



PITreader

- Control and signal devices

PILZ
THE SPIRIT OF SAFETY

This document is the original document.

All rights to this documentation are reserved by Pilz GmbH & Co. KG. Copies may be made for the user's internal purposes. Suggestions and comments for improving this documentation will be gratefully received.

Source code from third-party manufacturers or open source software has been used for some components. The relevant licence information is available on the Internet on the Pilz homepage.

Pilz®, PIT®, PMI®, PNOZ®, Primo®, PSEN®, PSS®, PVIS®, SafetyBUS p®, SafetyEYE®, SafetyNET p®, the spirit of safety® are registered and protected trademarks of Pilz GmbH & Co. KG in some countries.



SD means Secure Digital

1	Introduction	6
1.1	Validity of documentation	6
1.2	Using the documentation	6
1.3	Definition of symbols	6
1.4	Third-party manufacturer licence information	7
2	Overview	8
2.1	Device features	8
2.2	PITreader device view with base unit	9
3	Safety	10
3.1	Intended use	10
3.2	Safety regulations	10
3.2.1	Additional documents that apply	10
3.2.2	Use of qualified personnel	10
3.2.3	Warranty and liability	11
3.2.4	Disposal	11
4	Security	12
4.1	Implemented security measures	12
4.2	Required security measures	12
5	Function description	14
5.1	Authentication procedure	14
5.2	Authentication modes	14
5.2.1	Transponder data	14
5.2.1.1	Device groups	15
5.2.2	External	15
5.3	Authentication types "Basic" and "Single authentication"	18
5.4	Transponder key	18
5.4.1	Serial number of the transponder key	19
5.4.2	Transponder key's security ID (SID)	19
5.5	User data	20
5.5.1	System parameters	21
5.6	Coding	22
5.6.1	Basic coding	23
5.6.2	OEM coding	23
5.7	Block list	24
5.8	Real-time clock and operating hours counter	24
5.9	Modbus/TCP	24
5.9.1	LED control	24
5.9.2	Function codes (Client connections)	25
5.9.3	Modbus/TCP data areas	25
5.9.4	Data transfer limits	28
5.10	HTTP(S) connection	28
5.11	24 V I/O port	29
5.12	Connect the base unit to a safe evaluation unit	29

6	Install the base unit	30
6.1	General installation guidelines	30
6.2	Dimensions in mm	31
7	Wiring	32
7.1	Standalone	32
7.2	Base unit with safe evaluation unit	32
8	Configuration	33
8.1	Web application	33
8.2	Connect to PITreader	33
8.3	Manage certificates	34
8.3.1	Managing certificates	34
8.3.2	Incorporate certificate into a public key infrastructure (PKI)	35
8.4	Location description	35
8.5	Data logging with personal data	35
8.6	Set device group	35
8.7	Write/program transponder key	36
8.7.1	Program permissions	36
8.7.2	Configure the validity of the transponder key	36
8.7.3	Teach in transponder key to basic coding	36
8.7.4	Teach in transponder key to OEM coding	37
8.7.5	Limit transponder key to identically coded PITreader	38
8.7.6	Edit user data values	38
8.8	Set basic coding	39
8.9	Set OEM coding	39
8.10	Use block list	39
8.11	Configure user data	40
8.12	API Clients	41
8.13	Save and restore configuration	41
8.14	Reset to default settings	42
9	Firmware update	43
10	Operation	44
10.1	LED indicator	44
10.2	Safely decommission PITreader	45
10.3	Diagnostics	45
11	Technical details	46
12	Supplementary data	48
12.1	Radio approval	48
12.2	Network data	48
12.3	Overview of permissions	49
13	Order reference	51
13.1	Authentication system	51

13.2 Transponder key 51

13.3 Accessories 51

14 EC declaration of conformity 52

1 Introduction

1.1 Validity of documentation

This documentation is valid for the product PITreader. It is valid until new documentation is published.

This operating manual explains the function and operation, describes the installation and provides guidelines on how to connect the product.

1.2 Using the documentation

This document is intended for instruction. Only install and commission the product if you have read and understood this document. The document should be retained for future reference.

1.3 Definition of symbols

Information that is particularly important is identified as follows:



DANGER!

This warning must be heeded! It warns of a hazardous situation that poses an immediate threat of serious injury and death and indicates preventive measures that can be taken.



WARNING!

This warning must be heeded! It warns of a hazardous situation that could lead to serious injury and death and indicates preventive measures that can be taken.



CAUTION!

This refers to a hazard that can lead to a less serious or minor injury plus material damage, and also provides information on preventive measures that can be taken.



NOTICE

This describes a situation in which the product or devices could be damaged and also provides information on preventive measures that can be taken. It also highlights areas within the text that are of particular importance.



INFORMATION

This gives advice on applications and provides information on special features.

1.4 Third-party manufacturer licence information

This product includes Open Source software with various licences.

More detailed information is available in the web application of the PITreader by calling up the menu **Support -> Show legal information**.

The relevant source codes can be requested via opensource@pilz.de.

Your request should include the following: (a) the firmware name, (b) the firmware version, (c) your name, (d) your company name (if applicable), (e) your reply address and (f) your E-mail address (if possible).

Pilz can charge a fee for the data medium and for sending.

The request for the source code must be received 3 years at the latest after the receipt of the relevant MPL. Irrespective of this period we will send you a complete, machine-readable copy of the source code as long as Pilz offers spares or technical support for this device.

2 Overview

The product can be used with the following external components/systems:

- ▶ Transponder key (PITreader key) for authentication
- ▶ Web application on a PC for configuration
- ▶ Operator terminal (HMI) for authentication
- ▶ Safety controller (FS-PLC) for safe operating mode selection or authentication
- ▶ Safe evaluation unit (e.g. PIT m4SEU, order no. 402 250) for safe operating mode selection (only on PITreader base unit)

2.1 Device features

- ▶ System for authentication and authorisation on control systems
- ▶ Authentication is via transponder key
- ▶ Configurable via a web application
- ▶ Ethernet interface for Modbus/TCP
- ▶ LED to display device status

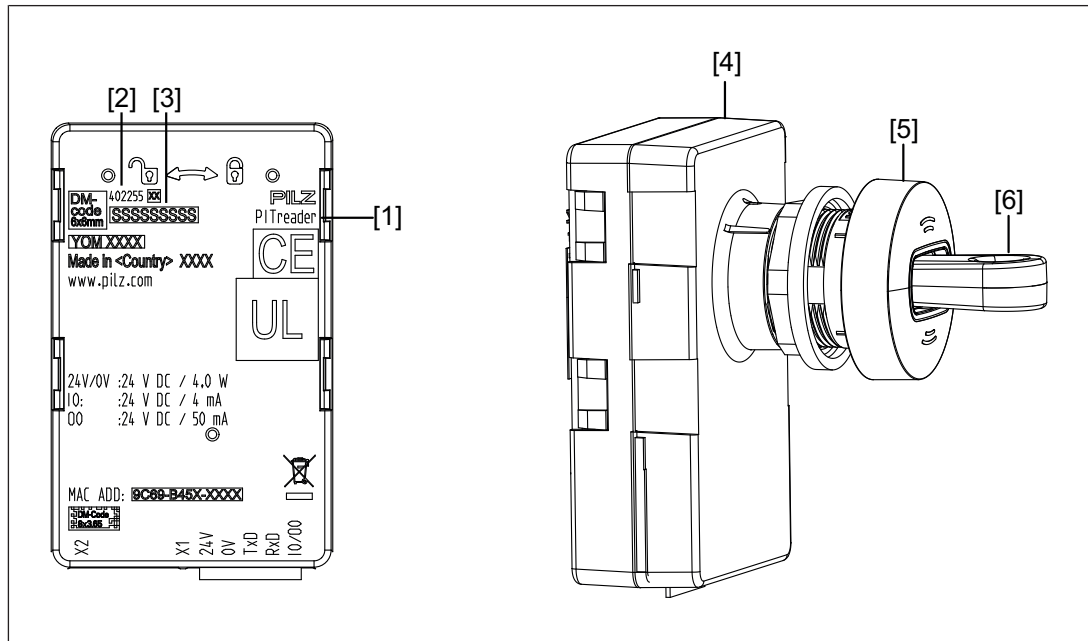
Only on PITreader base unit:

- ▶ Interface for connecting a safe evaluation unit (SEU) for operating mode selection
- ▶ For mounting cutouts D22 (diameter 22.3 mm +0.4 mm/-0.0 mm) in accordance with EN 60947-5-1 with anti-rotation device

Only PITreader S base unit type devices and versions of the PIT gb with the "X" extension in the device name (e.g. PIT gb XLLE y up ETH, PIT gb XLLE y down ETH):

- ▶ Integrated OPC Server UA

2.2 PITreader device view with base unit



Legend

- X1 Voltage supply, 24 V input/output and connection of a safe evaluation unit (PIT m4SEU)
- X2 Ethernet interface
- [1] Device description
- [2] Order number
- [3] Serial number
- [4] PITreader base unit, including spring-loaded terminal (order no. 402 255)
- [5] PITreader key adapter h (order no. 402 308)
- [6] PITreader key (see also [Transponder key](#)  18))

3 Safety

3.1 Intended use

The PITreader is a system for authentication and authorisation on control systems. Authentication is via transponder key.

The following is deemed improper use in particular

- ▶ Any component, technical or electrical modification to the product,
- ▶ Use of the product outside the areas described in this manual,
- ▶ Use of the product outside the technical details (see [Technical details](#) [ 46]).



NOTICE

EMC-compliant electrical installation

The product is designed for use in an industrial environment. The product may cause interference if installed in other environments. If installed in other environments, measures should be taken to comply with the applicable standards and directives for the respective installation site with regard to interference.

3.2 Safety regulations

3.2.1 Additional documents that apply

You should also read and take note of the following documents:

- ▶ Operating manual of the PITreader you are using
(e.g. PIT gb RLLE y up ETH, PIT gb RLLE y down ETH)
- ▶ Operating manual PITreader REST API
- ▶ Operating manual PITreader OPC Server UA

3.2.2 Use of qualified personnel

The products may only be assembled, installed, programmed, commissioned, operated, maintained and decommissioned by competent persons.

A competent person is a qualified and knowledgeable person who, because of their training, experience and current professional activity, has the specialist knowledge required. To be able to inspect, assess and operate devices, systems and machines, the person has to be informed of the state of the art and the applicable national, European and international laws, directives and standards.

It is the company's responsibility only to employ personnel who

- ▶ Are familiar with the basic regulations concerning health and safety / accident prevention,
- ▶ Have read and understood the information provided in the section entitled Safety
- ▶ Have a good knowledge of the generic and specialist standards applicable to the specific application.

3.2.3 Warranty and liability

All claims to warranty and liability will be rendered invalid if

- ▶ The product was used contrary to the purpose for which it is intended,
- ▶ Damage can be attributed to not having followed the guidelines in the manual,
- ▶ Operating personnel are not suitably qualified,
- ▶ Any type of modification has been made (e.g. exchanging components on the PCB boards, soldering work etc.).

3.2.4 Disposal

- ▶ When decommissioning, please comply with local regulations regarding the disposal of electronic devices (e.g. Electrical and Electronic Equipment Act).

4 Security

To secure plants, systems, machines and networks against cyberthreats it is necessary to implement (and continuously maintain) an overall industrial security concept that is state of the art.

Perform a risk assessment in accordance with VDI/VDE 2182 or IEC 62443-3-2 and plan the security measures with care. If necessary, seek advice from Pilz Customer Support.

4.1 Implemented security measures

- ▶ The web application is protected against unauthorised access by a password prompt.
- ▶ The password is saved in an encrypted format.
- ▶ If a password is changed, you will be prompted to enter the old password for authentication.
- ▶ Defend against CSRF attacks (Cross-Site Request Forgery) by assigning a unique token to a session.
- ▶ A user will automatically be logged out of the web application after 15 minutes of inactivity.

4.2 Required security measures

- ▶ The product is not protected against physical manipulation. We therefore recommend that you install the product in a lockable control cabinet or operator panel.
A safe evaluation unit PIT m4SEU may only be connected via the terminals TxD/RxD in the inside of a control cabinet or operator panel.
- ▶ The configuration computer that accesses the product has to be protected from attacks by a firewall or other suitable measures. We recommend that a virus scanner is used on this configuration computer and updated regularly.
- ▶ If necessary, protect the configuration computer and the product from unauthorised use by assigning passwords and taking further measures if required. We also recommend that the user logged on to this configuration computer does not have administrator rights.
- ▶ Ensure that the product is separated by a router (layer 3 switch or firewall) from the company network.
- ▶ Assign only safe passwords. When assigning passwords, please note:
 - The password should have at least 8 characters.
 - The password should contain upper and lower case characters, as well as special characters and numbers.
 - If possible, the password should not be available in dictionaries.
 - The password should not be made up of standard variants and repetitions or keyboard patterns (so not: 1234abcd).
 - Use a password manager for optimum management of complex passwords.
 - Language-dependent characters are not available in every keyboard language.
 - Make sure you regularly change the passwords of the user accounts on the system or ask the users to change their passwords themselves.
 - Make the users aware of the responsible use of their access data.

- ▶ Limit Modbus/TCP connections to the internal machine network. Secure the connection against external networks.
- ▶ As soon as possible, install firmware updates that Pilz provides for the product.
- ▶ Keep the transponder key in a safe place and protect it from unauthorised access. Advise users of the security risks of sharing transponder keys.
- ▶ Log data may contain personal data. Only store exported logs on a storage medium that is adequately protected.
- ▶ Before disposal, the product must be securely decommissioned. To do this, all the data must be deleted from the device.
 - Set the configuration back to its default settings or delete the configuration.
 - Switch off the product.

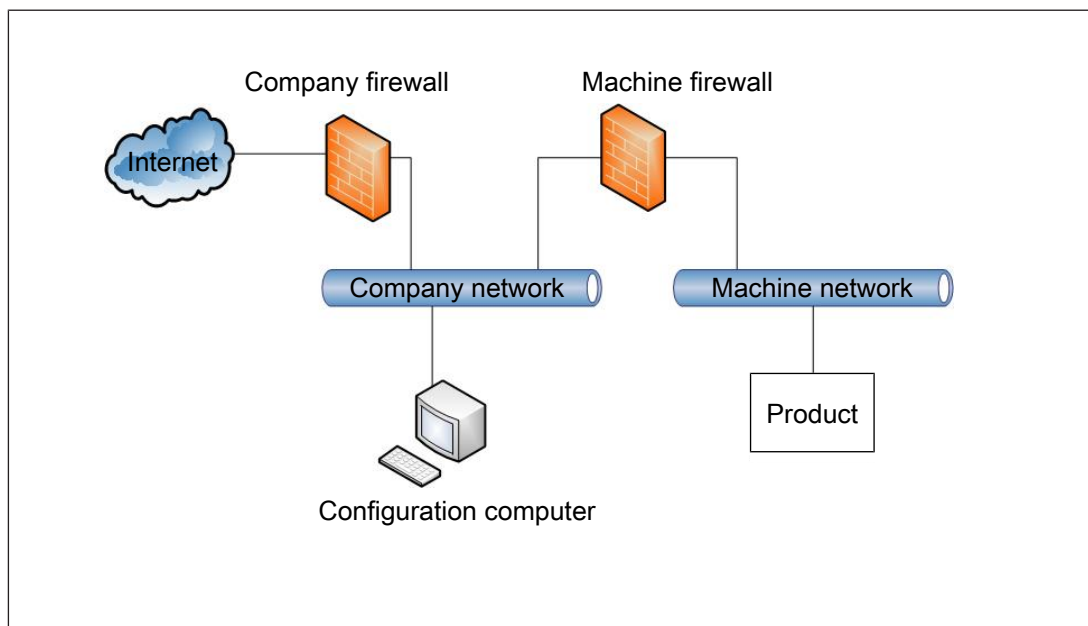


Fig.: Example network topology

- ▶ Note the [network data](#) [48] for risk analysis and the security measures.

5 Function description

5.1 Authentication procedure

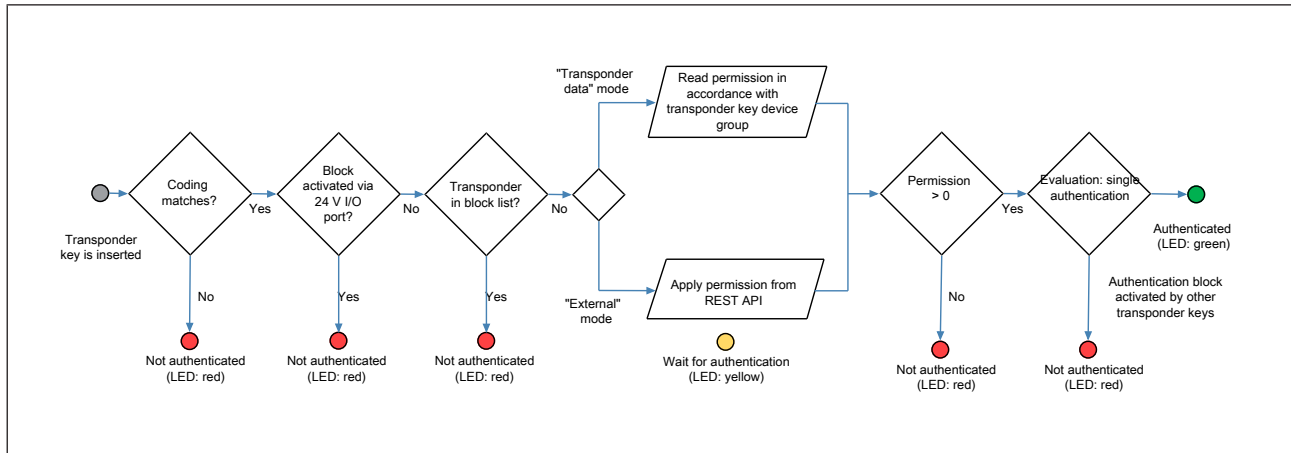


Fig.: Authentication procedure

5.2 Authentication modes

The PITreader supports two authentication modes:

► **Transponder data** [14]

Pre-defined, group-based authentication in the transponder key

► **External** [15]

Authentication takes place externally e.g. via PLC, HMI

When delivered, the transponder data authentication mode is set. The authentication mode can be changed in the web application.

5.2.1 Transponder data

In transponder data authentication mode, a user can authenticate himself on a safe evaluation unit (e.g. PIT m4SEU) and the connected control system by inserting a transponder key into the read area of the PITreader. Authentication is carried out using the permissions stored on the transponder key.

Safe operating mode selection can be implemented via a safe evaluation unit (e.g. PIT m4SEU) (only with PITreader base unit).

A controller (PLC, HMI) can use Modbus/TCP to read the transponder key that is currently authenticated.

**INFORMATION**

Please note that in transponder data authentication mode, authentication depends solely on possession of the transponder key. Loss of a transponder key can therefore lead to a security risk.

We recommend that you enter the security IDs of all the published transponder keys in a list, so that they can be transferred into the [Block list](#)  24] if they are lost.

5.2.1.1**Device groups**

There are 32 selectable device groups, G0 to G31.

PITreader devices are combined within a device group. One user (one transponder key) has the same permission on all PITreader devices within a group. Another user can have a different permission. Device groups can be used for a machine type, for example (in this case a user has the same permission on all turning machines, for example), see also [Set device group](#)  35].

One permission can be stored on a transponder key per device group. Each device group can have up to 65 different permissions.

- ▶ 0: No permission
- ▶ 1 to 64: Permission 1 to 64

For example a permission may relate to the enabling of functions, which can be assigned based on the level of training.

Permissions are code words for failsafe communication with a guaranteed minimum hamming distance. An overview of the code words for the permissions can be found under [Overview of permissions](#)  49].

Only one permission at a time is valid in the PITreader. Additional permissions stored on the transponder key can be called up via the Modbus/TCP interface of the PITreader and if necessary can be used for customer-specific purposes.

**INFORMATION**

By employing user data, the number of device groups can be extended to more than 32. A PITreader can be assigned to device group 0 ... 9999. Permissions for device groups 0 ... 31 can be stored on a transponder key as well as permissions for a maximum of 48 other device groups in the range 32 ... 9999. See [User data](#)  20].

5.2.2**External**

In external authentication mode, a user can authenticate himself on the connected control system or on the HMI by inserting a transponder key into the read area of the PITreader. The following connection options are available:

External authentication (Modbus/TCP)

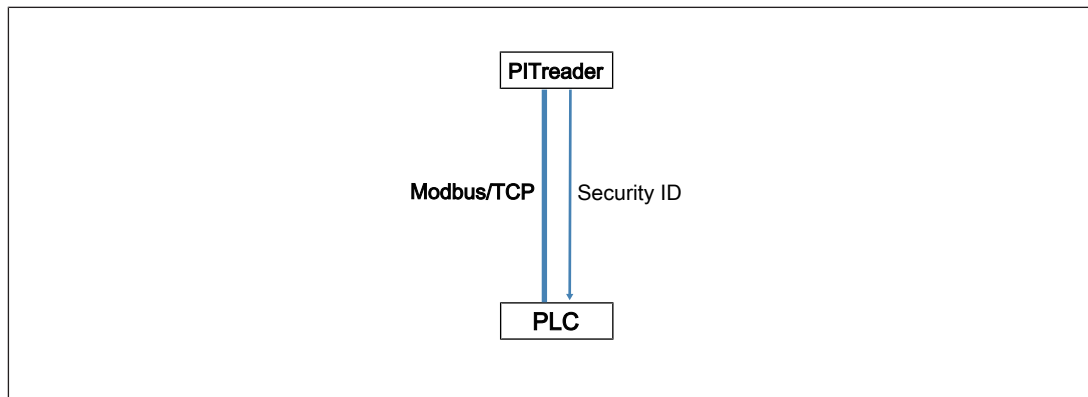


Fig.: External authentication (Modbus/TCP)

The PITreader provides the transponder key data via the Modbus/TCP connection. The permission for the user can be identified using a permission database (on the PLC) and the data from the transponder key (e.g. the security ID). The authentication is external (on the PLC).

No authentication takes place within the PITreader and the device LED lights up red when the transponder key is inserted.

To display the externally identified authentication status via the device LED, the colour and flash mode can be overwritten via the Modbus/TCP interface (see also [Modbus/TCP](#) [24]).



INFORMATION

A safe evaluation unit (e.g. PIT m4SEU) **cannot** be used in external authentication mode via Modbus/TCP.

External authentication (REST API)

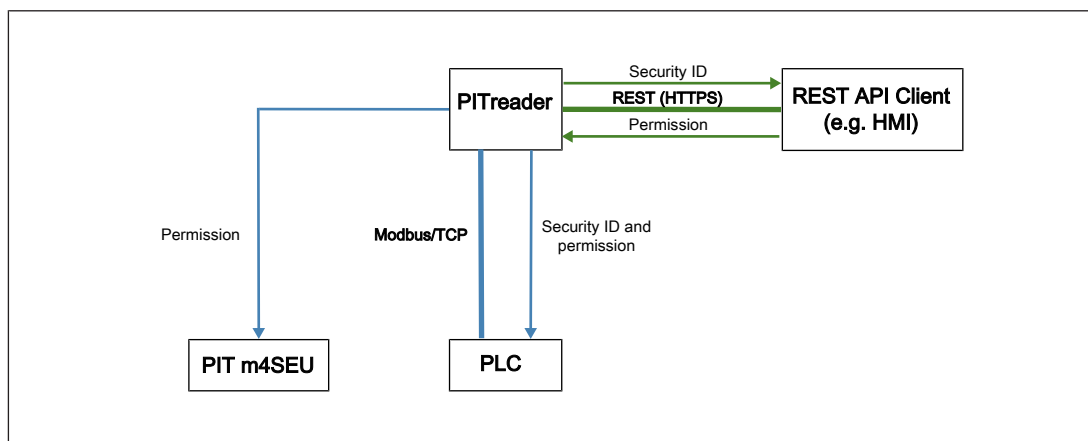


Fig.: External authentication (REST API)

The permission for the user can be identified using a permission database (on the PMI) and the data from the transponder key (e.g. the security ID).

Authentication is carried out in the PITreader and the authentication status is displayed via the device LED.

External authentication (OPC UA)

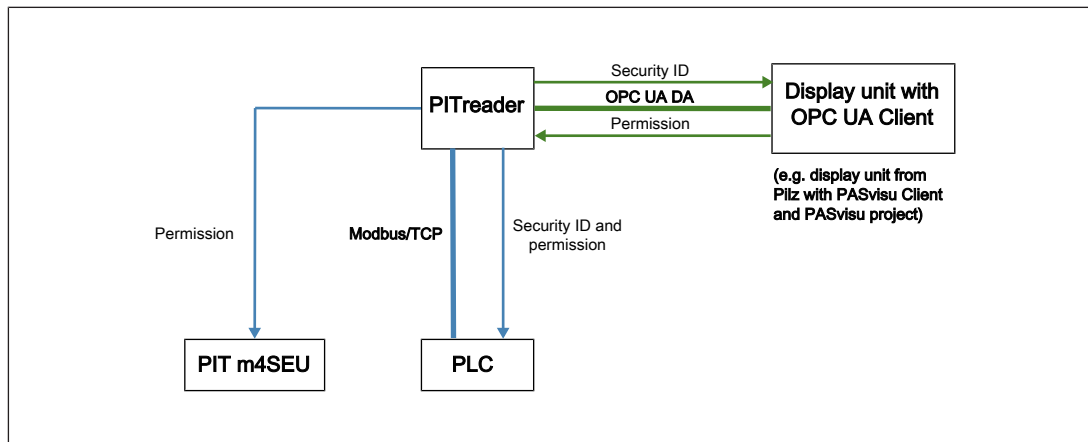


Fig.: External authentication (OPC UA)

The permission for the user can be identified using a permission database (on the OPC UA Client) and the data from the transponder key (e.g. the security ID).

Authentication is carried out in the PITreader and the authentication status is displayed via the device LED.

5.3 Authentication types "Basic" and "Single authentication"

The PITreader supports the following authentication types:

► Basic

The "Basic" authentication type includes the "Transponder data" and "External" authentication modes with all their functions and possibilities (see [Authentication modes](#) [📖 14]).

► Single authentication

The authentication type "single authentication" includes all the functions and possibilities of the "Basic" authentication type. Users also obtain special rights when "single authentication" is configured. Users can log in to a device using their transponder key in order to activate an authentication block for all other transponder keys. The authentication block remains activated until the same transponder key is used to log out. When the authentication block is active, the device LED lights up red.

Activate authentication block:

Log in for single authentication by inserting the transponder key on the PITreader. By logging in, an authentication block is activated for all other transponder keys. If the transponder key is removed, the authentication block remains activated.

Deactivate authentication block:

The authentication block is not deactivated until the same transponder key is used to log out. To log out, the same transponder key must be re-inserted and then removed again.

Note: The authentication block can also be reset via the web application. This requires administrator access rights to the web application. A reset via the web application will be logged.

5.4 Transponder key

The following types of transponder key are available (see also [Order reference](#) [📖 51]):

Designation	Permission	Serial number
PITreader key ye 1	Permission 1	01nnnnnnnn
PITreader key ye 2	Permission 2	02nnnnnnnn
PITreader key ye 3	Permission 3	03nnnnnnnn
PITreader key ye 4	Permission 4	04nnnnnnnn
PITreader key ye 5	Permission 5	05nnnnnnnn
PITreader key ye 5 service	Permission 5 (Service)	13nnnnnnnn
PITreader key ye g	Without pre-programmed permission	00nnnnnnnn

With the exception of "PITreader key ye g", all transponder keys are pre-programmed in the factory and the permission cannot be modified. The permission applies to all PITreader groups.

In the case of "PITreader key ye g", the permission for the PITreader groups can be modified and also locked as an option.

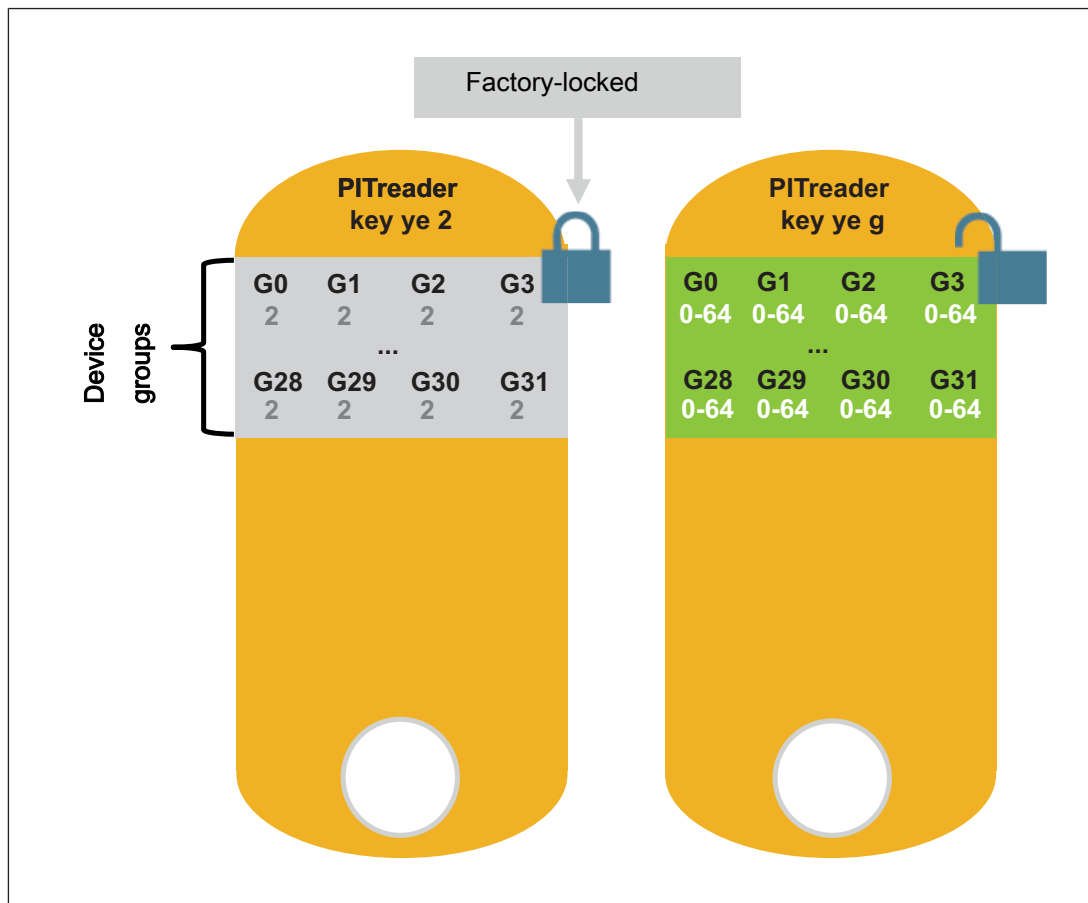


Fig.: Example of "PITreader key ye 2" and "PITreader key ye g"



NOTICE

When inserting the transponder key in the PITreader, make sure you can feel the transponder key lock in position.

5.4.1

Serial number of the transponder key

The serial number of the transponder key is composed of a prefix (2 digits) and a consecutive number (7 digits). When evaluating the serial number in an external system, make sure that the prefix and consecutive number are stored and communicated separately within the 4-byte serial number field (e.g. in the Modbus/TCP interface). The top byte contains the prefix, the lower 3 bytes contain the consecutive number.

5.4.2

Transponder key's security ID (SID)

All transponder keys are factory pre-programmed with a Security-ID (SID). A transponder key's security ID cannot be changed. A transponder key's security ID is a unique identifier, which is only valid for this one transponder key.

The security ID is used to uniquely identify a transponder key on the PITreader; i.e. a transponder key is authenticated on the PITreader with the help of the security ID. The permissions that are configured for a transponder key are linked to the security ID.

The security ID is displayed in the web application. In an application created by the user (e.g. evaluation and activation of the selected operating mode via HMI, web application, user software), the security ID can be read via Modbus/TCP, REST API or OPI UA. In such applications, the security ID should also be evaluated by the user and used for authentication.

Authentication can be blocked by entering a transponder key's security ID in a block list (see [Use block list](#)  39).

5.5 User data

A free data area is available on the transponder keys. Customer-specific data (e.g. language, user name, ...) can be stored in this free data area. The user data can also be used to extend the number of device groups to more than 32.

User data is organised in parameters. There are parameters whose function is determined by the user (user parameters) and there are system parameters. System parameters have a pre-defined function. See [System parameters](#)  21].

Each parameter has an ID, a name and a data type:

► Parameter-ID

The ID is a number in the range 1 ... 65535. It uniquely identifies a parameter.

Users can freely assign the ID.

Note: Users should not use IDs 1 ... 9999 because they might be used by Pilz for system parameters.

► Name

Users can freely assign the name.

► Data type

You can use the data types listed in the table. Each parameter value has the data length stated in the table. When a parameter is created, the type-ID is stated and not the name of the data type.

Type-ID	Name	Data length	Value range	Initial value
1	STRING	2 ... 255 Byte		Empty STRING
10	INT8U	1 Byte	0 ... 255	0
11	INT8S	1 Byte	-128 ... 127	0
12	INT16U	2 Byte	0 ... 65535	0
13	INT16S	2 Byte	-32768 ... 32767	0
14	INT32U	4 Byte	0 ... 4294967295	0
15	INT32S	4 Byte	-2147483648 ... 2147483647	0
20	DATETIME	4 Byte		Empty time/date
30	PERMISSION	4 Byte	0 ... 64 (Hamming-coded)	0

In order for the user data to be employed it must be configured on the PITreader. The individual parameters are created in the configuration. A maximum of 64 parameters can be created on the PITreader.

If parameters are created on a PITreader, the range of device groups extends from 0 ... 31

to 0 ... 9999. In order to use the groups 32 ... 9999, the system parameter with ID 1 must be created (see [System parameters](#)  21)).

This section describes how to configure the user data: [Configure user data](#)  40]

The values of the parameters are stored on the transponder key. Values for a maximum of 64 parameters and a maximum of 48 device groups can be stored on the transponder key. The data length of the values determines how many values can actually be stored. The more parameters are used, the fewer device groups are possible. The memory usage on the transponder key is displayed in the web application.

For each parameter, a separate value can be stored for each device group that's required (group number 0 ... 9999). To save memory it is possible to configure one default value per parameter. This default value will be used for all device groups 0 ... 9999, for which no separate value is configured.

This section describes how to write values for the parameters on a transponder key: [Edit user data values](#)  38].

The user data can be read from the transponder key via Modbus/TCP, via REST API or via the OPC Server UA (see operating manual PITreader REST API or PITreader OPC Server UA). The PITreader always returns just one value for a parameter, which is the value for the device group to which the PITreader belongs.

Should the parameter not exist on the transponder key, the data type's initial value is returned.

If the parameter exists on the transponder key but the device group does not, the default value is returned. If no default value is stored, the data type's initial value is returned.

5.5.1 System parameters

There are parameters with pre-defined functions. The ID and data type are specified for these parameters. Users may assign the name.

ID	Data type	Meaning
1	PERMISSION	Permission Permissions for device groups 32 ... 9999 Note: In the user data, permissions can also be defined for groups 0 to 31, but these are ignored. The permissions entered in the web application under Transponder -> Permissions always apply for device groups 0 to 31.
2	DATETIME	Start date Details of when the permission for a device group will start to be valid. This value can be defined for groups 0 ... 9999. Note: The start date is only evaluated if the Evaluate validity date option is activated for the PITreader.
3	DATETIME	End date Details of when the permission for a device group will cease to be valid. This value can be defined for groups 0 ... 9999. Note: The end date is only evaluated if the Evaluate validity date option is activated for the PITreader.

5.6 Coding

Through the coding process, PITreader devices can be restricted to recognising certain transponder keys coded with the same identifier.

There are two different codings:

- ▶ [Basic coding](#)  23]
- ▶ [OEM coding](#)  23]

The identifiers for both codings can be stored on a PITreader. Only the identifier for one of the codings can be stored on the transponder key.

The effect of the codings is the same, but they differ in the way the identifiers are changed and deleted on the PITreader and the way in which the transponder key is taught in.

Identifiers are safely stored within the device in a hardware security block. When transponder keys are taught in they are given a tamper-proof, cryptographic signature, which securely protects your system from manipulation and unknown transponder keys.

Teaching in a coded transponder key

If additional transponder keys are to be added to a PITreader that uses coding, the new transponder keys must be taught in on an appropriately coded PITreader before they are first used.



INFORMATION

If an (as yet) uncoded transponder key is inserted into the read area of the PITreader or the PITreader and transponder key are coded with different identifiers, the transponder key will not be read and the PITreader will indicate an error (LED flashes red). In this case the data from the transponder key will not be readable via the Modbus/TCP connection and there can be no (external) authentication of the transponder key.

Protection against unauthorised reading of a coded transponder key

Both coded and uncoded transponder keys will work on an uncoded PITreader; i.e. the data from a coded transponder key can also be read by an uncoded PITreader. To prevent this, a coded transponder key can also be configured so that reading is limited to identically coded PITreader devices (see [Limit transponder key to identically coded PITreader](#)  38]).

Monitoring the coding using a check sum

For both basic and OEM coding, a check sum can be used to monitor whether the coding in the PITreader has been changed.

Properties of the check sum:

- ▶ Data length of the check sum: 16 Byte
- ▶ If coding has not been set, then the check sum is 0.
- ▶ If coding has been set, then a check sum is calculated. The check sum is recalculated each time the coding is changed; i.e. each time the coding changes, the check sum changes.

The check sum can be read via Modbus/TCP or the REST API. The check sum is also displayed in the web application (see [Set basic coding](#) [39] and [Set OEM coding](#) [39]).

5.6.1 Basic coding

With basic coding, PITreader can only identify transponder keys that have the same basic identifier or, if appropriate, an OEM identifier (see [OEM coding](#) [23]).

For example, basic coding can be used to code a “company identifier”, which means that only internally coded transponder keys are identified.

Basic coding can be deleted from the device manually, without knowing the basic identifier. Basic coding is deleted automatically when the device is reset to its factory settings.

Basic coding is achieved by configuring the PITreader with a basic identifier (see [Set basic coding](#) [39]). Transponder keys are taught in to a basic identifier when permissions are written to the transponder key on a coded PITreader (see [Teach in transponder key to basic coding](#) [36]).

5.6.2 OEM coding

With OEM coding, a second identifier can be stored in the PITreader to check the transponder keys. PITreader devices with OEM coding accept transponder keys with the same OEM identifier or with the right basic identifier (see [Basic coding](#) [23]).

For example, machine manufacturers can use OEM coding to create one transponder key that service staff can use with all customers.

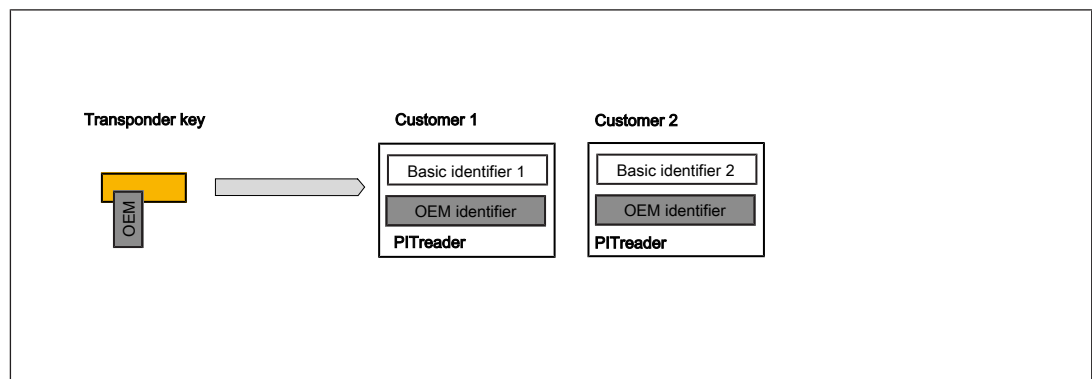


Fig.: OEM coding

OEM coding can only be deleted from the PITreader manually if the OEM identifier is entered. OEM coding is not deleted when resetting to the factory default settings. See also [Set OEM coding](#) [39].

New transponder keys with the OEM identifier can only be created by a person who knows the OEM identifier or who is using a PITreader that has been configured specifically for this purpose. See [Teach in transponder key to OEM coding](#) [37].

5.7 Block list

You can lock the authentication of certain transponder keys. Once a transponder key is in the block list, it can no longer be authenticated on the PITreader. This function can be useful, for example, when a user has lost his transponder key. It can stop unauthorised persons authenticating themselves on the PITreader.

The block list can be used in any authentication mode.

See also [Use block list](#)  39].

5.8 Real-time clock and operating hours counter

The PITreader has a real-time clock and an operating hours counter.

The real-time clock can be set to a new data/time value in the web application.

Synchronisation with an SNTP Server can be activated in the web application. If an SNTP Server has been configured, the very first synchronisation with the configured SNTP Server will occur after 10 seconds. Subsequently, synchronisation with the SNTP Server will be carried out in the time configured by the user.

5.9 Modbus/TCP

A Modbus/TCP connection to a controller (PLC, HMI) can be established via the Ethernet interface. Up to 4 Modbus/TCP connections are supported. The PITreader is always the connection Server (Modbus/TCP Slave).

The port number for data exchange via Modbus/TCP is configurable; the standard port number is 502.

The Modbus/TCP Server function can be deactivated in the web application.

5.9.1 LED control

The LED's colour and flash mode can be overwritten via the Modbus/TCP connection.

The LED colour can adopt one of the following values:

- ▶ 0 = switched off (default setting)
- ▶ 1 = blue
- ▶ 2 = yellow
- ▶ 3 = red
- ▶ 4 = green

The flash mode can adopt one of the following values:

- ▶ 0 = lit continuously (default setting)
- ▶ 1 = flashes slowly (1 Hz)

5.9.2 Function codes (Client connections)

The Modbus/TCP Server in the PITreader supports the following function codes (FC):

Function code	Function	
02	Read Discrete Input	The connection Client reads bit data from the connection Server, data length ≥ 1 bit, (receive data from 1x)
03	Read Holding Register	The connection Client reads word data from the connection Server, data length ≥ 1 word, (receive data from 4x)
04	Read Input Register	The connection Client reads word data from the connection Server, data length ≥ 1 word, (receive data from 3x)
06	Write Single Register	The connection Client writes to a word datum in the connection Server, data length = 1 word, (send data to 4x)
16	Write Multiple Registers	The connection Client writes to multiple word data in the connection Server, data length ≥ 1 word, (send data to 4x)

5.9.3 Modbus/TCP data areas



INFORMATION

On the PITreader, the addressing for Modbus/TCP data areas starts at "1".
On other devices, addressing may start at "0".
Please refer to the operating manual provided by the relevant manufacturer.

The product supports the following Modbus/TCP data areas:

► Discrete Inputs (Bit)

PITreader -> Modbus Client, bit access read (with FC02)

Address	Content
1x4001	Is authenticated (data from the transponder key)

► Input Register (Word/16 Bits)

PITreader -> Modbus Client, register access read (with FC04)

Address	Content
3x0001 ... 3x0002	PITreader order number (coded) Bits 31 to 24: Product group (00 = empty, 01 = G1) Bits 23 to 20: Revision (00 = empty) Bits 19 to 0: Product number Examples: PITreader base unit (402255): 0x 00 0 6234F PIT gb RLLE y up ETH (G1000020):: 0x 01 0 00014
3x0003 ... 3x0004	PITreader serial number
3x0005 ... 3x0006	Operating hours counter in minutes
3x0007 ... 3x0008	RTC time stamp, seconds since 01.01.2000 00:00 (UTC)
3x0009	LED colour (see also LED control [24])
3x0010	LED flash mode (see also LED control [24])
3x0011	Diagnostic status (all diagnostic messages are assigned a severity; severity 3 = error, severity 8 = warning, severity 13 = status information)
3x0013 ... 3x0016	PITreader order number (ASCII)
3x0017	PITreader revision (ASCII)
3x0019	SEU status information (see also operating manual PIT m4SEU, section 5.5) Default value if no SEU is connected: 0x00F0 (decimal: 240)
3x0025 ... 3x0028	Security ID (data from the transponder key)
3x0029 ... 3x0030	Reserved
3x0031 ... 3x0032	Permission (code word)
3x0033	Permission (integer, 0 to 64)
3x0034	Authentication status (0 = not authenticated, 1 = transponder authenticated successfully)
3x0035 ... 3x0036	Order number (transponder key)
3x0037 ... 3x0038	Serial number (transponder key) (see also Serial number of the transponder key [19])
3x0039	Reserved
3x0040	Reserved
3x0059 ... 3x0060	Group 0
3x0061 ... 3x0062	Group 1
3x0063 ... 3x0064	Group 2
3x0065 ... 3x0066	Group 3
3x0067 ... 3x0068	Group 4
3x0069 ... 3x0070	Group 5
3x0071 ... 3x0072	Group 6
3x0073 ... 3x0074	Group 7

Address	Content
3x0075 ... 3x0076	Group 8
3x0077 ... 3x0078	Group 9
3x0079 ... 3x0080	Group 10
3x0081 ... 3x0082	Group 11
3x0083 ... 3x0084	Group 12
3x0085 ... 3x0086	Group 13
3x0087 ... 3x0088	Group 14
3x0089 ... 3x0090	Group 15
3x0091 ... 3x0092	Group 16
3x0093 ... 3x0094	Group 17
3x0095 ... 3x0096	Group 18
3x0097 ... 3x0098	Group 19
3x0099 ... 3x0100	Group 20
3x0101 ... 3x0102	Group 21
3x0103 ... 3x0104	Group 22
3x0105 ... 3x0106	Group 23
3x0107 ... 3x0108	Group 24
3x0109 ... 3x0110	Group 25
3x0111 ... 3x0112	Group 26
3x0113 ... 3x0114	Group 27
3x0115 ... 3x0116	Group 28
3x0117 ... 3x0118	Group 29
3x0119 ... 3x0120	Group 30
3x0121 ... 3x0122	Group 31
3x0159 ... 3x0166	Check sum for basic coding
3x0167 ... 3x0174	Check sum for OEM coding
3x1000 ... 3x1519	User data (see also information below and User data  20)



INFORMATION

Values from the user data always start at register limits. With data that only requires a data width of 1 Byte, the actual value is written in the low byte and the high byte is filled with "0".

The address of the Modbus/TCP Register is displayed in the web application under **Configuration -> User data**. The address can also be calculated using the following formula:

$\text{Address}_n = \text{Address}_{(n-1)} + \text{RoundUp_2-Byte} (\text{Length}_{(n-1)})$

► Holding Register (Word/16 Bits)

Modbus Client -> PITreader, register access read (with FC03) and write (with FC06 or FC16)

Address	Content
4x6001	Overwrite colour (PITreader LED access)
4x6002	Overwrite flash mode (PITreader LED access)
4x6003	Activate (=1) or deactivate (=0) overwrite



INFORMATION

When reading data areas that contain no data, "0" is returned.

5.9.4

Data transfer limits

This table contains the maximum data lengths supported per telegram:

Data transfer		Max. data length per telegram
Read data (Bit)	FC 02 (Read Discrete Inputs)	1 ... 2000
Read data (Word)	FC 03 (Read Holding Registers)	1 ... 125
	FC 04 (Read Input Register)	
Write data (Word)	FC 06 (Write Single Register)	1 Word
	FC 16 (Write Multiple Registers)	1 ... 123 Words

5.10

HTTP(S) connection

A connection to a configuration computer can be established via the Ethernet interface. The PITreader can be configured via a web application and it is possible to read and write transponder keys (see also chapters entitled [Configuration](#)  33] and [Firmware update](#)  43]).

5.11 24 V I/O port

The PITreader has a 24 V I/O port. No function is assigned to the I/O port upon delivery. The I/O port can be configured either as an output or an input in the web application.

I/O port as output

If the I/O port is configured as an output, the current authentication status can be output via this output.

In the web application it is possible to set the minimum permission on the transponder key, from which point the output is to be switched on. If the permission on the transponder key is equal to or higher than the set permission, the output assumes the "1" state.

I/O port as input

If the I/O port is configured as an input, an authentication block can be activated via this input. The authentication block is active as long as 24 V is present at the input.

Note: The authentication block functions irrespective of the authentication type "single authentication" (see [Authentication types "Basic" and "Single authentication"](#)  18).

5.12 Connect the base unit to a safe evaluation unit

A safe evaluation unit PIT m4SEU can be connected to the PITreader via the terminals TxD/RxD of X1 (see also PIT m4SEU operating manual).

6 Install the base unit

6.1 General installation guidelines

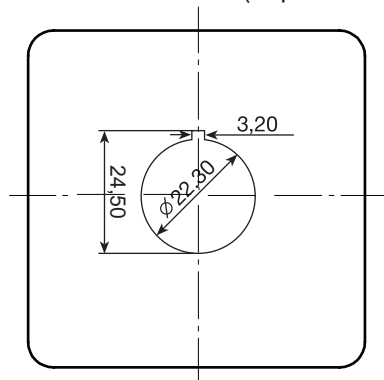


NOTICE

Damage due to electrostatic discharge!

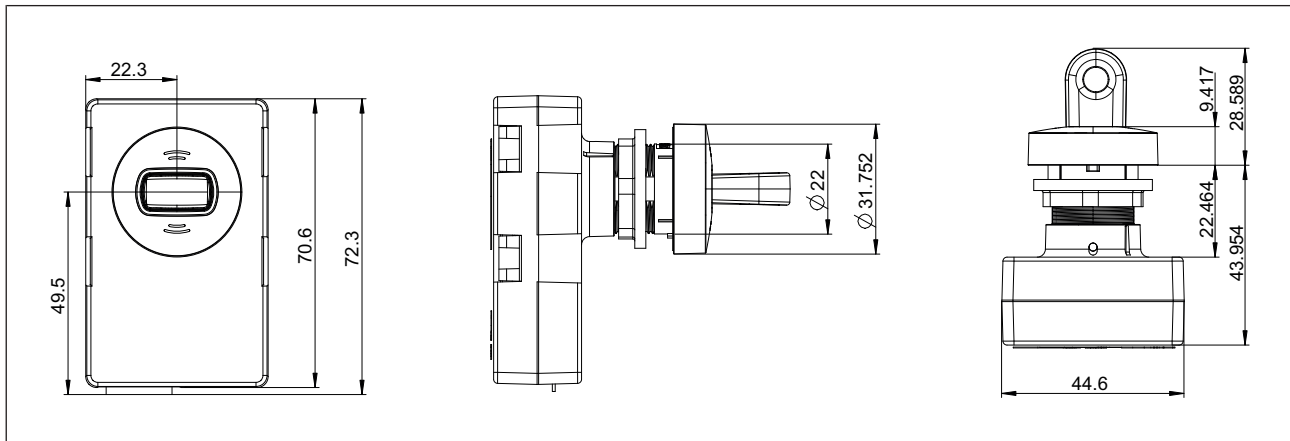
Electrostatic discharge can damage components. Ensure against discharge before touching the product, e.g. by touching an earthed, conductive surface or by wearing an earthed armband.

- ▶ Install the device in the front panel of a control cabinet or in a control console.
Material thickness:
 - non-metallic: 2 ... 6 mm
 - metal: 2 ... 4 mm.
- ▶ Provide the front panel of the control cabinet or control console with a mounting cutout (Ø 22.3 mm +0.4 mm/-0.0 mm, D22 in accordance with EN 60947-5-1) and give the cutout a recess for the latch (to protect against twisting):



- ▶ Guide the PITreader key adapter h (order no. 402 308) into the mounting cutout and secure it from the other side using a plastic nut (M22). Note the torque setting of 1.3 ... 2.1 Nm. We recommend that you use the installation wrench "PIT es wrench" for fixing the plastic nut (see [Order reference](#)  51]).
- ▶ Plug the PITreader base unit (order no. 402 255) on to the neck of the PITreader key adapter h (order no. 402 308) and turn it 15° clockwise until it locks into position.

6.2 Dimensions in mm



7 Wiring

7.1 Standalone

Follow the instructions below:

1. Connecting the supply voltage

⇒ Connect the supply voltage to X1 (Pin "24V" and "0V").

It is essential to note:

The power supply must meet the regulations for extra low voltages with protective electrical separation (SELV, PELV).

The cables for the device's supply voltage must be fitted with a 4 A fuse, characteristic B/C.

2. Connect the PITreader to a controller (PLC, HMI) via the Ethernet interface (X2).

7.2 Base unit with safe evaluation unit

Follow the instructions below:

1. Connect the PITreader to a safe evaluation unit PIT m4SEU (see also PIT m4SEU operating manual).

8 Configuration

8.1 Web application

The PITreader is configured via a web application. Configuration is only possible after logging in to the web application.

The web application is available in German and English.

System requirements:

The web application is called up via a standard browser.

The following web browsers are supported:

- ▶ Microsoft Internet Explorer (IE), from Version 10
- ▶ Microsoft Edge, all versions
- ▶ Mozilla Firefox, from Version 52
- ▶ Google Chrome, from Version 48

Other web browsers may work, but have not been tested.

A secure connection to the PITreader can be established via HTTPS. The PITreader supports HTTPS connections with TLS v1.2.

8.2 Connect to PITreader

The following section describes the typical procedure for creating a connection to the PITreader and for opening the web application.

1. Establish Ethernet connection

- ⇒ Connect the configuration PC directly to the Ethernet interface X2 of the PITreader.

2. Adjust IP address of the configuration PC

To access the PITreader, the IP address of the PC has to be in the same subnet as the IP address of the PITreader.

Default setting PITreader :

IP address: 192.168.0.12

Netmask: 255.255.255.0

- ⇒ Change the IP address in the network settings of your configuration PC.

3. Call up web application

- ⇒ Start the web browser and enter the IP address of the PITreader.

If a certificate error is displayed in the internet browser, temporarily add an exception rule and/or circumvent this warning message to still access the web application (see also [Manage certificates](#)  34).

The start page is displayed. To make changes to the configuration you will need to log in to the web application.

4. Log in to the web application

⇒ Right-click on **Login** in the top right corner and enter the user name and password.

Default credentials:

User name: admin

Password: <Serial number of the PITreader> (the serial number is on the bottom of the device (see [PITreader device view with base unit](#) [📖 9]).

After 5 failed attempts, login will be locked for 5 minutes.

5. Change initial password

The message "The default password has not been changed" is displayed. Change the initial password under **User -> Change password**. Enter a secure password with at least 8 characters (for features of a secure password see [Security](#) [📖 12]).

6. Change network settings

To integrate the PITreader into an existing network, change the network settings of the PITreader. The settings are adapted in the web application under **Configuration -> Settings**. Click on **Save** to apply the changes.

7. Start web application with the new IP address

When the network settings have been changed the PITreader restarts and is then accessible under the new IP address.

8.3 Manage certificates

8.3.1 Managing certificates

The PITreader uses X.509 certificates to secure communication between the device and the web application. By default the system uses a self signed server certificate. This certificate is generated automatically by the PITreader.

To enable communication, the certificate is downloaded from the web application to the PC and is checked by the web browser. If you use a self-signed certificate, you will be warned that the connection is not secure when you try to establish a connection to the PITreader. In order to establish a connection, you must add a security exception rule to your web browser.



CAUTION!

Risk of data manipulation

Possible loss of data security.

You may add a security exception rule to your web browser only if you are sure that you are communicating with the PITreader.

Alternatively you can download the current certificate for the PITreader's HTTPS connection under **Settings -> Certificate** in the web application and import it into the web browser.

New certificates are generated when the PITreader is reset to its factory settings.

You can also upload a separate server certificate with private key.

Certificates and private keys are not part of the device configuration and cannot be downloaded to other devices using the function **Save configuration/Restore configuration**.

8.3.2 Incorporate certificate into a public key infrastructure (PKI)

To incorporate a PITreader into an existing public key infrastructure you can either upload a separate server certificate to the device together with its private key or download a certificate signing request (CSR) from the PITreader, import it into your existing PKI and upload the signed certificate back to the device.

Certificates can be loaded on to the device in PEM (certificate or certificate + private key) or DER format (certificate only).

The device supports certificates based on one of the following cryptographic processes:

- ▶ ECC (prime256v1, secp256r1 or NIST P-256), **recommended**
- ▶ RSA (2048 Bit)

8.4 Location description

In the web application, under **Configuration -> Settings -> Location description**, you can enter a description of the location of the PITreader. A maximum of 47 characters are permitted.

8.5 Data logging with personal data

In the web application you can select whether personal data (security ID, user and IP address) is to be logged in the diagnostic log under **Configuration -> Settings -> Function**. This function is activated in the default configuration.

8.6 Set device group

In the web application, under **Configuration -> Settings -> Function**, you can assign a device group to the PITreader (see also [Device groups](#)  15). Under **Configuration -> Device groups** you can enter a name for each of the device groups from 0 ... 31. A maximum of 47 characters are permitted. If you have entered a name for a device group, when you assign the device group under **Configuration -> Settings -> Function**, the corresponding name is displayed in the selection list. If no name has been entered, the number of the device group is displayed.

8.7 Write/program transponder key

8.7.1 Program permissions

In the web application you can read the permissions for the transponder key (under **Transponder -> Data**) and write permissions for the transponder key (under **Transponder -> Permissions -> Programming**).

You have the option to adopt the same permission for all device groups (default setting) or to assign a different permission for each of the 32 device groups (uncheck **Apply to all**). You also have the option to lock the permissions on the transponder key, thereby preventing the permissions being changed at a later date.



NOTICE

Please note:

- Once a transponder key has been locked, no changes can be made to the group permissions.
- The lock cannot be cancelled.

If you have set a basic identifier, the transponder key will also be automatically taught in to the basic coding of the PITreader when writing/programming the permissions.

8.7.2 Configure the validity of the transponder key

You can limit the validity of transponder keys to a certain time period. To do this go to **Configuration -> Settings -> Function**, activate **Evaluate validity date** and set the valid time zone. The selected time zone is only used to evaluate the validity date.

You can enter a start date and an end date for the validity of the transponder key (in the format day, month, year "DD.MM.YYYY") under **Transponder -> Permissions**.

8.7.3 Teach in transponder key to basic coding

If you are using an unlocked transponder key and have set a basic coding, you can teach in the transponder key to basic coding under **Transponder -> Permissions -> Program**.

If you are using a locked transponder key or a transponder key that Pilz has pre-programmed in the factory and you have set a basic identifier, you can teach in the transponder key to the basic coding under **Transponder -> Data -> Teach in transponder**.

You can change the basic coding by teaching in the transponder key to a different basic coding. You can remove the basic coding by rewriting the permissions on the transponder key on a PITreader without a set basic coding.

8.7.4 Teach in transponder key to OEM coding

You can teach in a transponder key to OEM coding in exactly the same way as you teach in basic coding, see [Teach in transponder key to basic coding](#) [36]. All you do is enter the OEM identifier instead of the basic identifier.

The screenshot displays the PITreader web application interface. At the top, there is a yellow header with the text 'PITreader'. Below this is a navigation bar with two tabs: 'Configuration' and 'Coding'. The 'Coding' tab is currently selected. On the left side, there is a vertical sidebar with various menu items: 'Status', 'Configuration', 'Settings', 'Coding', 'Block list', 'Certificate', 'API Clients', 'Device groups', 'User data', 'Transponder', 'User', 'Diagnostics', 'Maintenance', and 'Support'. The main content area is titled 'Coding' and is divided into two sections: 'Basic coding' and 'OEM coding'. Each section contains three input fields: 'Status' (which is pre-filled with 'Not set'), 'Identifier', and 'Comment'. Below these fields is a 'Set coding' button. In the 'Basic coding' section, the 'Identifier' field contains the text 'myOEM_Code', and a blue arrow points to this field. The 'OEM coding' section is currently empty, with all fields being blank.

Fig.: Teach in transponder key to OEM coding

As a machine manufacturer, if you wish to code transponder keys for service staff, ideally you should use a PITreader that is only used for this purpose.

This guarantees that new transponder keys with the OEM identifier can only be created by a person who knows the OEM identifier or who is using a PITreader that has been configured specifically for this purpose.

8.7.5 Limit transponder key to identically coded PITreader

You can prevent the data from a coded transponder key being read by an uncoded PITreader. You can limit coded transponder keys to identically coded PITreader devices through the configuration. You can configure this option for transponder keys with both basic and OEM coding.

If you wish to limit coded transponder keys to identically coded PITreader devices, then go to **Transponder -> Data**, select **Limit to PITreaders that are identically coded** and then click on **Program**.

8.7.6 Edit user data values

The web application can be used to display the values of the parameters on the transponder key. The values can be changed.

All actions are carried out under **Transponder -> User data**.

Notes:

- ▶ The web application always displays the parameters that are created on the PITreader (see [Configure user data \[40\]](#)). If there are more parameters on the transponder key, these will be ignored. If there are fewer parameters on the transponder key, the data type's initial value is displayed for the parameters that are missing.
When the user data is saved on the transponder key, all existing user data is overwritten.
- ▶ Under **Transponder -> User data**, the web application also shows how much of the memory for the user data is already occupied on the transponder key.
- ▶ Permissions for device groups
If you have increased the number of device groups to more than 32, you can enter permissions for groups 0 to 31 in the user data, but these will be ignored. For device groups 0 to 31, the permissions entered under **Transponder -> Permissions** always apply.

8.8 Set basic coding

You can code the PITreader by going to **Configuration -> Coding** in the web application, entering an **Identifier** in the **Basic coding** area and clicking on the **Set coding** button. A comment field is also available, which you can use to enter a comment about your basic coding. Both fields are limited to a max. 63 characters.

After you have coded the PITreader, the information **Basic coding set** is displayed under **Status** and the corresponding check sum is displayed under **Check sum**. You have the option to delete or change the basic coding.

The comment about the basic identifier can be adapted retrospectively and can be saved in the device via the **Save comment** button.



INFORMATION

Once set, the basic identifier can no longer be read or displayed. The comment field can therefore be used to store a hint for the set basic identifier.

See also [Coding](#) [📖 22].

8.9 Set OEM coding

You can code the PITreader with an OEM identifier by going to **Configuration -> Coding** in the web application, entering an **Identifier** in the **OEM coding** area and clicking on the **Set coding** button. A comment field is also available, which you can use to enter a comment about your OEM identifier. Both fields are limited to a max. 63 characters.

After you have coded the PITreader, the information **OEM coding set** is displayed under **Status** and the corresponding check sum is displayed under **Check sum**. You have the option to delete the OEM coding or to change the OEM coding. To do this you will need to enter the current OEM identifier.

The comment about the OEM identifier can be adapted retrospectively and can be saved in the device via the **Save comment** button.



INFORMATION

Once set, the OEM identifier can no longer be read or displayed. The comment field can therefore be used to store a hint for the set OEM identifier.

You will need to code all PITreader devices that you supply to your customer with this OEM identifier.

See also [Coding](#) [📖 22].

8.10 Use block list

You can lock the authentication of certain transponder keys by entering the security IDs of these keys (and a comment as an option) under **Configuration -> Block list**.

You can export the block list to a CSV file or import a block list. When importing, please note the following:

- ▶ The CSV file must contain two columns. The first column must contain the security ID and the second column the comment.
- ▶ The first line of the CSV file can contain column headings and is skipped during import.
- ▶ Each security ID may appear only once in the block list. Before importing you should check that there are no duplicated entries in the CSV file.
- ▶ Fields and values may be framed in quotation marks ("). If a field or value contains a quotation mark, the whole field must be framed in quotation marks and the quotation marks inside the field duplicated.
- ▶ A semicolon is used as the separator.
- ▶ During import, the imported entries replace all the block list entries in the web application.

See also [Block list](#) [ 24].

8.11 Configure user data

In order for the user data to be employed, the parameters must be created on the PITreader. This can be done using the REST API (see operating manual PITreader REST API). Alternatively, a configuration file with the parameters can be imported in the web application.

The configuration file is imported in the web application under **Configuration -> User data**. The configuration file is a JSON file, which can be created and edited using any text editor.

For example, if you should create a parameter with the parameter-ID 10000, the name "my-Parameter", the STRING data type (type ID = 1) and a maximum number of 30 characters, the configuration file will contain the following:

```
{
  "version": 1,
  "comment": "Custom example",
  "parameters": [
    { "id": 10000, "name": "myParameter", "type": 1, "size": 31 }
  ]
}
```

"size" only needs to be stated with the STRING data type. The stated number of characters is 1 greater than the desired number of characters.

The parameters currently available on the PITreader are displayed in the web application under **Configuration -> User data**. The user data can be versioned. A comment may be added to the version. The comment may contain all valid UTF-8 characters.

The parameters currently created on the PITreader can be exported to a configuration file.



INFORMATION

If you only wish to extend the number of device groups to more than 32, you can use the JSON file supplied with the firmware update as the configuration file. You can simply import the file.

8.12 API Clients

Under **Configuration -> API Clients** you can create appropriate connection settings for automated access to device data via the HTTPS interface. A detailed description can be found in the separate document “Operating manual PITreader REST API”.

8.13 Save and restore configuration

All the settings that have been made in the web application can be saved in a file. To do this go to **Maintenance -> Save** in the web application and click on **Save configuration**.

If you have saved a configuration on the computer, then you can restore the configuration by uploading the backup file in the web application. To do this go to **Maintenance -> Restore** and click on **Restore configuration**.

The backup contains the settings, the block list, the names of the device groups and the user data configuration. TLS certificates, OPC UA certificates and coding identifiers are not included in the backup and cannot be restored.

8.14 Reset to default settings

The PITreader base unit can be reset to its factory default settings via a short circuit at the terminals TxD/RxD or in the web application. Different data is deleted depending on which type of reset is selected.

Short circuit at the terminals TxD/RxD

The configuration data (including coding) and the block list are reset.

Follow the instructions below:

1. Before booting the device, create a short circuit at the terminals TxD and RxD.
The LED lights up yellow, the device does not boot.
2. Remove the short circuit.
The LED flashes yellow.
3. Recreate the short circuit within 10 seconds.
The LED lights up yellow and the device is reset to its factory default settings.



NOTICE

If the short circuit is not recreated within 10 seconds, the PITreader will start up without the configuration data having been reset to the factory default settings.

4. If the device has successfully been reset to the factory default settings, the LED lights up green.
5. Remove the short circuit
The LED no longer lights up yellow / green and the boot process is continued.



INFORMATION

The description of how to reset the PITgatebox to the factory default settings using PITreader can be found in the operating manual PIT gb RLLE y ETH.

In the web application

In the web application you can choose which data to reset.

The following data can be reset to the factory default settings in the web application:

- ▶ Device configuration
- ▶ Diagnostic log
- ▶ Transponder block list
- ▶ Names of device groups
- ▶ Configuration of user data

Follow the instructions below:

Go to **Maintenance -> Factory reset**, click on **Reset to factory default settings** and select the data you wish to reset.

9 Firmware update

If a new firmware version is available, the firmware of the PITreader can be updated. The update is carried out in the web application under **Maintenance -> Update firmware**.

An update package can be downloaded to the device from the download area on the Pilz website. There are two different file extensions, .fw and .fwu. The Web application shows what update package with what file extension is to be used with your device.

It is not possible to install a firmware version that is older than the one currently active in the PITreader.



NOTICE

Update the firmware regularly to obtain security-related updates.

10 Operation

10.1 LED indicator

Legend



LED on



LED flashes

Colour	State	Meaning
Yellow		Device is starting up or the firmware is being updated (if the device is re-starting after uploading a firmware update and the firmware update is being applied, the LED flashes yellow)
Yellow		Device is in external authentication mode and as yet no authentication has been set for the inserted transponder key
Blue		Device is ready for operation, no transponder key has been inserted
Green		Transponder key has been recognised as valid
Red		Transponder key has been recognised as invalid Possible reasons: ▶ When the transponder key is inserted: Authentication is denied (e.g. permission = 0). ▶ When the transponder key is not inserted: Authentication on the device is blocked (e.g. via 24 V I/O port or single authentication) You'll find further information in the web application under Status -> Authentication
Red		Error (e.g. hardware error, configuration error, invalid or uncoded transponder key, ...). Possible remedies in the event of a configuration error, when the device is no longer accessible under the set IP address: ▶ Try to open the web application with the default IP address or ▶ Reset the device to its factory default settings.

If the PITreader is reset to its default settings via a short circuit at TxD/RxD, the LED assumes the following states:

Description	Colour	State
Short circuit is present	Yellow	
Short circuit is removed		
Short circuit is recreated, the device is reset to its default settings		
The device has successfully been reset to its default settings	Green	

See also [Reset to default settings](#)  42].

10.2 Safely decommission PITreader

Before disposal, the PITreader must be safely decommissioned. To do this, all the data must be deleted from the device.

Follow the instructions below:

- ▶ Reset the configuration to the default settings as described in the chapter entitled [Reset to default settings](#)  42].

10.3 Diagnostics

Diagnostics on the PITreader are performed via

- ▶ The LED
- ▶ Diagnostic list and diagnostic log

You can read the diagnostic list and diagnostic log in the web application under **Diagnostics**.

Under **Log** you can use a filter to set whether **All message types** or only **Audit trail messages** (messages about the process cycle) are to be displayed. You can create a backup of the diagnostic messages selected in the filter via the **Export log** button. A CSV file is created during export.

If you have connected a safe evaluation unit PIT m4SEU, all the information is logged via the PIT m4SEU's status information interface.

11 Technical details

General	
Certifications	CE, FCC, IC, UL/cUL
Sensor's mode of operation	Transponder
Transponder	
Energy supply to transponder	passive (battery free)
Frequency band	13,24 - 13,88 MHz
Max. transmitter output	170 mW
Electrical data	
Supply voltage	
Voltage	24 V
Kind	DC
Type of power supply	SELV/PELV
Voltage tolerance	-15 %/+20 %
Output of external power supply (DC)	4 W
External unit fuse protection F1	4 A, circuit breaker 24 V DC, characteristic B/C
Status indicator	LED
Power dissipation	2,5 W
Inputs	
Signal level at "1"	15 - 30 V DC
Input current range	4 mA
Galvanic isolation	No
Semiconductor outputs	
Overall performance ext. loading, semiconductor	1,2 W
Number	1
Switching current per output	50 mA
Galvanic isolation	No
Short circuit-proof	yes
Ethernet interface	
Number	1
IP address, factory setting	192.168.0.12
Connection type	RJ45
Transmission rate	10/100 Mbit/s
Times	
Supply interruption before de-energisation	10 ms
Environmental data	
Ambient temperature	
In accordance with the standard	EN 60068-2-14
Temperature range	-20 - 55 °C
Storage temperature	
In accordance with the standard	EN 60068-2-1/-2
Temperature range	-25 - 70 °C

Environmental data

Climatic suitability

In accordance with the standard	EN 60068-2-78
Humidity	93 % r. h. at 40 °C

Max. operating height above sea level	2000 m
---------------------------------------	---------------

EMC	EN 301489-1 V2.1.1
-----	---------------------------

Vibration

In accordance with the standard	EN 60068-2-6
Frequency	5 - 8,4 Hz, 8,4 - 150 Hz
Amplitude	3,5 mm
Acceleration	max. 1g

Shock stress

In accordance with the standard	EN 60068-2-27
Acceleration	15g
Duration	11 ms

Protection type

In accordance with the standard	EN 60529
Housing	IP20
Front	IP65/IP67
Mounting area (e.g. control cabinet)	≥ IP54

Mechanical data

Mounting position	Any
-------------------	------------

Material

Bottom	PC
Front	PC

Connection type	Spring-loaded terminal, plug-in
-----------------	--

Mounting type	plug-in
---------------	----------------

Max. torque setting for fixing screws	1,3 - 2,1 Nm
---------------------------------------	---------------------

Conductor cross section with spring-loaded terminals:

Flexible with/without crimp connector	0,2 - 1,5 mm², 24 - 14 AWG
---------------------------------------	-----------------------------------

Spring-loaded terminals: Terminal points per connection	1
---	----------

Stripping length with spring-loaded terminals	8 mm
---	-------------

Dimensions

Height	54 mm
Width	72 mm
Depth	45 mm

Weight	47 g
--------	-------------

Where standards are undated, the 2018-12 latest editions shall apply.

12 Supplementary data

12.1 Radio approval

FCC/IC approval

USA/Canada



FCC ID: VT8- PITRD01
IC: 7482A- PITRD01

FCC/IC-Requirements:

This product complies with Part 15 of the FCC Rules and with Industry Canada licence-exempt RSS standards.

Operation is subject to the following two conditions:

- 1) this product may not cause harmful interference, and
- 2) this product must accept any interference received, including interference that may cause undesired operation.

Changes or modifications made to this product not expressly approved by Pilz may void the FCC authorization to operate this equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Le présent produit est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- (1) le produit ne doit pas produire de brouillage, et
- (2) l'utilisateur de le produit doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

12.2 Network data

Log	Direc- tion	Trans- port log	Port no.	Can be deactiv- ated	Description
HTTP	In	TCP	1 ... 65535 Default: 80	No	Web application: Browser is always forwarded to HTTPS
HTTPS	In	TCP	1 ... 65535 Default: 443	No	Web application: Transport protection by TLSv1.2. Access to the web application via user name and password. The server is authenticated via an X.509 certificate.
Modbus TCP	In	TCP	1 ... 65535 Default: 502	Yes	Modbus/TCP Server
NTP	Out	UDP	1 ... 65535 Default: 123	Yes Default: Inactive	SNTP Client
OPC UA	In	TCP	4840	Yes Default: Inactive	PITreader OPC Server UA

12.3 Overview of permissions

Permission	Code
0	0x00000000
1	0x000001ff
2	0x00003e0f
3	0x00003ff0
4	0x0001c633
5	0x0001c7cc
6	0x0001f83c
7	0x0001f9c3
8	0x00064a55
9	0x00064baa
10	0x0006745a
11	0x000675a5
12	0x00078c66
13	0x00078d99
14	0x0007b269
15	0x0007b396
16	0x000a94aa
17	0x000a9555
18	0x000aaaa5
19	0x000aab5a
20	0x000b5299
21	0x000b5366
22	0x000b6c96
23	0x000b6d69
24	0x000cdeff
25	0x000cdf00
26	0x000ce0f0
27	0x000ce10f
28	0x000d18cc
29	0x000d1933
30	0x000d26c3
31	0x000d273c
32	0x00304c6a
33	0x00304d95
34	0x00307265
35	0x0030739a

Permission	Code
36	0x00318a59
37	0x00318ba6
38	0x0031b456
39	0x0031b5a9
40	0x0036063f
41	0x003607c0
42	0x00363830
43	0x003639cf
44	0x0037c00c
45	0x0037c1f3
46	0x0037fe03
47	0x0037fffc
48	0x003ad8c0
49	0x003ad93f
50	0x003ae6cf
51	0x003ae730
52	0x003b1ef3
53	0x003b1f0c
54	0x003b20fc
55	0x003b2103
56	0x003c9295
57	0x003c936a
58	0x003cac9a
59	0x003cad65
60	0x003d54a6
61	0x003d5559
62	0x003d6aa9
63	0x003d6b56
64	0x00c04e98

13 Order reference

13.1 Authentication system

Product type	Features	Order no.
PITreader base unit	RFID authentication system, base unit. Required accessories: PITreader key adapter	402 255
PITreader S base unit	RFID authentication system, base unit with extended function range. Required accessories: PITreader key adapter	402 256
PITreader key adapter h	1x PITreader key adapter horizontal + 1x nut for PITreader base unit	402 308

13.2 Transponder key

Product type	Features	Order no.
PITreader key ye 1	Transponder key for authentication system PITreader, permission for operating mode 1 Colour: yellow Material: plastic	402 261
PITreader key ye 2	Transponder key for authentication system PITreader, permission for operating mode 1 and 2 Colour: yellow Material: plastic	402 262
PITreader key ye 3	Transponder key for authentication system PITreader, permission for operating mode 1, 2 and 3 Colour: yellow Material: plastic	402 263
PITreader key ye 4	Transponder key for authentication system PITreader, permission for operating mode 1, 2, 3 and 4 Colour: yellow Material: plastic	402 264
PITreader key ye 5	Transponder key for authentication system PITreader, permission for operating mode 1, 2, 3, 4 and 5 Colour: yellow Material: plastic	402 265
PITreader key ye 5 service	Transponder key for authentication system PITreader, permission for operating mode 1, 2, 3, 4 and 5 (Service) Colour: yellow Material: plastic	402 269
PITreader key ye g	Generic transponder key for authentication system PITreader, permissions freely configurable Colour: yellow Material: plastic	402 260

13.3 Accessories

Product type	Features	Order no.
PIT es wrench	Installation wrench for PIT es pushbutton	400 222

14 **EC declaration of conformity**

This product/these products meet the requirements of the following directives of the European Parliament and of the Council.

- ▶ 2014/53/EU on radio equipment

The complete EC Declaration of Conformity is available on the Internet at www.pilz.com/downloads.

Authorised representative: Norbert Fröhlich, Pilz GmbH & Co. KG, Felix-Wankel-Str. 2, 73760 Ostfildern, Germany

Support

Technical support is available from Pilz round the clock.

Americas

Brazil

+55 11 97569-2804

Canada

+1 888 315 7459

Mexico

+52 55 5572 1300

USA (toll-free)

+1 877-PILZUSA (745-9872)

Asia

China

+86 21 60880878-216

Japan

+81 45 471-2281

South Korea

+82 31 778 3300

Australia and Oceania

Australia

+61 3 95600621

New Zealand

+64 9 6345350

Europe

Austria

+43 1 7986263-0

Belgium, Luxembourg

+32 9 3217570

France

+33 3 88104003

Germany

+49 711 3409-444

Ireland

+353 21 4804983

Italy, Malta

+39 0362 1826711

Scandinavia

+45 74436332

Spain

+34 938497433

Switzerland

+41 62 88979-32

The Netherlands

+31 347 320477

Turkey

+90 216 5775552

United Kingdom

+44 1536 462203

**You can reach our
international hotline on:**

+49 711 3409-222

support@pilz.com

Pilz develops environmentally-friendly products using ecological materials and energy-saving technologies. Offices and production facilities are ecologically designed, environmentally-aware and energy-saving. So Pilz offers sustainability, plus the security of using energy-efficient products and environmentally-friendly solutions.



CECE®, CHRE®, CMSE®, InduraNET p®, Leansafe®, Master of Safety®, PAS4000®, PAScale®, PASconfig®, Pilz®, PIR®, PLID®, PMCPprime®, PMCPprotego®, PMCTendo®, PMD®, PMJ®, PNOZ®, PRIZ®, PRCM®, PRIMO®, PRISM®, PSENET p®, PSS®, PVS®, SafetyBUS p®, SafetyNET p®, THE SPIRIT OF SAFETY® are registered and protected trademark of Pilz GmbH & Co. KG in some countries. We would point out that product features may vary from the details stated in this document, depending on the status at the time of publication and the scope of the equipment. We accept no responsibility for the validity, accuracy and entirety of the text and graphics presented in this information. Please contact our Technical Support if you have any questions.

1004806-EN-06, 2021-03 Printed in Germany
© Pilz GmbH & Co. KG, 2019

We are represented internationally. Please refer to our homepage www.pilz.com for further details or contact our headquarters.

Headquarters: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone: +49 711 3409-0, Telefax: +49 711 3409-133, E-Mail: info@pilz.com, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY