

Ideas On Wire

WIEGUARD 3[®]

Wiegand physical lock access system with Ethernet connectivity

User's Manual



Table of Contents

Wiegand physical lock access system with Ethernet connectivity.....	1
Table of Contents.....	2
Preface.....	5
Disclaimer.....	5
1. Overview.....	6
Features.....	6
Technical information.....	7
LED and beeper.....	7
2. Keypad usage.....	8
Extra functions.....	8
Erase code.....	8
Timeout feature.....	8
Input Lock-out feature.....	8
Log on ungranted open door event.....	8
3. Reset code.....	8
Predefined state.....	9
4. Fixed codes.....	9
5. Fixed PIN + card (2-factor authentication access).....	9
6. Fixed plus Blink code.....	9
7. Timed code.....	10
8. Rolling code.....	10
9. Enabling rolling (hidden) code.....	10
10. Summary of possible keycodes.....	11
11. Cards.....	11
12. Stealth card.....	12
13. Door latch activation.....	12
Lock-out prevent feature.....	12
14. Web interface.....	13
Authenticate step.....	13
Firmware version.....	13
Control panel page.....	14
Power lock.....	14
Reset board.....	14
Beep.....	14

LED green.....	14
Init EEPROM.....	14
State.....	15
Timed PIN	15
Data pull time	15
Door state	15
Logout.....	15
PINs page	16
Adding cards	16
Cards page	17
Configuration page	18
Erase data on RST code.....	18
Ignore RST code	18
W26/W34	18
SILENT mode	18
No POST send	18
Params online pull	19
Pull interval (min)	19
PIN6 days	19
UID (Unit Identification Code)	19
IP address and Gateway address	20
Router configuration.....	20
15. Logging access activity over the internet.....	20
The backend.....	20
Advanced status reporting.....	20
Backend information	20
Board emulator.....	21
Data pulls log	24
Access Entries log	25

WIEGUARD 3[®]

A full-fledged Wiegand physical access control system with Ethernet connectivity

Preface

The present manual refers to firmware version 3.19.

The appendix A is to be considered as strictly confidential information not to be released to the public.

Disclaimer

The information contained in this manual is intended for the end user only. Furthermore, sensitive information contained in the appendix A is kept solely for the developer's documentation.

Specifically, when the system is utilized in real world applications, in order to keep the security of the access system and avoid possible vulnerability exploitation by third party, detailed technical data are to be kept confidential and not to be shared publicly. Any breach of secrecy of the below details might render insecure the whole system, resulting in possible functional modifications, misuse and including total or partial disruption of service.

Please use the below information at your own risk.

1. Overview

The WIEGUARD3® Wiegand Ethernet module is a door access embedded electronic project which allows easy access to an electrically operated door latch upon receiving the authorized code or RFID access card over a standard Wiegand communication protocol keypad reader.

Features

The following characteristics refer to firmware version 3.19, which is the latest released at the time of publishing this text. Changes or additional features might be present on future versions of the firmware.

The main features of the access system can be summarized as follows:

- The system can be used as a keycode only, card only or mixed mode
- Response to a maximum of 9 (8 customizable + 1 hidden) keypad codes, max 8 digits long each:
 - 3 Fixed PIN codes (master or administrator's use)
 - 1 fixed PIN followed by card input (for a 2-factor level of security)
 - 1 fixed PIN followed by a variable numerical part (blink based component, randomly generated)
 - 1 timed out code (valid only for a fixed duration of time)
 - 1 OTP Rolling code (one-time-access, for service use)
 - 1 "fixed until hidden", enabling one extra hidden code for rolling (e.g.: a new code becomes valid for the next tenant, disabling the current code)
 - Note: the recognition of the code is in reverse order from bottom with highest priority
- Board recovery Reset code (soft reset, hardcoded PIN, also restores factory values)
- Factory reset card (stealth erase)
- Support of both RFID cards and MIFARE cards (Wiegand W26 and W34 protocol standards), depending on fitted reader hardware;
- Max number of stored RFID or MIFARE cards: 8 (can store up to 186 cards with FW modification);
- Web interface for easy monitoring and configuration
 - Control panel for diagnostics and controls:
 - Power lock button
 - Power lock until door open button
 - Reset board
 - Buzzer acoustic signal button for testing, alarm or notification purposes
 - LED activation for testing purposes
 - Restore EEPROM memory content to standard values
 - Turing current state
 - Monitor door open sensor status
 - Keypad PINs configuration
 - Cards configuration
 - Add new card
 - Toggle individual activation or remove any previously stored cards
 - Configurable parameters
 - Remote synchronization of all User settings

- Activity logging over internet (requires internet connection through Ethernet cable) with IP, station ID, timestamp, access type, code used and status. Entry User is additionally set at the backend server. This also includes room occupancy status, abnormal door opening operations and security violation.
- Secure rolling-token access to change system settings
- No wireless, only wired connections, to guarantee lag-free and robust from tampering operation;
- Possibility to set real-time alarms via email on wrong attempts and unexpected door openings;
- Facility ID coding, to allow multi-stations system;
- Password protected configuration webserver to avoid unauthorized access to settings;
- Watchdog feature to ensure fail-safe, uninterrupted operation of the microcontroller;
- Independent offline operation, no need for internet connection;
- Low-power consumption, no batteries required;
- User Settings are saved immediately locally and will be retained in case of power interruption;
- Small form factor and no ventilation needed;
- Easy to install and no maintenance required;
- Remote configuration change, either by direct access or pull synchronization, to accommodate any network setup;
- On request, a customized reader can be used instead, for example, to allow only cards or only keypad inputs
- Users name association is made on the server backend control panel

Technical information

The system currently supports 26-bit and 34-bit standard Wiegand protocol. The electronics features a low-power microcontroller board and an independent Ethernet chipset and an output driven by a solid state switch for the actuator and software reset function.

A watchdog failure protection function prevents any possible hanging of the software, should any unexpected external circumstances arise.

The board features an HTTP web server as the interface to configure its parameters, connectivity is via hardwired standard RJ45 Ethernet cable. Decision has been made to remove Wi-Fi connectivity by design, for increased security to avoid wireless hacking or tampering and for higher speed and reliability.

LED and beeper

Whenever the system is operational at idle state, the LED on the keypad will be lit in the red color. The beeper will operate quickly twice at start-up.

Each button on the keypad will emit a short beep note (depending on reader) to acknowledge each keypress.

Upon successful identification of a valid access code or card, a rapid sequence of 4 beeps will follow and LED will turn to green color for few seconds.

If a wrong code or card is used, a longer sequence of 3 slower beeps will follow and LED will stay in red color.

2. Keypad usage

The standard reader is a numeric keypad fitted on the system which has 12 blue back-illuminated buttons plus it has the functionality to read contactless RFID cards:

- 0 to 9 digits
- Star key (*)
- Enter key (ENT)

To enter a keycode, press the sequence of numeric digits followed by the Enter key.

Note: each key must not exceed 5 seconds interval from each other, otherwise the key sequence will be erased (see Timeout feature below).

The keypad surface is also used to read 125KHz RFID or 13.56MHz MIFARE (depending on reader type) cards. A green LED and a first beep tone will acknowledge whenever a recognized RFID format card is in proximity.

Extra functions

Erase code

To erase a wrongly entered key sequence prior to the enter key (ENT), press the ESC key.

Timeout feature

The entered key sequence will automatically erase after a period of inactivity if no enter (ENT) key is pressed and no numeric button is pressed within 5 seconds from last input. A short acoustic double beep tone will be produced to notify the timeout.

Input Lock-out feature

To protect the reader from brute force input attacks in rapid succession, the system is equipped with a lock-out time delay after a predefined number of repeated invalid access attempts.

See Appendix A for details about this feature.

Log on ungranted open door event

From firmware version 2.0, thanks to the fitted magnetic door switch, the system also features a logging functionality whenever the door is detected to be open without a valid input being entered. This is sent remotely to the server (internet access has to be present and system properly connected to the router) and thus saved on the database for activity logging purposes. This feature is useful to monitor any unauthorized door opening (lock violation or when the mechanical open overrides the electrical control).

3. Reset code

The reset code is a 8 digits long, hardcoded in source code (flash memory) and cannot be changed at user interface level. This code can be ignored through a configuration option (code is enabled by default) and has priority on top of the other possible configurable user codes.

The reset code will cause the microcontroller program to restart and will also initialize the EEPROM memory content to standard values (unless the corresponding option at user's configuration is disabled), erasing any previously stored user keys and cards settings.

See Appendix A for details about this feature.

Predefined state

In a freshly EEPROM memory reset state, the following condition and values are valid:

- Number of codes stored: 1
- Standard code length for the first PIN: 4
- Predefined PIN code: (See Appendix A for details about this code)
- Number of cards stored: 0

EEPROM permanent memory content can be initialized with the above factory values by using the respective button on the web interface configuration control panel, followed by a board reset (either by control panel or temporary power disconnection) or via soft reset code on the keypad.

4. Fixed codes

The first 3 codes can be configured as static codes (denoted as Code1, Code2 and Code3 in the modes below). They can be used for regular owners or administration purposes.

These codes are stored in the EEPROM memory and can only be changed at device control panel, from 1 to a maximum of 8 digits independently. A soft reset of the board (like temporary power disconnection) will retain the storage of these codes as well as all other customized user settings.

5. Fixed PIN + card (2-factor authentication access)

For an added level of security, a two-factor identification (numerical code + physical input) can be used by entering first a PIN code (denoted as Code4), followed by reading a specific card among the ones saved. The selected card is automatically taken as the first one in the list (marked as Card 1 in the system configuration webpage).

Note: the use of this card alone will not be recognized to grant access, while the other cards, if any saved, will still operate normally without this pin. When this PIN is not set, also the first card will operate as normal, without requiring any pin first.

So, if globally a PIN+Card only access is desired, all other PINs and cards must be disabled/removed.

6. Fixed plus Blink code

The 5th code is a special secure one, mix of fixed component which is set by the user, plus a variable part which must be entered interactively based on the system challenge provided to the user in front of the reader. The challenge will be provided immediately after the first (fixed) part has been entered correctly, followed by the ENT key. If no variable part is entered within a specific time window, then the code sequence is reset and a new code can be entered. The beeper will quickly beep twice to notify the expiry of such timeout, similarly to the keycode Timeout feature.

Please see Appendix A for details about the challenge and how to calculate the variable code part.

Such feature comes handy when in crowded places the risk of eavesdropping is high and so to avoid the risk of compromising the use of a fixed code.

7. Timed code

When active, the 6th PIN is a code which stays valid for a set duration of time from board power-up or from last PIN saving. This functionality is useful to avoid offline tampering. The validity duration can be changed on the configuration page of the webserver from 1 to 49 days (default: 30 days).

After such time the code rolls over to the next calculated one.

Note: this period of time is only counting while the board is kept powered up continuously and the PIN will therefore only change while powered up long enough to include the changing time window.

Please see Appendix A for further details.

The way the PIN is changed follows the same rule as per rolling code, see next chapter on Rolling code.

8. Rolling code

The rolling code (denoted as Code7) or One-Time-Code (OTC or OTP) is a special, changing code to be used as a single time access.

After a successful recognition of the rolling code sequence, the same code will not be valid anymore and will be replaced by the next code in the given order.

See Appendix A on confidential information for details about how the next code is generated from current one.

Length can also be freely set from 1 to 8 digits.

This functionality is useful when granting single access (e.g.: cleaning maid mode) or to prevent eavesdropping of the code.

9. Enabling rolling (hidden) code

This is a special code (denoted as Code8) and it is normally behaving like a fixed code.

However, once this code is set, it will enable an additional code (denoted as Code9, not visible in the PIN configuration page) to be recognized by the system.

This last additional code (Code9) is calculated from the current special code (Code8) the same way as the OTC (rolling) code explained in the previous chapter. Once this code (Code9) is entered, then the current special code (Code8) is replaced by this hidden one and the current hidden code is in turn replaced accordingly by a new one, calculated as before.

This feature is useful when handing over the access to a new user (e.g.: overtaking tenant), disabling at the same time the old code upon first usage of the hidden one.

10. Summary of possible keycodes

The following table summarizes all possible key codes available to the user, with their functional description:











Designation	Description	Notes
PIN1	 User defined code, fixed	See Appendix A for standard value
PIN2	 User defined code, fixed	
PIN3	 User defined code, fixed	
PIN4	 User defined code + Card1	Card1 will only be recognized after the PIN. If this PIN is not set, Card1 will operate normally
PIN5	 User defined code + blink code	Requires a further keypad input in response to a random blinking LED sequence - see notes
PIN6	 Timed variable code	Changing every set period of time
PIN7	 Single entry rolling code (OTP)	Valid only once, it changes to the next automatically after use
PIN8	 Code valid until PIN9 is used	Changes to PIN9 once that is used
PIN9	 Hidden PIN calculated from PIN8	PIN changes to next after use. Not active if no PIN 8 is set
Reset code	 Hardcoded, not changeable	Reset board and restore E ² PROM memory content to factory values - see Appendix A for configurable options

Table 1 - possible PIN codes and their respective operation modes. All codes can be up to 8 digits long.

11. Cards

Cards can be added and their enable state toggled individually from the Control Panel, Cards page. Depending on configuration, RFID or IC (MIFARE) Wiegand type cards are recognized by the keypad sensor. On this webpage the cards can also be permanently removed individually.

Both facility and card ID information are stored to match valid access cards data.

A maximum of 8 cards can be stored. On customer's request, the device firmware can be customized to accommodate more cards up to a maximum of 186.

12. Stealth card

A special card, pre-programmed by the manufacturer, is dedicated to restoring EEPROM content back to factory values and reset the board, similarly to the effect of the reset code. Likewise, this card has priority over all other user configured cards.

Contrary to the keypad reset code though, the stealth card behaves with the following differences:

- It cannot be ignored by user configuration
- It always erases memory content before resetting the board
- It does not beep on board reset, blinks the green LED 3 times instead

This feature comes handy as a “super-user” permanently enabled reset, for example in cases where the keypad reset code has been disabled by the user or forgotten, nonetheless an administrator physical recovery of the board is required. Also, this way is totally silent¹ and fast, as it does not require to remember a keycode and enter it, hence the name “stealth”.

13. Door latch activation

The door latch is powered by a +12V, max 1A current signal upon the following events:

- a valid keycode or card is detected; latch is energized and
 - stays active for about 5 seconds if door stays closed (lock-out prevent feature); LED turns green for the same time duration;
 - goes off as soon as the door is detected open within the above 5 seconds; LED turns green for whole time latch is active
- after the “Open Door lock” button is pressed on the control panel; latch is energized for about 2 seconds
- after the “Power lock until door open” button is pressed on the control panel; latch is energized until door is detected open or a maximum of 10 seconds

Lock-out prevent feature

A magnetic (reed) sensor switch is fitted, typically on the upper frame of the door, detecting whether the door is open or shut. This signal is used to trigger a timeout of about 5 seconds to keep the lock energized and allow the user to open the door within this time frame. After door is open, lock will disengage after about 0.2 seconds.

Fail-safe: In case this door sensor is not fitted or the sensor becomes defective, (for example, cable disconnection or reporting always an open-door state) then the lock engages as per door closed condition above (i.e.: up to the maximum duration, 5 seconds).

¹ Depending on the device used, the keypad might still produce a sound when detecting a card in its proximity.