP SRL declares that **Access control keypad PNI DK220** complies with the Directive EMC 2014/30/EU. The full text of the EU declaration of conformity is available at the following Internet address:

<https://www.mypni.eu/products/8533/download/certifications>

BG:

Опростена декларация за съответствие на ЕС

SC ONLINESHOP SRL декларира, че **Клавиатура за контрол на достъпа PNI DK220** спазва директивата EMC 2014/30/EU. Пълният текст на ЕС декларацията за съответствие е достъпен на следния интернет адрес:

<https://www.mypni.eu/products/8533/download/certifications>

DE:

Vereinfachte EU- Konformitätserklärung

SC ONLINESHOP SRL erklärt, dass das **Zutrittskontrolltastatur PNI DK220** der Richtlinie EMC 2014/30/EU. Sie finden den ganzen Text der EU-Konformitätserklärung an der folgenden Internetadresse:

<https://www.mypni.eu/products/8533/download/certifications>

ES:

Declaración UE de conformidad simplificada

SC ONLINESHOP SRL declara que el **Teclado de control de acceso PNI DK220** cumple con la Directiva EMC 2014/30/EU. El texto completo de la declaración de conformidad de la UE está disponible en la siguiente dirección de Internet:

<https://www.mypni.eu/products/8533/download/certifications>

FR

Déclaration de conformité simplifiée de l'UE

SC ONLINESHOP SRL déclare que **Clavier de contrôle d'accès PNI DK220** est conforme à la directive EMC 2014/30/EU et RED 2014/53/UE. Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante:

<https://www.mypni.eu/products/8533/download/certifications>

HU:

Egyszerűsített EU Megfelelési Közlemény

SC ONLINESHOP SRL kijelenti azt, hogy a **Beléptető billentyűzet PNI DK220** megfelel az EMC 2014/30/EU. Az EU-megfeleléségi nyilatkozat teljes szövege a következő internetes címen érhető el:

<https://www.mypni.eu/products/8533/download/certifications>

IT:

Dichiarazione UE di conformità semplificata

SC ONLINESHOP SRL dichiara che il **Tastiera controllo accessi PNI DK220** è conforme alla direttiva EMC 2014/30/UE. Il testo completo della dichiarazione di conformità europea è disponibile al seguente indirizzo Internet:

<https://www.mypni.eu/products/8533/download/certifications>

NL:

Vereenvoudigde EU-conformiteitsverklaring

SC ONLINESHOP SRL verklaart dat **Toegangscontrole toetsenbord PNI DK220** voldoet aan de richtlijn EMC 2014/30/EU. De volledige tekst van de EU-conformiteitsverklaring is beschikbaar op het volgende internetadres:

<https://www.mypni.eu/products/8533/download/certifications>

PL:

Uproszczona deklaracja zgodności UE

SC ONLINESHOP SRL oświadcza, że **Klawiatura kontroli dostępu PNI DK220** jest zgodny z dyrektywą EMC 2014/30/EU. Pełny tekst deklaracji zgodności UE dostępny jest pod następującym adresem internetowym:

<https://www.mypni.eu/products/8533/download/certifications>

RO:

Declaratie UE de conformitate simplificata

SC ONLINESHOP SRL declara ca **Tastatura control acces PNI DK220** este in conformitate cu Directiva EMC 2014/30/EU. Textul integral al declaratiei UE de conformitate este disponibil la urmatoarea adresa de internet:

<https://www.mypni.eu/products/8533/download/certifications>

