



Visualisation; Diagnostics

Easy to Configure

Programming IEC 61131-3

Rapid Installation

## PITreader PITreader Firmware V2.0.x

**PILZ**  
THE SPIRIT OF SAFETY

- ▶ Control and signal devices

Pre

This document is the original document.

Where unavoidable, for reasons of readability, the masculine form has been selected when formulating this document. We do assure you that all persons are regarded without discrimination and on an equal basis.

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.

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

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Introduction</b>                             | <b>6</b>  |
| 1.1      | Validity of documentation                       | 6         |
| 1.2      | Using the documentation                         | 6         |
| 1.3      | Terminology                                     | 6         |
| 1.4      | Definition of symbols                           | 7         |
| 1.5      | Third-party manufacturer licence information    | 8         |
| <b>2</b> | <b>Overview</b>                                 | <b>9</b>  |
| 2.1      | Device features                                 | 9         |
| 2.2      | Unit views                                      | 10        |
| 2.2.1    | Unit view PITreader Key                         | 10        |
| 2.2.2    | Unit view PITreader Card                        | 11        |
| 2.2.3    | Unit view PIT gb with PITreader                 | 11        |
| 2.2.4    | View PITreader transponder key                  | 12        |
| 2.2.5    | View PITreader transponder card                 | 12        |
| 2.2.6    | View PITreader transponder sticker              | 13        |
| <b>3</b> | <b>Safety</b>                                   | <b>14</b> |
| 3.1      | Intended use                                    | 14        |
| 3.2      | Safety regulations                              | 14        |
| 3.2.1    | Additional documents that apply                 | 14        |
| 3.2.2    | Use of qualified personnel                      | 14        |
| 3.2.3    | Warranty and liability                          | 15        |
| 3.2.4    | Disposal  | 15        |
| <b>4</b> | <b>Security</b>                                 | <b>16</b> |
| 4.1      | Implemented security measures                   | 16        |
| 4.2      | Required security measures                      | 16        |
| <b>5</b> | <b>Function description</b>                     | <b>18</b> |
| 5.1      | Authentication procedure                        | 18        |
| 5.2      | Authentication modes                            | 19        |
| 5.2.1    | "Transponder data" authentication mode          | 19        |
| 5.2.1.1  | Device groups                                   | 19        |
| 5.2.2    | "External" authentication mode                  | 20        |
| 5.2.3    | "Permission list" authentication mode           | 22        |
| 5.3      | Authentication types                            | 22        |
| 5.3.1    | "Basic" authentication type                     | 22        |
| 5.3.2    | "Single authentication" authentication type     | 22        |
| 5.3.3    | "2-person rule" authentication type             | 23        |
| 5.4      | Transponders                                    | 25        |
| 5.4.1    | Permission on a transponder                     | 25        |
| 5.4.2    | Data areas of a transponder                     | 27        |
| 5.4.3    | Transponder recognition with one PITreader Card | 28        |
| 5.4.4    | Evaluation of a transponder's serial number     | 28        |
| 5.4.5    | Transponder's security ID (SID)                 | 29        |
| 5.5      | User data                                       | 30        |
| 5.5.1    | System parameters                               | 31        |

|          |   |           |
|----------|---|-----------|
| 5.6      | Coding.....   | 32        |
| 5.6.1    | Basic coding.....   | 33        |
| 5.6.2    | OEM coding.....   | 34        |
| 5.7      | Block list.....   | 35        |
| 5.8      | Real-time clock and operating hours counter.....                    | 35        |
| 5.9      | Modbus/TCP.....   | 36        |
| 5.9.1    | LED control.....  | 36        |
| 5.9.2    | Function codes (Client connections).....                            | 37        |
| 5.9.3    | Modbus/TCP data areas.....  | 38        |
| 5.9.3.1  | Data transfer limits.....   | 41        |
| 5.10     | HTTP(S) connection.....   | 42        |
| 5.11     | 24 V I/O port.....  | 42        |
| 5.12     | Connect the base unit to a safe evaluation unit.....                | 42        |
| <b>6</b> | <b>Installation and removal.....</b>                                | <b>43</b> |
| 6.1      | General guidelines for installation and removal.....                | 43        |
| 6.2      | Installation and removal of a PITreader Key.....                    | 44        |
| 6.2.1    | Installation of PITreader Key.....                                  | 44        |
| 6.2.2    | Removal of PITreader Key.....                                       | 47        |
| 6.3      | Installation and removal of a PITreader Card.....                   | 48        |
| 6.3.1    | installation of PITreader Card.....                                 | 48        |
| 6.3.2    | Removal of PITreader Card.....                                      | 51        |
| 6.3.3    | Apply sticker.....  | 51        |
| 6.4      | Installation and removal of a PIT gb with PITreader.....            | 51        |
| 6.5      | Dimensions.....   | 52        |
| 6.5.1    | Dimensions of PITreader Key.....                                    | 52        |
| 6.5.2    | Dimensions of PITreader Card.....                                   | 52        |
| 6.5.3    | Dimensions of PIT gb with PITreader.....                            | 52        |
| 6.5.4    | Dimensions of PITreader transponder key.....                        | 53        |
| 6.5.5    | Dimensions of PITreader transponder card.....                       | 53        |
| 6.5.6    | Dimensions of PITreader transponder sticker.....                    | 54        |
| <b>7</b> | <b>Wiring.....</b>  | <b>55</b> |
| 7.1      | Base unit without safe evaluation unit (standalone).....            | 55        |
| 7.2      | Base unit with safe evaluation unit.....                            | 55        |
| <b>8</b> | <b>Configuration.....</b>   | <b>56</b> |
| 8.1      | Web application.....  | 56        |
| 8.2      | Network discovery with Multicast DNS (mDNS).....                    | 57        |
| 8.3      | Network configuration via Multicast protocol.....                   | 57        |
| 8.4      | Connect to PITreader.....   | 58        |
| 8.5      | Device user.....  | 59        |
| 8.6      | Manage certificates.....  | 60        |
| 8.6.1    | Managing certificates.....  | 60        |
| 8.6.2    | Incorporate certificate into a public key infrastructure (PKI)..... | 60        |
| 8.7      | Configure authentication mode.....                                  | 62        |
| 8.8      | Configure authentication type.....                                  | 62        |
| 8.9      | Location description.....   | 62        |

|           |   |           |
|-----------|---|-----------|
| 8.10      | Data logging with personal data .....                   | 62        |
| 8.11      | Set device group .....                                  | 62        |
| 8.12      | Set basic coding .....                                  | 63        |
| 8.13      | Set OEM coding .....                                    | 64        |
| 8.14      | Write/program transponder .....                         | 65        |
| 8.14.1    | Program permissions .....                               | 65        |
| 8.14.2    | Configure the validity of the transponder .....         | 65        |
| 8.14.3    | Teach in transponder to basic coding .....              | 65        |
| 8.14.4    | Teach in transponder to OEM coding .....                | 66        |
| 8.14.5    | Limit transponder to identically coded PITreaders ..... | 67        |
| 8.14.6    | Edit user data values .....                             | 67        |
| 8.15      | Permission list .....                                   | 68        |
| 8.16      | Use block list .....                                    | 68        |
| 8.17      | Configure user data .....                               | 69        |
| 8.18      | API Clients .....                                       | 70        |
| 8.19      | Save and restore configuration .....                    | 70        |
| 8.20      | Reset to default settings .....                         | 71        |
| <b>9</b>  | <b>Firmware update .....</b>                            | <b>73</b> |
| <b>10</b> | <b>Operation .....</b>                                  | <b>74</b> |
| 10.1      | LED indicator .....                                     | 74        |
| 10.2      | Safely decommission PITreader .....                     | 76        |
| 10.3      | Diagnostics .....                                       | 76        |
| 10.3.1    | Statistics .....  | 77        |
| <b>11</b> | <b>Maintenance and testing .....</b>                    | <b>79</b> |
| <b>12</b> | <b>Technical details .....</b>                          | <b>80</b> |
| <b>13</b> | <b>Supplementary data .....</b>                         | <b>83</b> |
| 13.1      | Radio approvals PITreader Key .....                     | 83        |
| 13.2      | Radio approvals PITreader Card .....                    | 83        |
| 13.3      | Network data .....                                      | 84        |
| 13.4      | Overview of permissions .....                           | 84        |
| <b>14</b> | <b>Order reference .....</b>                            | <b>87</b> |
| 14.1      | Authentication system PITreader Key .....               | 87        |
| 14.2      | Authentication system PITreader Card .....              | 87        |
| 14.3      | Transponder key .....                                   | 87        |
| 14.4      | Transponder cards .....                                 | 88        |
| 14.5      | Transponder sticker .....                               | 89        |
| 14.6      | Accessories .....                                       | 90        |
| <b>15</b> | <b>EC declaration of conformity .....</b>               | <b>91</b> |
| <b>16</b> | <b>UKCA-Declaration of Conformity .....</b>             | <b>92</b> |

# 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 Terminology

### **PITreader**

All RFID authentication systems from PILZ GmbH & Co. KG on which authentication is via a transponder are included under the term "PITreader". Transponder cards, transponder stickers and/or transponder keys can be used as transponders for authentication, for example.

The term "PITreader" is always used when the description applies to all product types.

Note: Products from the PSEN cs product range do NOT come under the term PITreader.

### **PITreader Card**

The term "PITreader Card" includes all product types of the PITreader on which transponder cards, transponder stickers and transponder keys can be used as transponders for authentication. The PITreader S card unit is one of these product types, for example.

The term "PITreader Card" is always used when the description applies exclusively to these product types.

### **PITreader Key**

The term "PITreader Key" includes all product types of the PITreader on which only transponder keys can be used as transponders for authentication. The PITreader S base unit is one of these product types, for example.

The term "PITreader Key" is always used when the description applies exclusively to these product types.

### **PIT gb with PITreader**

The term "PIT gb with PITreader" includes all product types of the pushbutton unit PIT gb RLL E y ETH that have a PITreader. PIT gb RLL E y up ETH and PIT gb RLL E y down ETH are some of these product types, for example.

The term "PIT gb with PITreader" is always used when the description applies exclusively to these product types.

Note: only pushbutton units with PITreader Key are currently available.

## 1.4 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.

## 1.5 Third-party manufacturer licence information

This product includes Open Source software with various licenses.

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](mailto: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.

preliminary



## 2 Overview

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

- ▶ Transponder 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. 402250) for safe operating mode selection (only on PITreader Key and PITreader Card)

### 2.1 Device features

- ▶ System for authentication and authorisation on control systems
- ▶ Authentication is via transponder (transponder cards, transponder stickers and/or transponder keys)
- ▶ Configurable via a web application
- ▶ Ethernet interface for Modbus/TCP
- ▶ LED to display device status

#### Distinguishing features

| Device feature   | PITreader Key         | PITreader Card        | PIT gb with PITreader                          |
|--|-----------------------|-----------------------|--|
| Transponders   |                       |                       |  |
| Transponder keys   | ◆                     | ◆                     | ◆  |
| Transponder cards  | ---                   | ◆                     | ---  |
| Transponder stickers   | ---                   | ◆                     | ---  |
| Integrated OPC UA Server   | PITreader S base unit | PITreader S card unit | PIT gb RLLE y up ETH<br>PIT gb RLLE y down ETH |
| Base unit with interface for connecting a safe evaluation unit (SEU) for operating mode selection                              | ◆                     | ◆                     | ---  |
| Base unit for mounting cutout D22 (diameter 22.3 mm +0.4 mm/-0.0 mm) in accordance with EN 60947-5-1 with anti-rotation device | ◆                     | ◆                     | ---  |

## 2.2 Unit views

### 2.2.1 Unit view PITreader Key

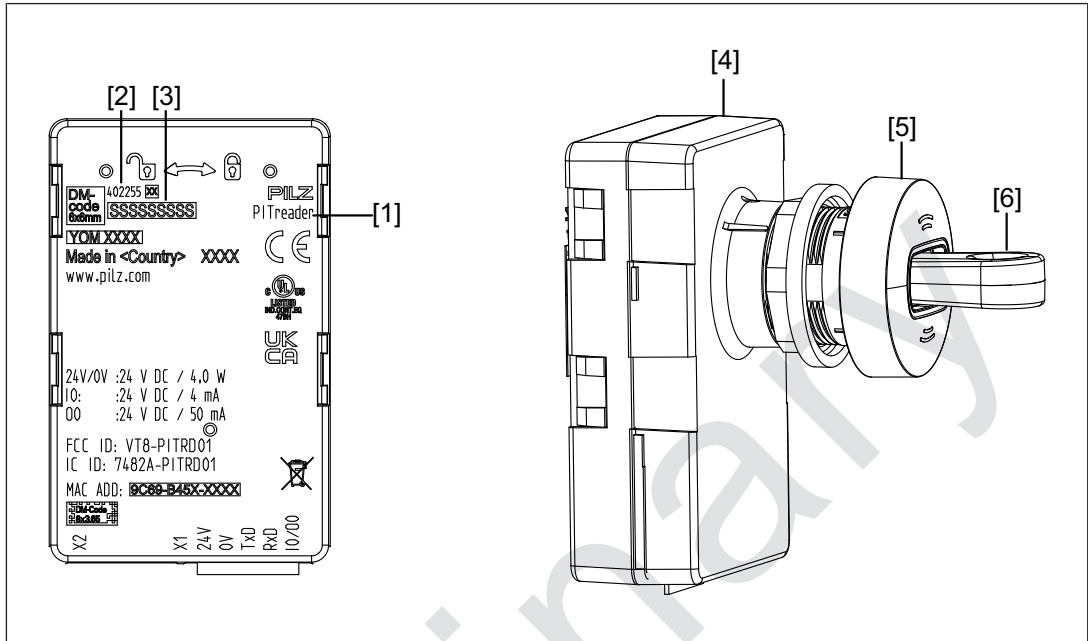


Fig.: Unit view PITreader Key, using PITreader base unit as an example

#### Legend

- X1 Voltage supply, 24 V input/output and connection of a safe evaluation unit (PIT m4SEU)
- X2 Ethernet interface
- [1] Device name
- [2] Order number
- [3] Serial number
- [4] Base unit (order no. 402255 or 402256), including spring-loaded terminal (402307)
- [5] Read head PITreader key adapter h (order no. 402308)  
(not supplied with the base unit, see also [Order reference \[87\]](#))
- [6] Transponder key (see also [Transponders \[25\]](#) and [Order reference \[87\]](#))

## 2.2.2 Unit view PITreader Card

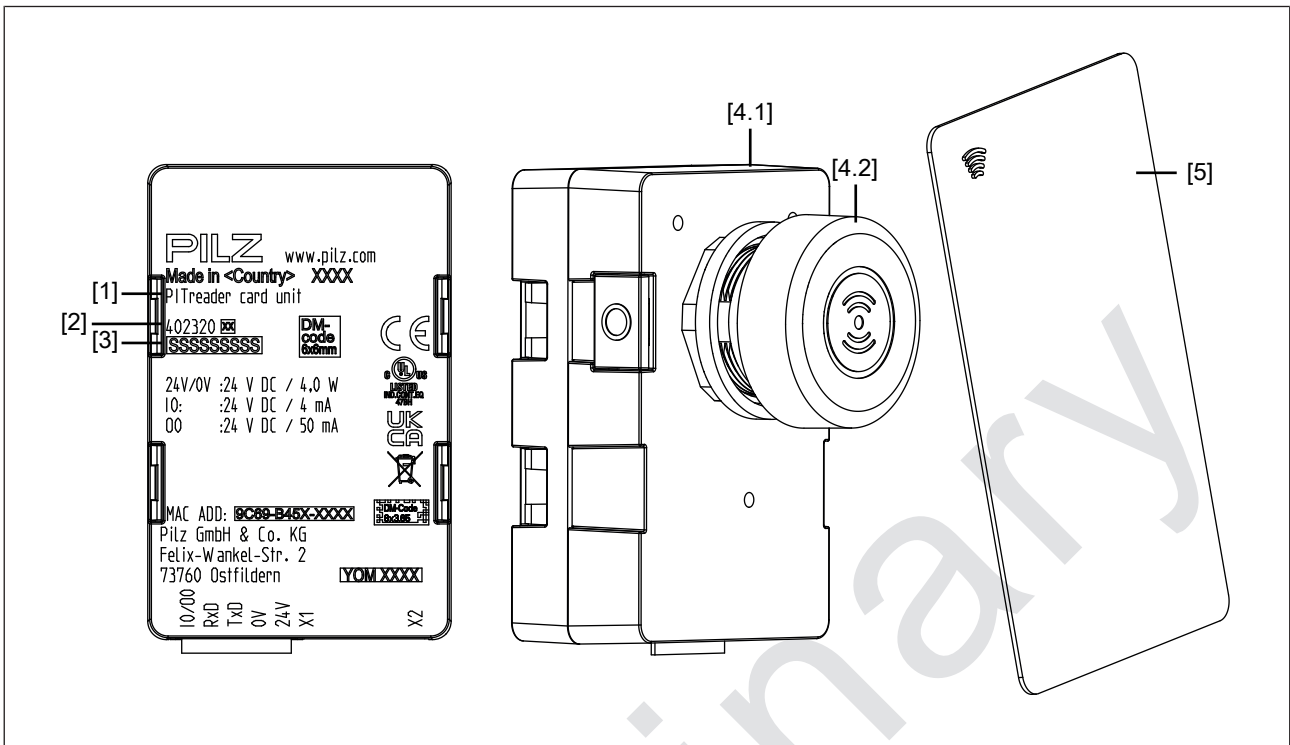


Fig.: Unit view PITreader Card with transponder card, using PITreader card unit as an example

### Legend

- X1 Voltage supply, 24 V input/output and connection of a safe evaluation unit (PIT m4SEU)
- X2 Ethernet interface
- [1] Device name
- [2] Order number
- [3] Serial number
- [4.1] Base unit (order no. 402320 or 402321), including spring-loaded terminal (402307)
- [4.2] Read head with silicone cap PITreader card cap (supplied with the base unit, see also [Order reference \[87\]](#))
- [5] Transponder (transponder card in this case, for example) (see also [Transponders \[25\]](#) and [Order reference \[87\]](#))

## 2.2.3 Unit view PIT gb with PITreader

You'll find the necessary information in the operating manual PIT gb RLLE y ETH.

## 2.2.4 View PITreader transponder key

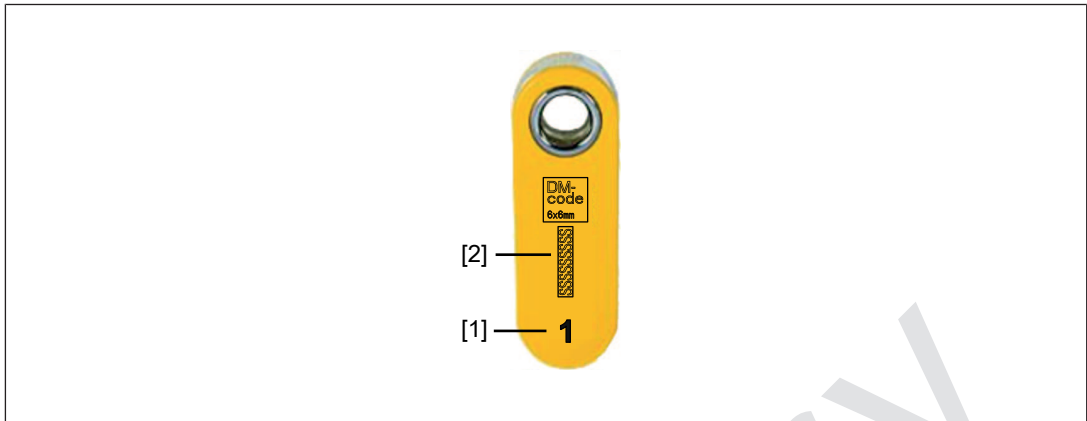


Fig.: Key view, using PITreader key ye 1 as an example

### Legend

- [1] Permission  
(see also [Permission on a transponder](#) [25] and [Order reference](#) [87])
- [2] Serial number

## 2.2.5 View PITreader transponder card

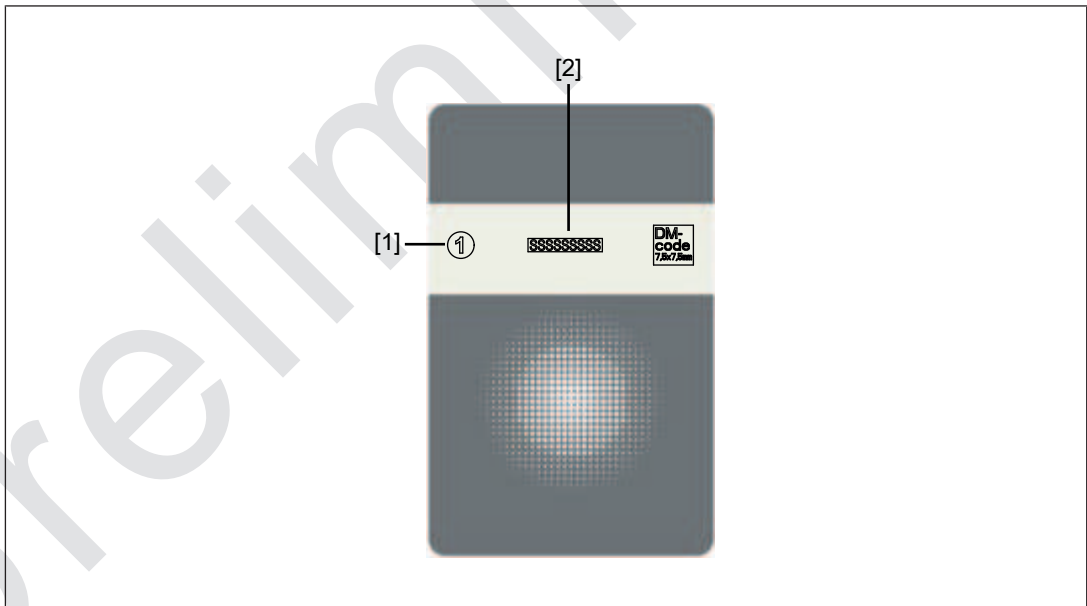


Fig.: Card view, using PITreader card ye 1 as an example

### Legend

- [1] Permission  
(see also [Permission on a transponder](#) [25] and [Order reference](#) [87])
- [2] Serial number

## 2.2.6 View PITreader transponder sticker

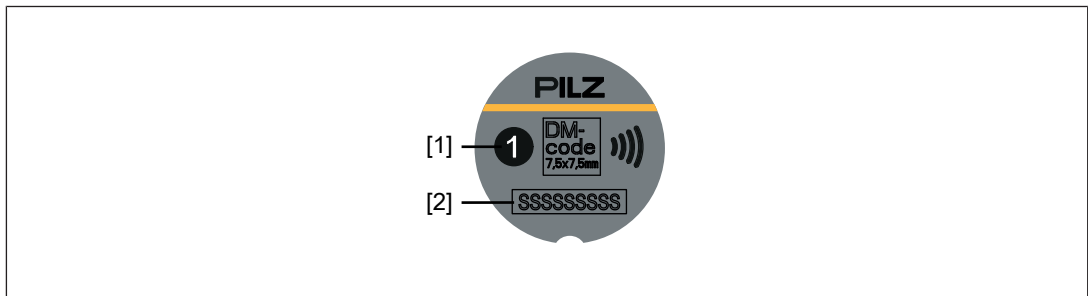


Fig.: Sticker view, using PITreader sticker ye 1 as an example

### Legend

- [1] Permission  
(see also [Permission on a transponder](#) [📖 25] and [Order reference](#) [📖 87])
- [2] Serial number

## 3 Safety

### 3.1 Intended use

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

#### Improper use

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 operating manual,
- ▶ Use of the product outside the technical details (see [Technical details](#) [80]).



#### 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:

- ▶ When using a PIT gb with PITreader (e.g. PIT gb RLLE y up ETH, PIT gb RLLE y down ETH):  
Operating manual for the pushbutton unit
- ▶ When using a safe evaluation unit PIT m4SEU:  
Operating manual PIT m4SEU
- ▶ 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 persons who are competent to do so.

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).

preliminary

## 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-independent characters are not available in every keyboard language.
  - Make sure you regularly change the passwords of the user accounts on the system and/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.
- ▶ An API token should be handled with the same care as a password. The requirements for passwords can be found in the operating manual for the PITreader.
- ▶ As soon as possible, install firmware updates that Pilz provides for the product.
- ▶ Keep the transponders in a safe place and protect them from unauthorised access. Advise users of the security risks of sharing transponders.
- ▶ During a factory reset, the coding in the device is also reset. As a result, uncoded transponders, or transponders that are coded differently, will again be accepted on this device. For this reason we recommend that the check sum for the coding is monitored in a higher-level controller, an HMI or evaluation unit.
- ▶ Log data may contain personal data. Only store exported logs on a storage medium that is adequately protected.
- ▶ In the event of a network scan via Multicast DNS, the product's serial number can be read even without authentication. It is essential that you assign a separate password in the web application, one which differs from the default password.
- ▶ Synchronisation of the real-time clock in the device via SNTP does not include any security mechanisms to protect against attacks by unauthorised persons (e.g. spoofing of the configured SNTP Server). Protect the real-time clock in the device on the application side via an appropriate firewall configuration, or by using a separate local time server within the machine network.
- ▶ A product's configuration backup file contains information about authentication on the product. Only store the backup file on a storage medium that is adequately protected.
- ▶ Before disposal, the product must be safely 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.

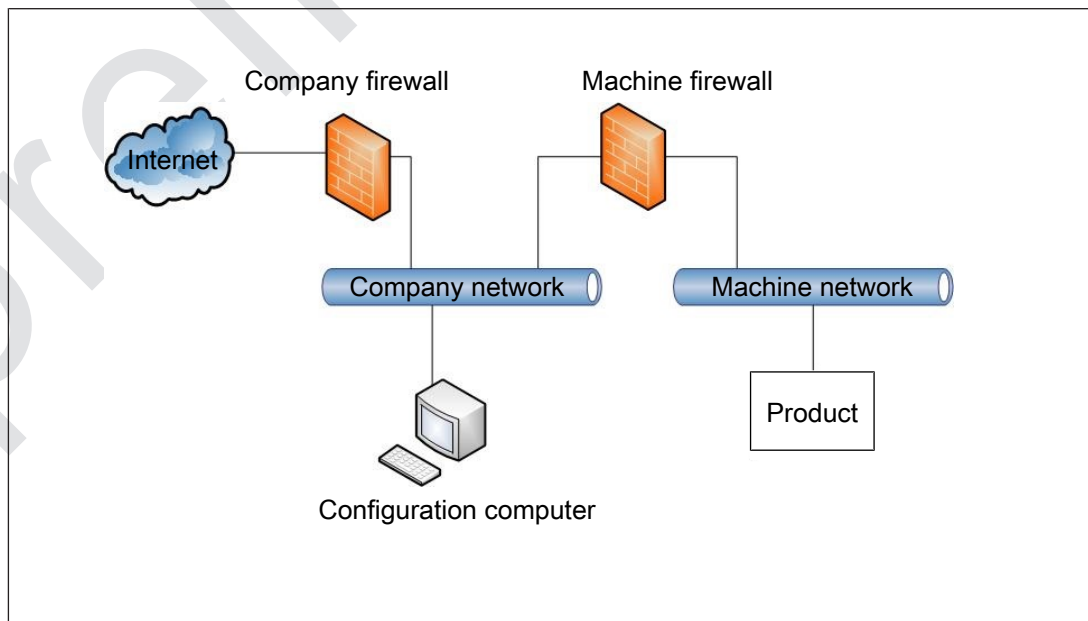


Fig.: Example network topology

- ▶ Note the [network data](#) [84] for risk analysis and the security measures.

## 5 Function description

### 5.1 Authentication procedure

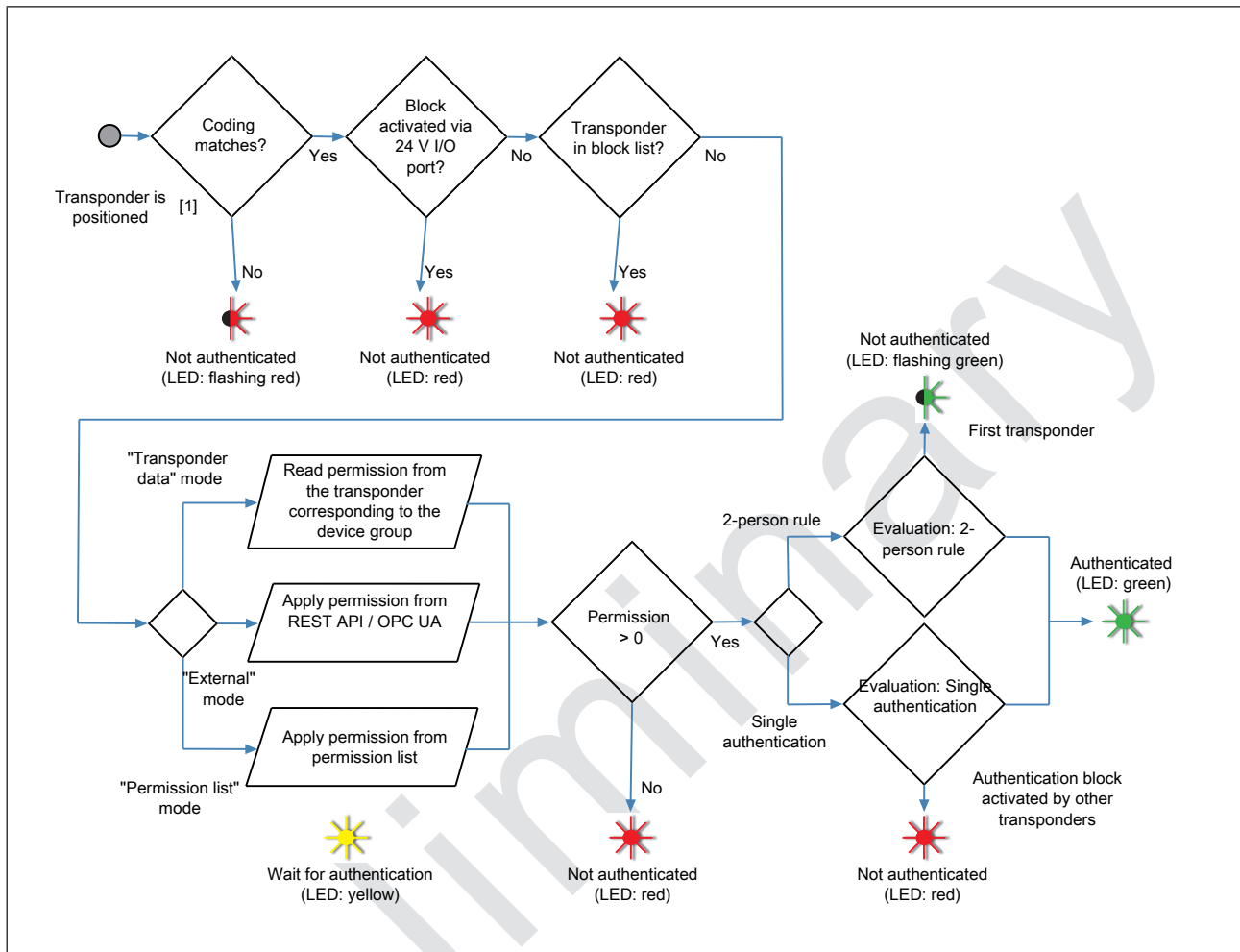


Fig.: Authentication procedure

[1]

Meaning:

- ▶ PITreader Key: the transponder is inserted into the read head.
- ▶ PITreader Card: the transponder is held in front of the read head.

## 5.2 Authentication modes

The PITreader supports the following authentication modes:

- ▶ ["Transponder data" authentication mode \[19\]](#)  
Pre-defined, group-based authentication in the transponder
- ▶ ["External" authentication mode \[20\]](#)  
Authentication takes place externally e.g. via PLC, HMI
- ▶ ["Permission list" authentication mode \[22\]](#)

"Transponder data" authentication mode is set upon delivery. The authentication mode can be changed in the web application; it is also possible to set whether the authentication mode may be overwritten via the REST API (see also [Configure authentication mode \[62\]](#)).

### 5.2.1 "Transponder data" authentication mode

In "transponder data" authentication mode, users can authenticate themselves on a safe evaluation unit (e.g. PIT m4SEU) and the connected control system by positioning a transponder in the read area of the PITreader. Authentication is carried out using the permissions stored on the transponder.

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

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



#### INFORMATION

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

We recommend that you enter the security IDs of all the published transponders in a list, so that they can be transferred into the [Block list \[35\]](#) 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) 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 \[62\]](#).

One permission can be stored on a transponder 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](#) [84].

Only one permission at a time is valid in the PITreader. Additional permissions stored on the transponder 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. The permissions for device groups 0 ... 31 can be stored on a transponder, and also for a maximum 48 other device groups in the range 32 ... 9999. See [User data](#) [30].

## 5.2.2 "External" authentication mode

In "external" authentication mode, users can authenticate themselves on the connected control system or on the HMI by positioning a transponder within the read area of the PITreader.

The following connection options are available:

### External authentication (Modbus/TCP)

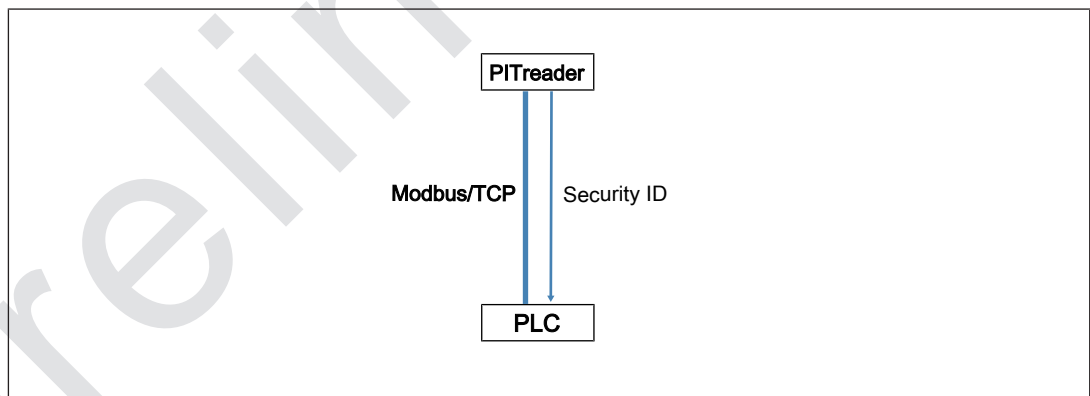


Fig.: External authentication (Modbus/TCP)

The PITreader provides the transponder 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 (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 yellow when the transponder is positioned.

To display the externally identified authentication status via the device LED, the colour and flash mode can be overwritten via the Modbus/TCP interface.

**Note:** A safe evaluation unit (e.g. PIT m4SEU) **CANNOT** be used in "External" authentication mode via Modbus/TCP.

### External authentication (REST API)

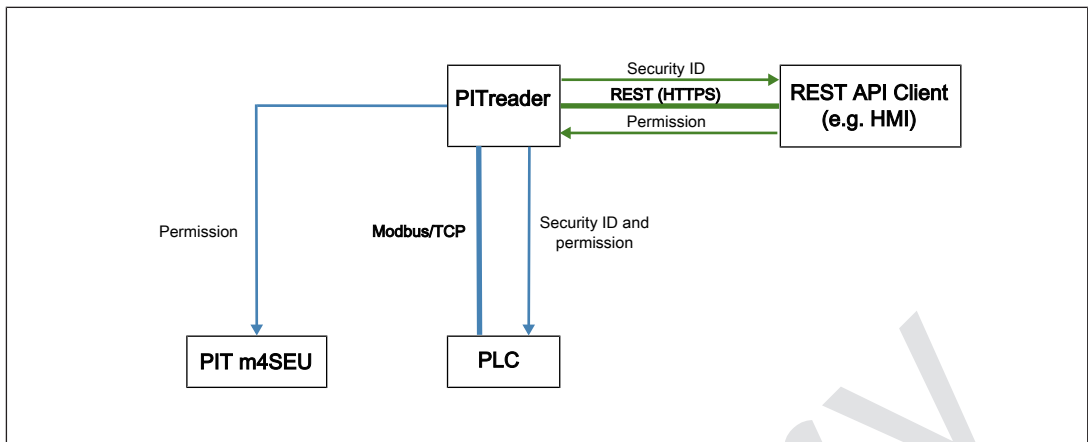


Fig.: External authentication (REST API)

The permission for the user can be identified using a permission database on the REST API Client (e.g. HMI) and the data from the transponder (e.g. security ID). Authentication occurs on the REST API Client. The information about the authentication status is adopted by the PITreader and forwarded to the controller and the safe evaluation unit (e.g. PIT m4SEU). The externally calculated authentication status is displayed via the device LED on the PITreader.

### External authentication (OPC UA)

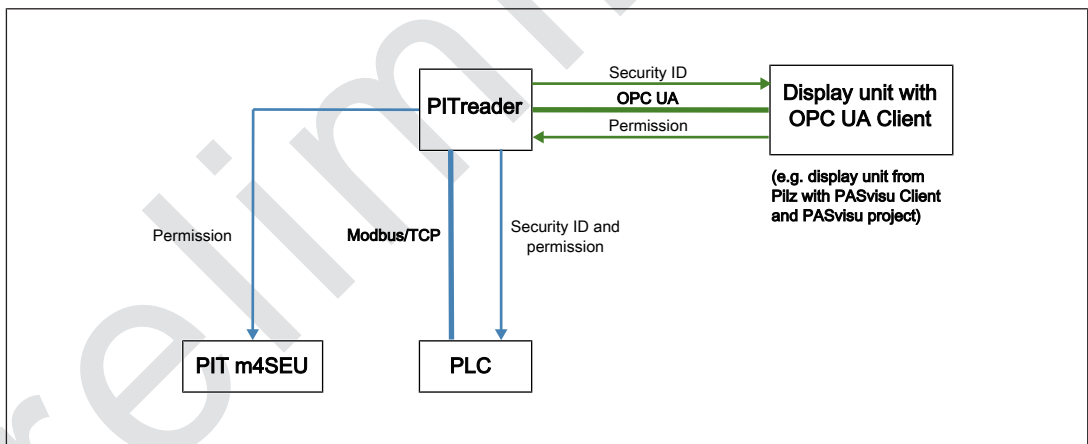


Fig.: External authentication (OPC UA)

The permission for the user can be identified using a permission database on the OPC UA Client (e.g. display unit) and the data from the transponder (e.g. security ID). Authentication occurs on the OPC UA Client. The information about the authentication status is adopted by the PITreader and forwarded to the controller and the safe evaluation unit (e.g. PIT m4SEU). The externally calculated authentication status is displayed via the device LED on the PITreader.

### 5.2.3 "Permission list" authentication mode

In "Permission list" authentication mode, the security ID stored on the transponder and the information stored in the permission list are evaluated for authentication (see also [Permission list \[📖 68\]](#)).

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

An external device (e.g. HMI) can read the currently authenticated user via an HTTP(S)-based web service call.

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

## 5.3 Authentication types

The PITreader supports the following authentication types:

- ▶ Basic
- ▶ Single authentication
- ▶ 2-person rule

### 5.3.1 "Basic" authentication type

The "Basic" authentication type includes the "Transponder data", "External" and "Permission list" authentication modes, with all their functions and options (see [Authentication modes \[📖 19\]](#)).

### 5.3.2 "Single authentication" authentication type

The "single authentication" authentication type 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, in order to activate an authentication block for all other transponders. The authentication block remains activated until the same transponder 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 positioning the transponder on the PITreader. By logging in, an authentication block is activated for all other transponders. If the transponder is removed, the authentication block remains activated.

- ▶ Deactivate authentication block:

The authentication block is not deactivated until the same transponder is used to log out. To log out, the same transponder must be repositioned 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.

### 5.3.3 "2-person rule" authentication type

The "2-person rule" authentication type includes all the functions and possibilities of the "Basic" authentication type.

With the "two-person rule" authentication type, two different transponders are needed for authentication. The authentication process is started with the first transponder. Actual authentication then occurs using the second transponder.

▶ Start authentication process

The authentication process is started by positioning the first transponder on the PITreader. The device LED flashes green.

The transponder runs through all the authentication steps up to the permission check (see [Authentication procedure \[18\]](#)). If there is sufficient permission and the "2-person rule" is configured, the permission is assessed internally as "permission 0"; i.e. authentication is not possible with the first transponder.

Once the first transponder is removed, a 30-second time window is activated. Authentication with the second transponder can occur within this time window. The device LED will flash green until either the 30-second time window has elapsed or the second transponder is positioned.

▶ Cancel authentication process

An authentication process that has been started will be cancelled if a second valid transponder is not positioned within the 30-second time window or the same transponder is repositioned.

An authentication process that has been started is not cancelled as a result of an invalid transponder.

▶ Restart authentication process after it has been cancelled

The authentication process can be restarted by repositioning and removing the first transponder.

▶ Authentication

When the authentication process is started, users can authenticate themselves with a second transponder within the 30-second time window.

Once the second transponder has been positioned, it runs through all the authentication steps (see [Authentication procedure \[18\]](#)). If it is a valid transponder, then authentication occurs.

Notes:

▶ Both transponders may be any transponder; i.e. there is no need for special or preconfigured transponders. However, the transponders must be valid for the specific application.

▶ The permission enabled via authentication through the second transponder is established internally. The permissions on the two transponders are evaluated and authentication occurs with the lower of the permissions on the two transponders.

Examples:

- Permission on the first transponder: 10
- Permission on the second transponder: 5
- > Authentication occurs with permission 5

- Permission on the first transponder: 1
- Permission on the second transponder: 5
- > Authentication occurs with permission 1

preliminary



## 5.4 Transponders

Transponders are available as transponder keys, transponder cards and transponder stickers. The functions are identical for all transponders.

### Application options of a transponder

| Transponder              | PITreader Key | PITreader Card | PIT gb with PITreader |
|--------------------------|---------------|----------------|-----------------------|
| Transponder keys         | ◆             | ◆              | ◆                     |
| Transponder cards        | ---           | ◆              | ---                   |
| Transponder stickers [1] | ---           | ◆              | ---                   |

[1]

Note: a transponder sticker is intended to be stuck on to an existing card. An existing company ID card can serve as the carrier for a transponder sticker, for example. This reduces the number of cards required.

### 5.4.1 Permission on a transponder

#### Transponder keys

The transponder keys are available in the following types, with the following permissions (see also [Order reference \[87\]](#)):

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

The permission can be identified from the first two digits (prefix) of the serial number.

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

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

### Transponder cards

The following types of transponder cards are available (see also [Order reference \[87\]](#)):

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

The permission can be identified from the first two digits (prefix) of the serial number.

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

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

### Transponder stickers

The following types of transponder stickers are available (see also [Order reference \[87\]](#)):

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

The permission can be identified from the first two digits (prefix) of the serial number.

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

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

## 5.4.2 Data areas of a transponder

Various data areas are available on a transponder.

These include:

▶ Data area for permission

- Transponder with factory pre-programmed permission (permission cannot be modified or is locked)
- Transponder with configurable permission (permission can be modified)  
As an option, the permission can be locked.

▶ Data area for permission of device groups

- On transponders with factory pre-programmed permission, the pre-programmed permission applies to the device groups G0 ... G31.
- On transponders with configurable permission, a separate permission can be configured for each of the device groups G0 ... G31. Possible permissions are 0 ... 64.

▶ Data area for the validity date of a permission (start/end date)

The data area cannot be locked.

▶ Data area for free (customised) user data

The data area cannot be locked.

### Example

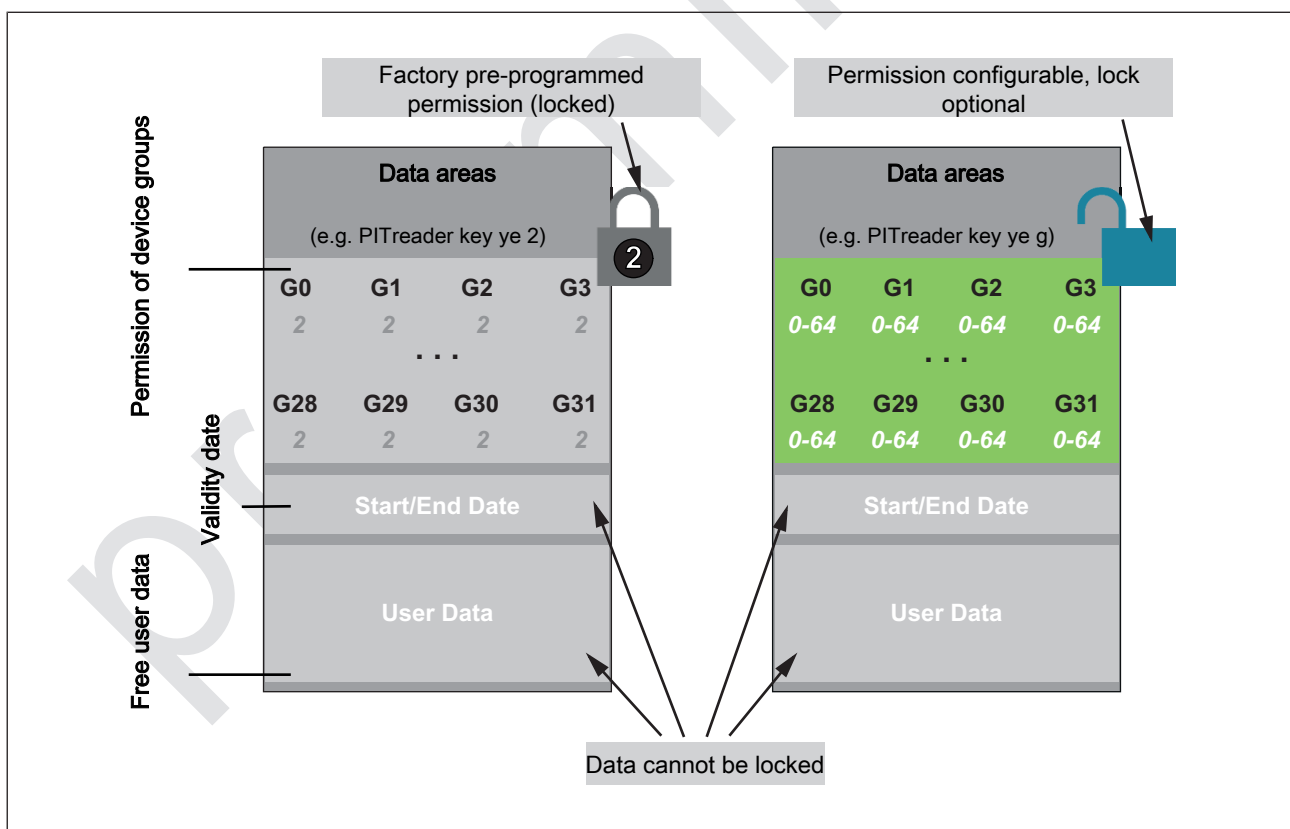


Fig.: Data areas of a transponder, using PITreader key ye 2 and PITreader key ye g as an example

### 5.4.3 Transponder recognition with one PITreader Card

► Maximum read distance when positioning a transponder

- PITreader transponder key

The optimum position for a transponder key is when the tip of the transponder key is positioned in the centre of the read head, thereby touching the surface of the read head.

- PITreader transponder card or PITreader transponder sticker

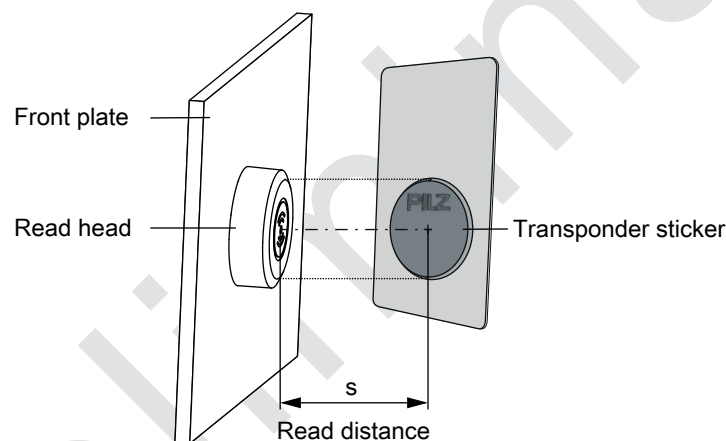
The centre of the transponder should ideally be positioned over the centre of the read head.

The optimum position for a transponder card or transponder sticker is when the read head of the PITreader Card and the read area of the transponder are aligned in parallel and both centres are positioned on top of each other.

With optimum positioning, the assured maximum read distance  $s$  is as follows:

- Metallic front plate:  $s = 10 \text{ mm}$
- Non-metallic front plate:  $s = 20 \text{ mm}$

Example:



► Transponder recognition with multiple transponders in the read area

Authentication only occurs when there is exactly one valid transponder in the read area. If there are other transponders in the read area, but these are not readable (e.g. transponder for third-party applications), then these transponders will be ignored.

Any errors in transponder recognition will be signalled via the LED display. Further information is available in the description of the LED status "flashing red", under [LED indicator \[74\]](#).

### 5.4.4 Evaluation of a transponder's serial number

The serial number of the transponder 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.

### 5.4.5 Transponder's security ID (SID)

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

The security ID is used to uniquely identify a transponder on the PITreader; i.e. a transponder is authenticated on the PITreader with the help of the security ID. The permissions that are configured for a transponder 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's security ID in a block list (see [Use block list \[📖 68\]](#)).

preliminary

## 5.5 User data

A free data area is available on a transponder. Customer-specific data (e.g. language, user name, ...) can be saved 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](#)  31].

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](#)  31]).

This section describes how to configure the user data: [Configure user data](#)  69]

The values of the parameters are stored on the transponder. Values for a maximum of 64 parameters and a maximum of 48 device groups can be stored on the transponder. 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 is displayed in the web application.

For each parameter, a separate value can be stored for each device group 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: [Edit user data values](#) [📖 67].

The user data can be read from the transponder via Modbus/TCP, via REST API or via the OPC UA Server (see operating manual PITreader REST API or PITreader OPC Server UA). The PITreader always returns exactly 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, the data type's initial value is returned. If the parameter exists on the transponder 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<br>Permissions for device groups 32 ... 9999<br>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 <b>Transponder -&gt; Permissions</b> always apply for device groups 0 to 31. |
| 2  | DATETIME   | Start date<br>Details of when the permission for a device group will start to be valid. This value can be defined for groups 0 ... 9999.<br>Note: The start date is only evaluated if the <b>Evaluate validity date</b> option is activated for the PITreader.                                  |
| 3  | DATETIME   | End date<br>Details of when the permission for a device group will cease to be valid. This value can be defined for groups 0 ... 9999.<br>Note: The end date is only evaluated if the <b>Evaluate validity date</b> option is activated for the PITreader.                                      |

## 5.6 Coding

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

There are two different codings:

- ▶ [Basic coding](#)  33]
- ▶ [OEM coding](#)  34]

The identifiers for both codings can be stored on a PITreader. However, a transponder can only be taught in on one of the two codings. A transponder is taught in on one of the two codings in the web application. To teach in a transponder to basic coding, the basic identifier must be entered as the basic coding. To teach in a transponder to OEM coding, the OEM identifier must equally be entered as the basic coding.

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

### Teaching in a coded transponder


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



#### INFORMATION

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

### Protection against unauthorised reading of a coded transponder

Both coded and uncoded transponders will work on an uncoded PITreader; i.e. the data from a coded transponder can also be read by an uncoded PITreader. To prevent this, a coded transponder can also be configured so that reading is restricted to identically coded PITreader devices (see [Limit transponder to identically coded PITreaders](#)  67)).

### 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, REST API or OPC UA. The check sum is also displayed in the web application (see [Set basic coding \[63\]](#) and [Set OEM coding \[64\]](#)).

### 5.6.1 Basic coding

Due to the basic coding, PITreader devices can only recognise transponders that have been coded using the same basic identifier or using an OEM identifier that may be stored in the PITreader (see [OEM coding \[34\]](#)).

For example, basic coding can be used to code a "Company identifier". As a result, only internally coded transponders are recognised.

Basic coding is achieved by configuring the PITreader with a basic identifier (see [Set basic coding \[63\]](#)). Transponders are taught in to a basic identifier when permissions are written to the transponder on a coded PITreader (see [Teach in transponder to basic coding \[65\]](#)).

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.

preliminary

## 5.6.2 OEM coding

With OEM coding, a second identifier can be stored in the PITreader to check the transponders. PITreader devices with OEM coding accept transponders with the same OEM identifier or with the matching basic identifier (see [Basic coding](#) [63]).

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

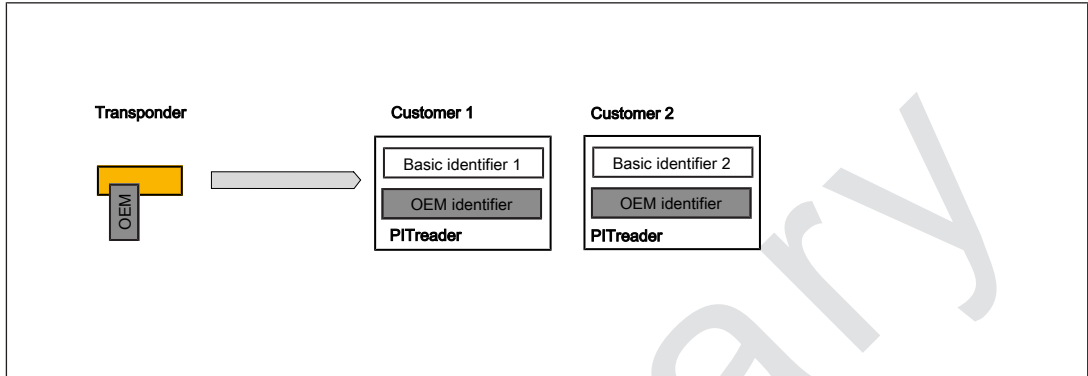


Fig.: OEM coding

New transponder with this 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 to OEM coding](#) [66].

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 [Set OEM coding](#) [64].

## 5.7 Block list

You can lock the authentication of certain transponders. Once a transponder 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. 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](#) [📖 68].

## 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.

preliminary

## 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,<br>data length $\geq 1$ bit,<br>(receive data from 1x)         |
| 03            | Read Holding Register    | The connection Client reads word data from the connection Server,<br>data length $\geq 1$ word,<br>(receive data from 4x)       |
| 04            | Read Input Register      | The connection Client reads word data from the connection Server,<br>data length $\geq 1$ word,<br>(receive data from 3x)       |
| 06            | Write Single Register    | The connection Client writes to a word datum in the connection Server,<br>data length = 1 word,<br>(send data to 4x)            |
| 16            | Write Multiple Registers | The connection Client writes to multiple word data in the connection Server,<br>data length $\geq 1$ word,<br>(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 | Contents                                     |
|---------|--|
| 1x4001  | Is authenticated (data from the transponder) |

► Input Register (Word/16 Bits)

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

| Address           | Contents   |
|-------------------|--|
| 3x0001 ... 3x0002 | PITreader order number (coded)<br>Bits 31 to 24: Product group (00 = empty, 01 = G1)<br>Bits 23 to 20: Revision (00 = empty )<br>Bits 19 to 0: Product number<br>Examples:<br>PITreader base unit (402255): 0x 00 0 6234F<br>PITreader card unit (402320): 0x 00 0 62390<br>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 <a href="#">LED control [36]</a> )  |
| 3x0010            | LED flash mode (see also <a href="#">LED control [36]</a> )  |
| 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)<br>Default value if no SEU is connected: 0x00F0 (decimal: 240)   |
| 3x0025 ... 3x0028 | Security ID (data from the transponder)  |
| 3x0029 ... 3x0030 | Reserved   |
| 3x0031 ... 3x0032 | Permission (code word)   |
| 3x0033            | Permission (integer, 0 to 64)  |

| Address           | Contents   |
|-------------------|--|
| 3x0034            | Authentication status (0 = not authenticated, 1 = transponder authenticated successfully)  |
| 3x0035 ... 3x0036 | Order number (transponder)   |
| 3x0037 ... 3x0038 | Serial number (transponder) (see also <a href="#">Evaluation of a transponder's serial number</a> [  28]) |
| 3x0039            | Reserved   |
| 3x0040            | Reserved   |
| 3x0059 ... 3x0060 | Permission group 0   |
| 3x0061 ... 3x0062 | Permission group 1   |
| 3x0063 ... 3x0064 | Permission group 2   |
| 3x0065 ... 3x0066 | Permission group 3   |
| 3x0067 ... 3x0068 | Permission group 4   |
| 3x0069 ... 3x0070 | Permission group 5   |
| 3x0071 ... 3x0072 | Permission group 6   |
| 3x0073 ... 3x0074 | Permission group 7   |
| 3x0075 ... 3x0076 | Permission group 8   |
| 3x0077 ... 3x0078 | Permission group 9   |
| 3x0079 ... 3x0080 | Permission group 10  |
| 3x0081 ... 3x0082 | Permission group 11  |
| 3x0083 ... 3x0084 | Permission group 12  |
| 3x0085 ... 3x0086 | Permission group 13  |
| 3x0087 ... 3x0088 | Permission group 14  |
| 3x0089 ... 3x0090 | Permission group 15  |
| 3x0091 ... 3x0092 | Permission group 16  |
| 3x0093 ... 3x0094 | Permission group 17  |
| 3x0095 ... 3x0096 | Permission group 18  |
| 3x0097 ... 3x0098 | Permission group 19  |
| 3x0099 ... 3x0100 | Permission group 20  |
| 3x0101 ... 3x0102 | Permission group 21  |
| 3x0103 ... 3x0104 | Permission group 22  |
| 3x0105 ... 3x0106 | Permission group 23  |
| 3x0107 ... 3x0108 | Permission group 24  |
| 3x0109 ... 3x0110 | Permission group 25  |
| 3x0111 ... 3x0112 | Permission group 26  |
| 3x0113 ... 3x0114 | Permission group 27  |
| 3x0115 ... 3x0116 | Permission group 28  |
| 3x0117 ... 3x0118 | Permission group 29  |

| Address           | Contents   |
|-------------------|--|
| 3x0119 ... 3x0120 | Permission group 30  |
| 3x0121 ...3x0122  | Permission 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 <a href="#">User data [📖 30]</a> ) |



**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:

$$\text{Address}_n = \text{Address}_{(n-1)} + \text{RoundingUp}_{2\text{-Byte}}(\text{Length}_{(n-1)})$$

- ▶ Holding Register (Word/16 Bits)  
Modbus Client -> PITreader, register access read (with FC03) and write (with FC06 or FC16)

| Address | Contents                                    |
|---------|---|
| 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.



### 5.9.3.1 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 transponders (see also chapters entitled [Configuration](#) [56] and [Firmware update](#) [73]).

## 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, from which point the output is to be switched on. If the permission on the transponder 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](#) [22]).

## 5.12 Connect the base unit to a safe evaluation unit

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

## 6 Installation and removal

### 6.1 General guidelines for installation and removal



#### **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.



#### **NOTICE**

##### **Damage caused by installation/removal when the voltage is live!**

Components may be damaged by installing/removing them when the power is live. Make sure that the power to the product is removed before it is installed/removed.

preliminary

## 6.2 Installation and removal of a PITreader Key

### 6.2.1 Installation of PITreader Key

#### Procedure

- ▶ Install the device in the front panel of a control cabinet or in a control console.

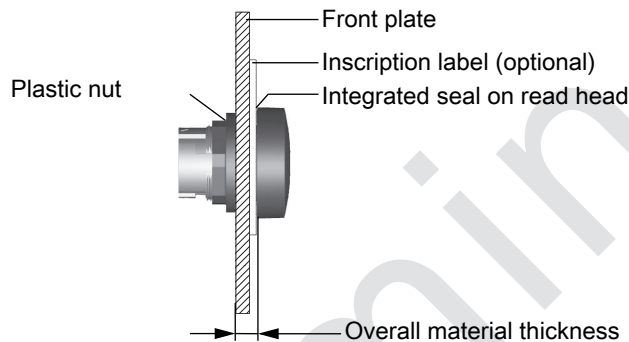
Maximum permitted material thickness:

- Non-metallic front plate: 2 ... 6 mm
- Metallic front plate: 2 ... 4 mm.

Note: When the read head is installed, the overall material thickness is the distance from the plastic nut lining up to and including the integrated seal on the read head; i.e.:

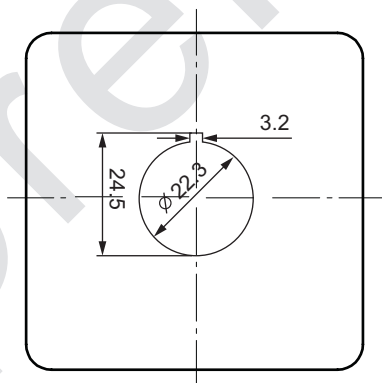
Material thickness<sub>Maximum</sub> = Material thickness<sub>Front Plate</sub> + Material thickness<sub>Optional Materials</sub>

Inscription labels, for example, count as "optional materials". When installed correctly, the material thickness of the seal can be ignored.



- ▶ 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 on the read head PITreader key Adapter h. The latch provides anti-rotation protection.

Example:



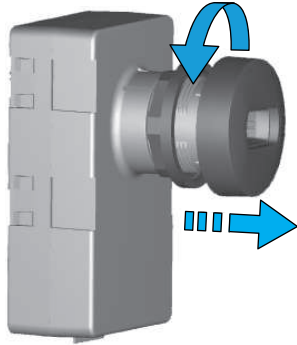
In the example, the recess can be positioned so that the base unit can be installed either with an upward or downward cable outlet.

Note: Through the positioning of the latch, two different ways of installing are possible, with regard to the base unit's cable outlet. The base unit can either be installed so that the latch points in the direction of the cable outlet, or so that it points in the opposite direction (base unit turned 180°). Position the recess to achieve the desired cable outlet.

- ▶ On your device, if the read head is not installed on the base unit, you can skip this step.

Otherwise:

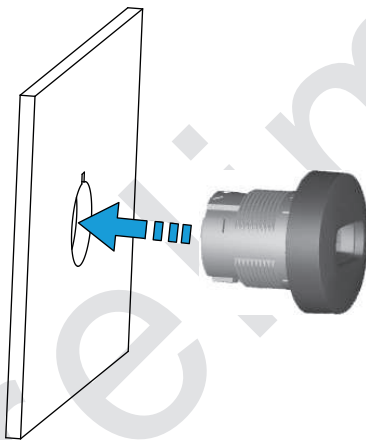
Hold the base unit firmly, rotate the read head 15° anti-clockwise and pull the read head from the base unit.



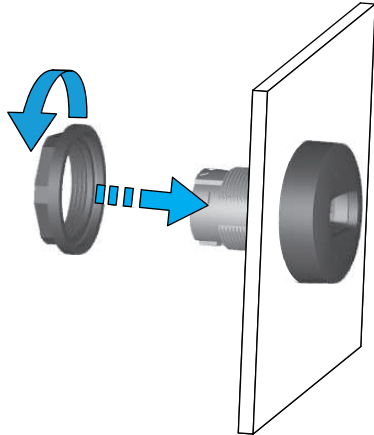
- ▶ Remove the plastic nut (M22) from the read head.



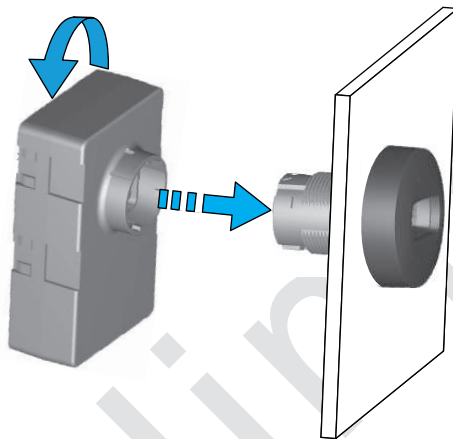
- ▶ From the front, insert the read head into the mounting cutout so that the latch is positioned in the recess on the mounting cutout.



- ▶ Use the plastic nut (M22) to secure the read head from the other side. 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 \[📖 87\]](#)).



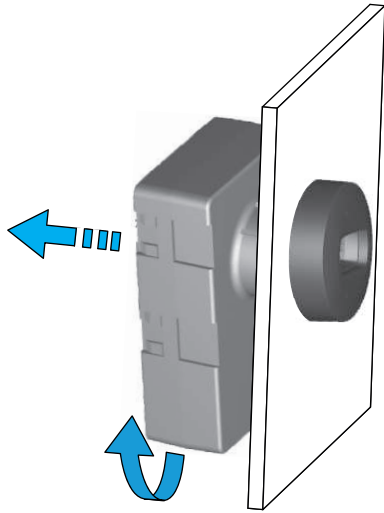
- ▶ Connect the base unit to the read head and rotate the base unit 15° clockwise until it locks in position.



## 6.2.2 Removal of PITreader Key

### Procedure

- ▶ Remove the power to the PITreader.
- ▶ Rotate the base unit 15° anti-clockwise.
- ▶ Pull gently on the base unit of the PITreader until the base unit detaches from the read head.



## 6.3 Installation and removal of a PITreader Card

### 6.3.1 installation of PITreader Card

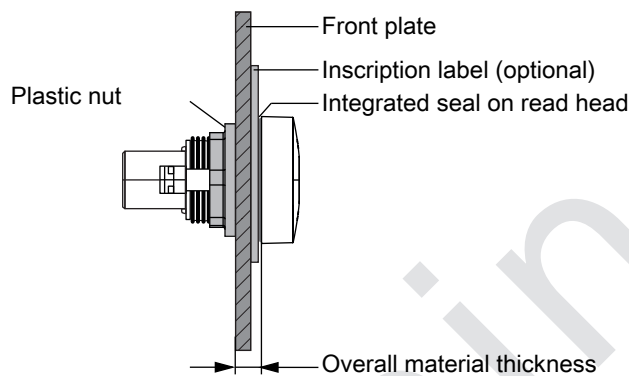
#### Procedure

- ▶ Install the device in the front panel of a control cabinet or in a control console.  
Maximum permitted material thickness: 2 ... 6 mm

Note: When the read head is installed, the overall material thickness is the distance from the plastic nut lining up to and including the integrated seal on the read head; i.e.:

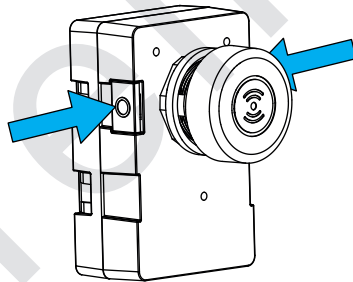
$$\text{Material thickness}_{\text{Maximum}} = \text{Material thickness}_{\text{Front Plate}} + \text{Material thickness}_{\text{Optional Materials}}$$

Inscription labels, for example, count as "optional materials". When installed correctly, the material thickness of the seal can be ignored.



The overall material thickness must not exceed the maximum permitted material thickness.

- ▶ Please note the following regarding the installation site:
  - When installing, ensure there is sufficient lateral distance to allow the two release buttons to be operated for removal.

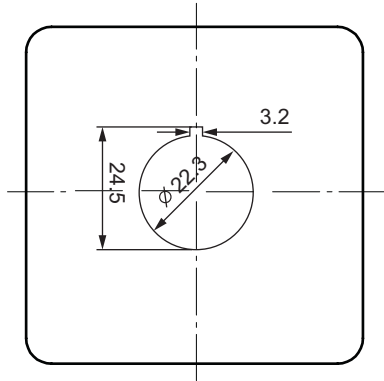


- With a NON-metallic front plate, if you wish to install several PITreader Cards side by side, then a minimum distance of 15 cm must be maintained between two PITreader Cards.



- ▶ Provide the front plate of the control cabinet or control console with a mounting cutout ( $\varnothing$  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 on the read head PITreader card Adapter. The latch provides anti-rotation protection.

Example:



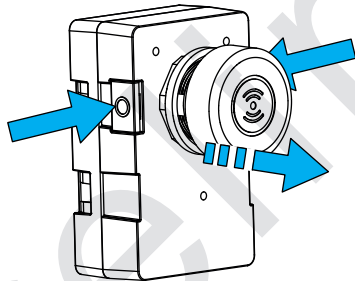
In the example, the position of the recess is such that the cable for the base unit exits upwards.

Note: The recess for the latch on the read head points in the direction of the cable outlet on the base unit. Position the recess to achieve the desired cable outlet.

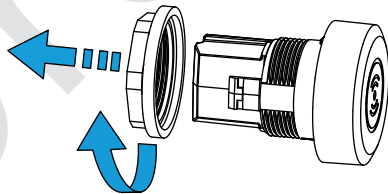
- ▶ On your device, if the read head is not installed on the base (e.g. as delivered), you can skip this step.

Otherwise:

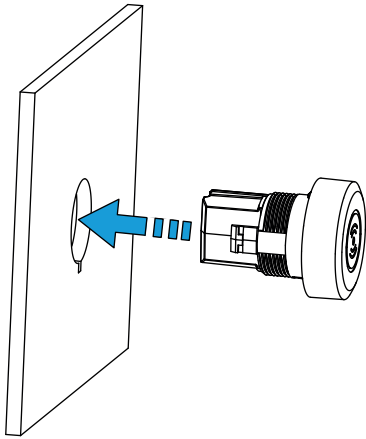
On the sides of the base unit housing, press and hold the two release buttons, then pull the read head from the base unit.



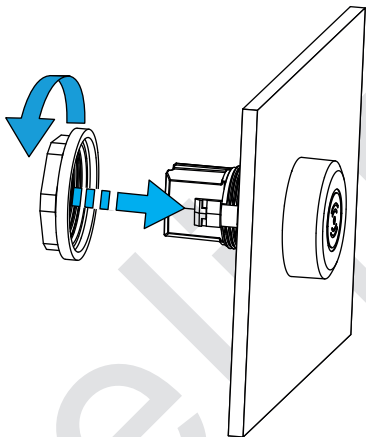
- ▶ Remove the plastic nut (M22) from the read head.



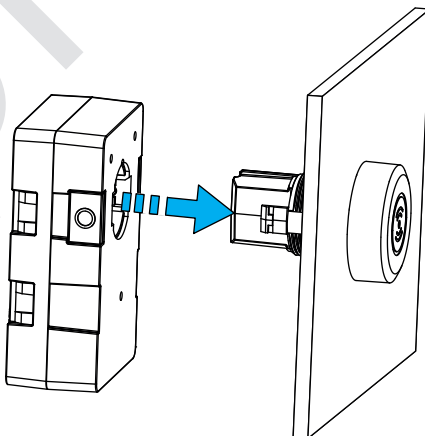
- ▶ From the front, insert the read head into the mounting cutout so that the latch is positioned in the recess on the mounting cutout.



- ▶ Align the silicone cap on the read head in the required direction.  
Note: After alignment, the latch must be positioned in one of the recesses on the silicone cap.
- ▶ Use the plastic nut (M22) to secure the read head from the other side.  
Note the torque setting of 1.3 ... 2.1 Nm. We recommend that you use the installation wrench "PIT es wrench to fasten the plastic nut (see [Order reference \[87\]](#)).



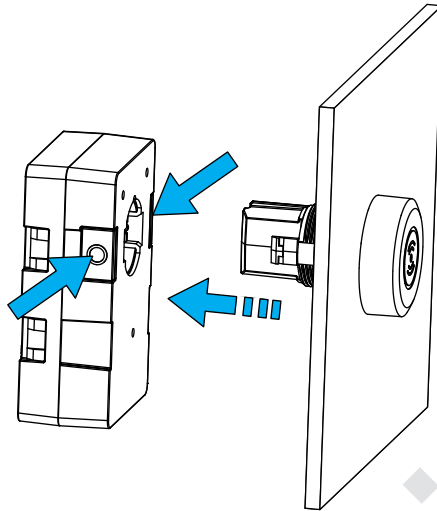
- ▶ Connect the base unit to the read head.  
The base unit must lock in position.



### 6.3.2 Removal of PITreader Card

#### Procedure

- ▶ Remove the power to the PITreader.
- ▶ On the sides of the base unit housing, press and hold the two release buttons.
- ▶ Pull gently on the base unit of the PITreader until the base unit detaches from the read head.



### 6.3.3 Apply sticker

A PITreader transponder sticker has a self-adhesive side. Use this side to apply the transponder sticker to an existing card (e.g. customer card).



#### NOTICE

##### Transponder recognition impaired

If the transponder sticker is applied to a metallic carrier material (e.g. card with a metallic surface), the PITreader may be unable to recognise the transponder.

Never apply the transponder sticker to a metallic carrier material.

### 6.4 Installation and removal of a PIT gb with PITreader

You'll find the necessary information in the operating manual PIT gb RLLE y ETH.

## 6.5 Dimensions

### 6.5.1 Dimensions of PITreader Key

Dimensions in mm

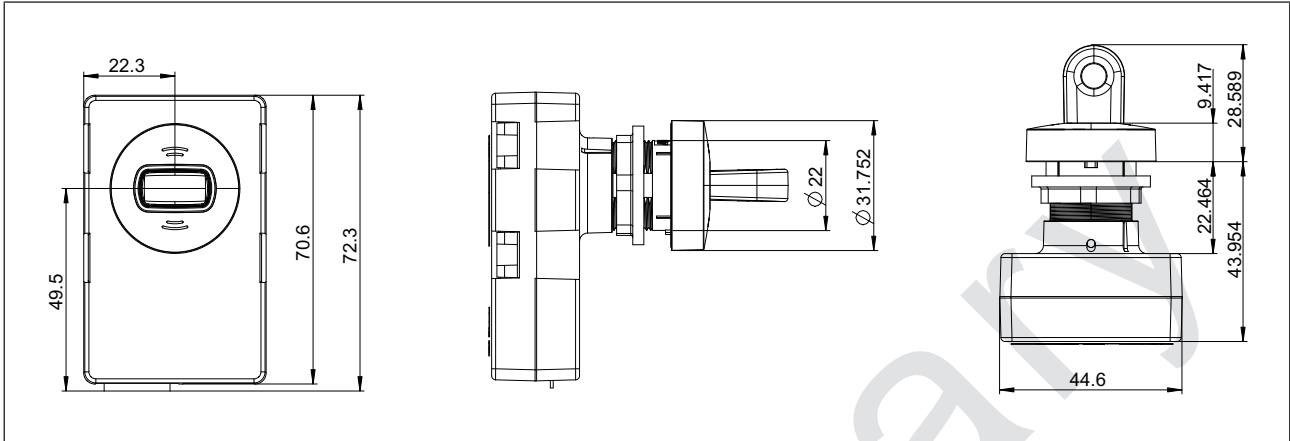


Fig.: Dimensions of a PITreader Key (base unit with spring-loaded terminal, read head PITreader key Adapter h and positioned transponder key)

### 6.5.2 Dimensions of PITreader Card

Dimensions in mm

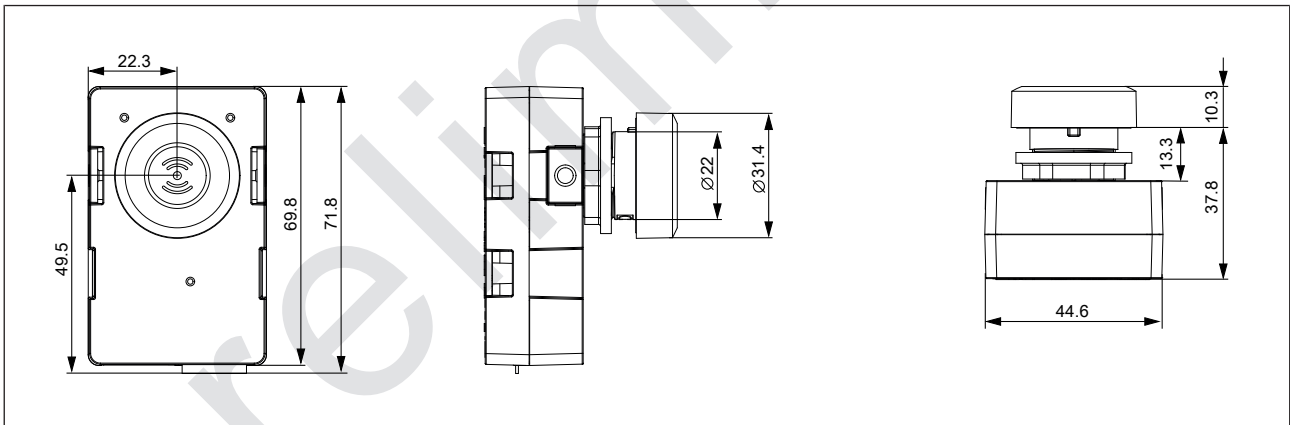


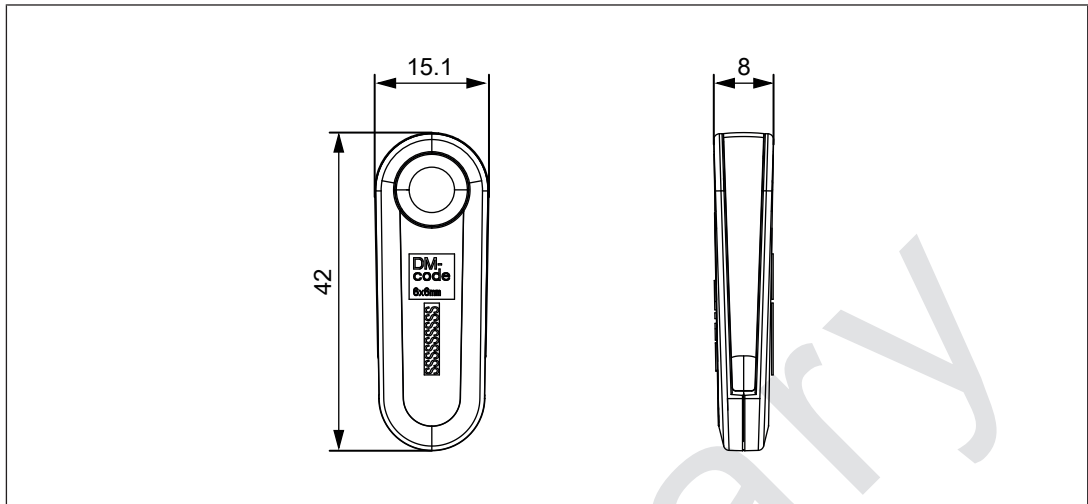
Fig.: Dimensions of a PITreader Card (base unit with spring-loaded terminal and read head PITreader card Adapter)

### 6.5.3 Dimensions of PIT gb with PITreader

You'll find the necessary information in the operating manual PIT gb RLL E y ETH.

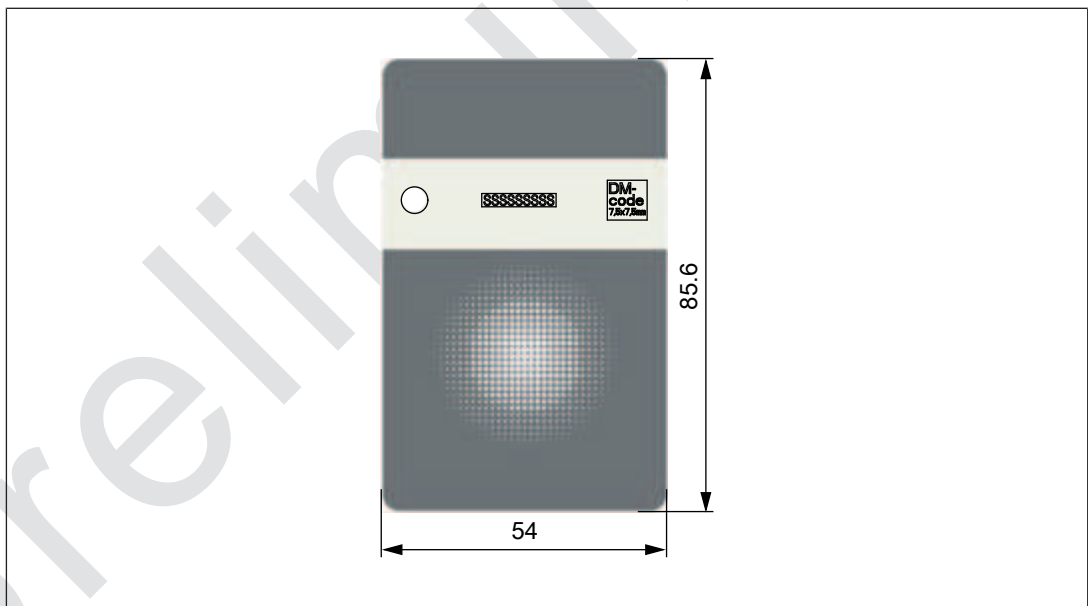
### 6.5.4 Dimensions of PITreader transponder key

Dimensions in mm



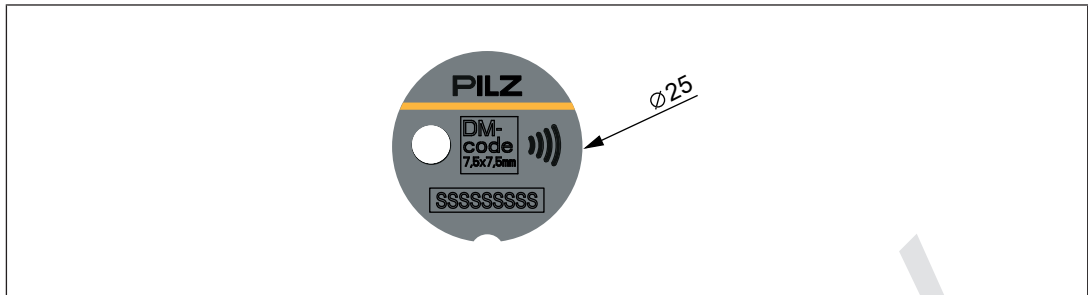
### 6.5.5 Dimensions of PITreader transponder card

Dimensions in mm



### 6.5.6 Dimensions of PITreader transponder sticker

Dimensions in mm



preliminary

## 7 Wiring

### 7.1 Base unit without safe evaluation unit (standalone)

This section describes how to wire the base unit of a PITreader Key or PITreader Card when you are not using a safe evaluation unit (SEU).

Information on wiring a PIT gb with PITreader can be found in the operating manual PIT gb RLL E y ETH.

#### Procedure

1. Connect 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

Information on wiring a PITreader Key or PITreader Card with a safe evaluation unit PIT m4SEU can be found in the operating manual PIT m4SEU.

## 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 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.

preliminary



## 8.2 Network discovery with Multicast DNS (mDNS)

A PITreader can be found in the network via the Multicast DNS protocol (mDNS).

Via mDNS, PITreader devices can be found under the following two domain names:

- ▶ pitreader.pilz.local

All PITreader devices in a network can be found via the address pitreader.pilz.local.

- ▶ pilz-<OrderNumber>-<SerialNumber>.local

Via the address pilz-<OrderNumber>-<SerialNumber>.local, an individual PITreader can be selectively addressed in a network.

A Multicast DNS query uses the Multicast Ipv4 group address 224.0.0.251. Multicast DNS queries to a PITreader take place via UDP and via port 5353.

A PITreader responds to the following Multicast DNS queries:

- ▶ QTYPE: ANY, A
- ▶ CLASS: IN

Multicast DNS queries with QTYPE ANY contain the following response sections:

- ▶ IP address of the PITreader
- ▶ Host name and domain
- ▶ HTTPS port number
- ▶ Order number
- ▶ Serial number
- ▶ MAC address

Multicast DNS queries with QTYPE A contain the following response sections:

- ▶ <IP address of the PITreader>

Network discovery via mDNS is active when a PITreader is delivered and can be deactivated by the user via the device settings.

## 8.3 Network configuration via Multicast protocol

Via IPv4 Multicast, a device can be commissioned without the user and their end device having to be in the same subnet.

The device's IP configuration can be performed via IPv4 Multicast:

- ▶ IP address
- ▶ Subnet mask
- ▶ Standard gateway

Via IPv4 Multicast, it is possible to flash the LEDs used to find, locate or identify the device. For configuration via IPv4 Multicast, the device listens to the IPv4 Multicast address 239.255.0.12 and UDP port 7075.

**Configuration via IPv4 Multicast is only possible when the password for the standard "admin" user is still active, corresponding to the delivery status.**

The network configuration via the Multicast protocol is active when a PITreader is delivered and can be deactivated by the user via the device settings.

## 8.4 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](#) [📖 60]).

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 [Unit view PITreader Key](#) [📖 10]).

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

### 5. Change default password

The message "The default password has not been changed" is displayed. Change the default password under **User -> Profile -> Change password**. Enter a secure password with at least 8 characters (for features of a secure password see [Security](#) [📖 16]).

### 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.

## 8.5 Device user

Additional device users can be created in the web application under **User -> Device user**. An "admin" device user is already created with the following properties:

- ▶ Status: Active
- ▶ Role: Administrator
- ▶ Authentication: Name/password
- ▶ Password: Serial number of the PITreader

Device users can be assigned roles; i.e. it is possible to define which activities a device user is allowed to perform in the web application.

There are 4 roles:

|                                       | Administrator | Device manager | Transponder manager | Guest (read-only) |
|---------------------------------------|---------------|----------------|---------------------|-------------------|
| Device settings                       | R/W           | (R/W)*         | R                   | R                 |
| TLS configuration                     | R/W           | R              | R                   | R                 |
| OPC UA configuration                  | R/W           | R/W            |                     |                   |
| Basic coding                          | R/W           | R/W            | R                   | R                 |
| OEM coding                            | R/W           |                |                     |                   |
| Device group name                     | R/W           | R/W            | R                   | R                 |
| User data configuration               | R/W           | R/W            | R                   | R                 |
| Manage device user                    | R/W           | R/W**          |                     |                   |
| Permission list                       | R/W           | R/W            | R/W                 |                   |
| Block list                            | R/W           | R/W            | R/W                 |                   |
| Transponder                           | R/W           | R/W            | R/W                 | R                 |
| External authentication and LED (API) | R/W           | R/W            | R/W                 | R                 |
| Reset single authentication           | R/W           | R/W            | R                   | R                 |
| Diagnostics                           | R             | R              | R                   | R                 |
| Firmware update                       | R/W           | R/W            |                     |                   |
| Save/restore device configuration     | R/W           | R/W***         |                     |                   |
| Factory reset                         | R/W           |                |                     |                   |

R = Read-only access, R/W = Read/write access

\* The following settings only: location description, device group, evaluate validity date, time zone, date/time

- \*\* With the exception of administrator users
- \*\*\* With the exception of administrator users, and only the permitted device configuration settings can be restored

A maximum of 20 device users can be managed. Each device user must be assigned a distinct name; each name may only occur once. One of the 4 roles can be assigned to each device user.

By specifying a remote IP address, access to the device with the relevant access data can be restricted to a certain IP address on the opposite terminal (IP address of the PC or controller).

## 8.6 Manage certificates

### 8.6.1 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 examined in 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, in the web application under **Settings -> Certificate**, you can download the current certificate for the HTTPs connection of the PITreader 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**.

### 8.6.2 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)

preliminary

## 8.7 Configure authentication mode

You can configure the authentication mode for the PITreader in the web application under **Configuration -> Settings**. Select either "Transponder data", "External" or "Permission list" authentication mode.

You can allow the permission for the device group and the user data to be overwritten externally via the REST API, irrespective of the authentication mode. To do this, activate the **Allow external overwriting** field under **Configuration -> Settings -> Function**.

If the **Allow external overwriting** field is activated, then

- ▶ The permission that is read from the transponder in "Transponder data" authentication mode, or is read from a file in "Permission list" authentication mode, is overwritten.
- ▶ The user data that is read from the transponder is overwritten.

The external user data is valid until the transponder is removed or another transponder is positioned in the read area. Only external user data for which there is an ID available in the user data configuration is overwritten.

## 8.8 Configure authentication type

You can configure the authentication type for the PITreader in the web application under **Configuration -> Settings**. Select one of the authentication types "Basic", "Single authentication" or "2-person rule".

## 8.9 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.

## 8.10 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.

## 8.11 Set device group

In the web application, under **Configuration -> Settings -> Function**, you can assign a device group to the PITreader (see also [Device groups](#) [📖 19]). 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.

## 8.12 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](#) [ 32].

## 8.13 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.

If you wish to use the OEM coding for your service staff, for example, then the appropriate identifier must be set as OEM coding on all PITreader devices that you send to your customers.

See also [Coding](#) [ 32].



## 8.14 Write/program transponder

### 8.14.1 Program permissions

In the web application you can read the permissions for the transponder (under **Transponder -> Data**) and write permissions for the transponder (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, thereby preventing the permissions being changed at a later date.



#### NOTICE

Note:

- Once a transponder 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 will also be automatically taught in to the basic coding of the PITreader when writing/programming the permissions.

### 8.14.2 Configure the validity of the transponder

You can limit the validity of transponder 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 (in the format day, month, year "DD.MM.YYYY") under **Transponder -> Permissions**.

### 8.14.3 Teach in transponder to basic coding

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

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

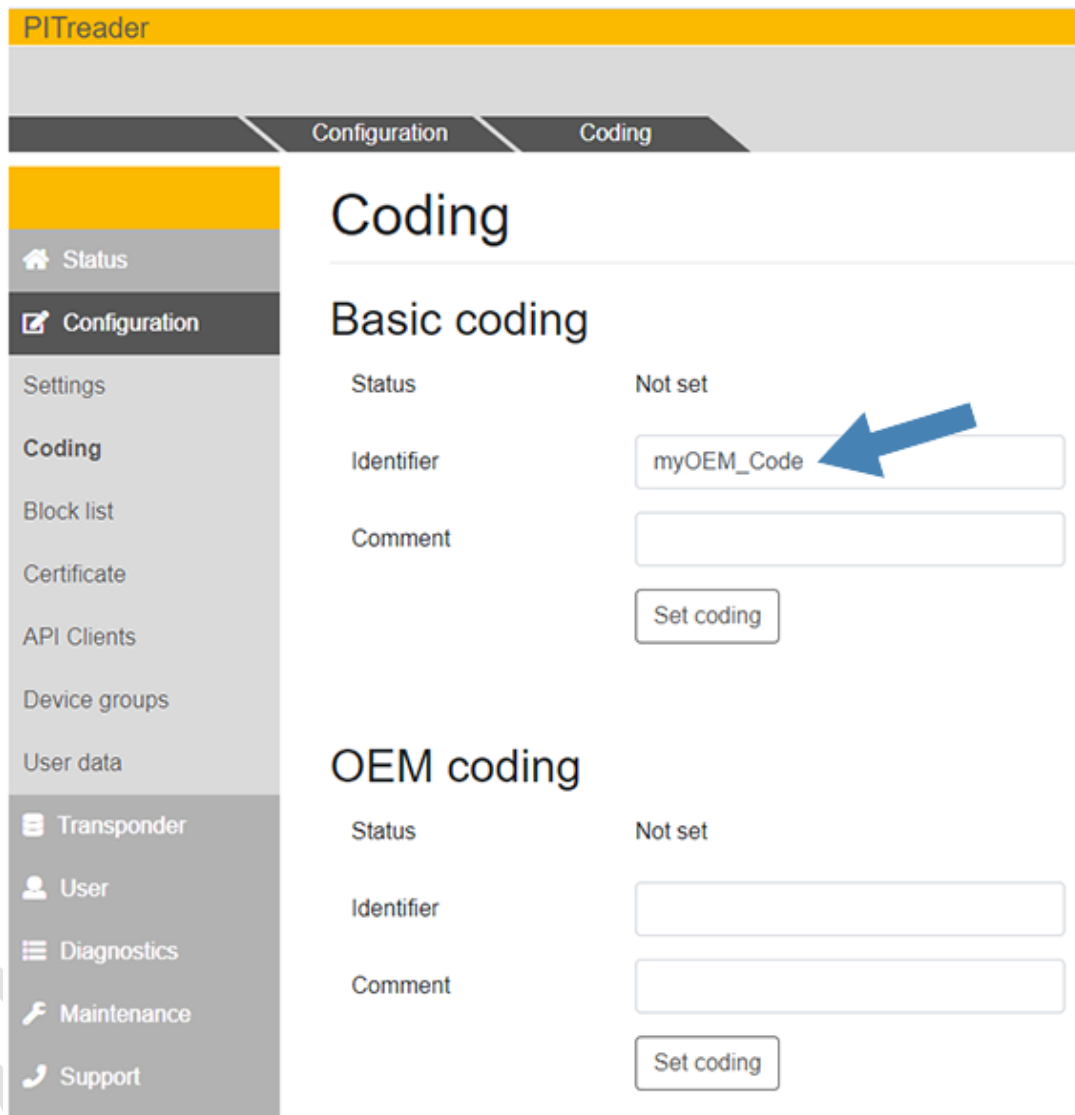
You can change the coding of the transponder by teaching in the transponder to a different basic coding. You can remove the coding of the transponder by rewriting the permissions on the transponder on a PITreader without a set basic coding.

### 8.14.4 Teach in transponder to OEM coding

Transponders can only be taught in to the base coding stored in a PITreader. To teach in a transponder to OEM coding, the OEM identifier must first be set as basic coding in the PITreader.

In the web application, under **Configuration -> Coding**, enter the OEM identifier instead of a basic identifier under **Basic coding** and click on **Set coding**.

Example:



If you are using an unlocked transponder, you can teach in the transponder to the OEM identifier under **Transponder -> Permissions -> Program**.

If you are using a locked transponder or a transponder that has been factory pre-programmed by Pilz, you can teach in the transponder to the OEM identifier under **Transponder -> Data -> Teach in transponder**.

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

Note: As a machine manufacturer, if you wish to code transponders for service staff, ideally you should use a PITreader that is only used for this purpose. This guarantees that new transponders with this OEM identifier can only be created by a person who knows the OEM identifier or who has a PITreader that has been configured specifically for this purpose.

### 8.14.5 Limit transponder to identically coded PITreaders

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

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

### 8.14.6 Edit user data values

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

Certain data on the PITreader can also be programmed using the PIT Transponder Manager Tool and transponders can be programmed.

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](#) [69]). Should there be more parameters on the transponder, these will be ignored. Should there be fewer parameters on the transponder, the data type's initial value is displayed for the parameters that are missing.  
When the user data is saved on the transponder, 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.
- ▶ 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.

## 8.15 Permission list

You can enter permissions in the web application under **Permission list**.

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

- ▶ The CSV file must contain two columns. The first column must contain the security ID, the second column must contain the permission for the security ID.
- ▶ 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 permission list. Before importing you should check that there are no duplicated entries in the CSV file.
- ▶ The permissions can be imported in hex or decimal notation (see also [Overview of permissions \[84\]](#)).
- ▶ A semicolon is used as the separator.
- ▶ Fields and values may be framed in quotation marks (").
- ▶ The import is only performed if all entries can be validated successfully.
- ▶ During import, the imported entries replace all the permission list entries in the web application.

See also ["Permission list" authentication mode \[22\]](#).

## 8.16 Use block list

You can lock the authentication of certain transponders by entering the security IDs of these transponders (and an optional comment) under **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 \[35\]](#).

## 8.17 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.

Certain data on the PITreader can also be programmed using the PIT Transponder Manager Tool and transponders can be programmed.

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.

## 8.18 API Clients

Under **User -> Device user** 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”.

## 8.19 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, device users, block list, permission list, name of device groups, user data configuration and OPC UA Client certificates. TLS certificates, OPC UA Server certificates and coding identifiers are not included in the backup and cannot be restored.

preliminary

## 8.20 Reset to default settings

The PITreader can be reset to its factory 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 basic 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
- ▶ Device user
- ▶ Diagnostic log
- ▶ Transponder block list
- ▶ Permission 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.

preliminary



## 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.

preliminary

## 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 positioned transponder   |
| Blue   |       | Device is ready for operation, no transponder has been recognised  |
| Blue   |       | Mode for locating the device is active (see <a href="#">Network configuration via Multicast protocol</a> [ 57])  |
| Green  |       | Transponder has been recognised as valid   |
| Green  |       | 2-person rule<br>Possible reasons:<br><ul style="list-style-type: none"> <li>▶ The authentication process was started with the first transponder.</li> <li>▶ When the first transponder is removed, the LED flashes until the second transponder is positioned in the read area or the 30 s time window has elapsed.</li> </ul>  |
| Red    |       | Transponder has been recognised as invalid<br>Possible reasons:<br><ul style="list-style-type: none"> <li>▶ Transponder in the read area:<br/>Authentication is denied (e.g. permission = 0).</li> <li>▶ No transponder in the read area:<br/>Authentication on the device is blocked (e.g. via 24 V I/O port or single authentication)</li> </ul> You'll find further information in the web application under <b>Status -&gt; Authentication</b> |

| Colour | State   | Meaning  |
|--------|---|--|
| Red    |  | <p>Error</p> <ul style="list-style-type: none"> <li>▶ Possible reasons: (PITreader Card only):                             <ul style="list-style-type: none"> <li>– A transponder from Pilz was not clearly recognised.</li> <li>– Several transponders from Pilz are recognised.</li> <li>– At least one transponder from a third-party manufacturer is recognised.</li> </ul> </li> </ul> <p>Possible remedies:</p> <ul style="list-style-type: none"> <li>– Remove transponder from the read area</li> <li>– Position exactly one transponder from Pilz in the read area.</li> </ul> <p>Note: Once the fault has been rectified, the fault indicator is deactivated automatically.</p> <ul style="list-style-type: none"> <li>▶ Other reasons (all PITreader):<br/>e.g. hardware error, configuration error, invalid or uncoded transponder, etc.</li> </ul> <p>Possible remedies in the event of a configuration error and when the device is no longer accessible under the set IP address:</p> <ul style="list-style-type: none"> <li>– Try to open the web application with the default IP address or</li> <li>– Reset the device to its factory default settings.</li> </ul> |

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](#)  [71].

## 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](#) [📖 71].

## 10.3 Diagnostics

The PITreader provides options for device diagnostics and statistical evaluation.

- ▶ Diagnostics using the device LED

Information regarding evaluation of the device LED can be found under [LED indicator](#) [📖 74].

- ▶ Diagnostics using the diagnostic list (web application)

The diagnostic list contains a list of the active alarms. You can read the diagnostic list in the web application under **Diagnostics**.

- ▶ Diagnostics using the diagnostic log (web application)

In the diagnostic log, the events are logged with a time stamp; i.e. the message is logged by "Message arrived" and "Message cleared". You can read the diagnostic log in the web application under **Diagnostics**.

Under **Diagnostics -> 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.



### NOTICE

#### Protecting personal data

Logs may contain personal data, depending on the filter that has been set.

When exporting a log with personal data, make sure to use a storage medium with adequate security.

- ▶ Statistics (web application)

You'll find information on various settings and evaluations under [Statistics](#) [📖 77].

### 10.3.1 Statistics

You can make various settings for the statistical evaluations in the web application under **Diagnosics -> Statistics**. Various information about the static evaluations is also displayed.

▶ **Start date**

The actual start data for statistical evaluation is displayed.

▶ **Refresh** button

The statistics can be recreated using the **Refresh** button.

▶ Define **Start date** and **end date**

By entering a start and end date it is possible to define a time window, for which the statistical evaluations are displayed.

▶ **Transponder** area

The table under **Transponder** is only displayed if personal data logging is activated under **Configuration -> Settings -> Function**. The transponders are identified in the table by their security IDs (**Security ID** column).

Statistical values for a transponder:

– **Duration (total)**

This column contains the calculated total time that a transponder has been in the read area.

For format of time display see [1].

– **Duration (median)**

This column contains the time that a transponder has been in the read area, calculated from a "median" perspective.

- For format of time display see [1]

- Definition of "Median" see [2]

– **Successful authentication**

This column contains the sum of all successful authentication attempts made by a transponder.

– **Failed authentication**

This column contains the sum of all failed authentication attempts made by a transponder.

Note:

Log entries that contain no security ID in the parameters due to the personal data logging setting are ignored in the statistical evaluation; i.e. the table under **Transponder** contains no entries for transponders that have no information in the **Security ID** column.

▶ **Authenticated permission** area

The table under **Authenticated permission** only lists the permissions that have been used at least once for a successful authentication.

Statistical values for a permission:

– **Permission**

This column contains the authenticated permission as a value between 0 and 64.

– **Quantity**

The value in this column indicates how often a permission has been used for a successful authentication.

– **Duration (total)**

This column contains the calculated total time for which the permission was active in the device.

- For format of time display see [1]

– **Duration (median)**

This column contains the time for which the permission was active in the device, calculated from a "median" perspective.

- For format of time display see [1]

- Definition of "Median" see [2]

Note:

If a transponder is removed and repositioned within a maximum of 2 s, then this is not evaluated as a new authentication in the statistics.

► **Activated operating mode** area

The evaluations are based on the data reported from a safe evaluation unit PIT m4SEU. For this reason, the table is only displayed when a safe evaluation unit is connected to a base unit.

Evaluations of the operating modes are displayed in the table under **Activated operating mode**.

– Operating mode

All operating modes are listed in the column (operating mode 1 ... 5).

– Duration (total)

This column contains the calculated total time for which the operating mode was active in the device.

- For format of time display see [1]

– Duration (median)

This column contains the time for which the operating mode was active in the device, calculated from a "median" perspective.

- For format of time display see [1]

- Definition of "Median" see [2]

[1]

Time format: <Day(d) Hour(h) Minute(m) Second(s)>

Examples:

► 1h 0m 1s

► 1d 0h 20m 5s

[2]

The median of a series of values is the value that is right in the middle, if you sort the values by size.

## 11 Maintenance and testing

It is not necessary to perform maintenance work on the product in normal operation. Please return any faulty products to Pilz.

preliminary

## 12 Technical details

The technical details of the PITreader base unit (order no. 402255) and the technical details of the PITreader S base unit (order no. 402256) are identical.

The technical details of the PITreader card unit (order no. 402320) and the technical details of the PITreader S card unit (order no. 402321) are identical.

| <b>General</b>                                  | <b>402255</b>   | <b>402320</b>   |
|---|---|---|
| Certifications                                  | <b>CE, FCC, IC, UKCA, cULus Listed</b>                  | <b>CE, UKCA</b>   |
| Sensor's mode of operation                      | <b>Transponder</b>                                      | <b>Transponder</b>  |
| <b>Transponder</b>                              | <b>402255</b>   | <b>402320</b>   |
| Transponder type                                | <b>Transponder key</b>                                  | <b>Transponder card, Transponder key, Transponder sticker</b> |
| Energy supply to transponder                    | <b>passive (battery free)</b>                           | <b>passive (battery free)</b>                                 |
| Frequency band                                  | <b>13,24 - 13,88 MHz</b>                                | <b>13,24 - 13,88 MHz</b>                                      |
| Max. transmitter output                         | <b>170 mW</b>   | <b>170 mW</b>   |
| <b>Electrical data</b>                          | <b>402255</b>   | <b>402320</b>   |
| Supply voltage                                  |   |   |
| Voltage   | <b>24 V</b>   | <b>24 V</b>   |
| Kind  | <b>DC</b>   | <b>DC</b>   |
| Type of power supply                            | <b>SELV/PELV</b>  | <b>SELV/PELV</b>  |
| Voltage tolerance                               | <b>-15 %/+20 %</b>                                      | <b>-15 %/+20 %</b>  |
| Output of external power supply (DC)            | <b>4 W</b>  | <b>4 W</b>  |
| External unit fuse protection F1                | <b>4 A, circuit breaker 24 V DC, characteristic B/C</b> | <b>4 A, circuit breaker 24 V DC, characteristic B/C</b>       |
| Status indicator                                | <b>LED</b>  | <b>LED</b>  |
| Power dissipation                               | <b>2,5 W</b>  | <b>2,5 W</b>  |
| <b>Inputs</b>                                   | <b>402255</b>   | <b>402320</b>   |
| Signal level at "1"                             | <b>15 - 30 V DC</b>                                     | <b>15 - 30 V DC</b>   |
| Input current range                             | <b>4 mA</b>   | <b>4 mA</b>   |
| Galvanic isolation                              | <b>No</b>   | <b>No</b>   |
| <b>Semiconductor outputs</b>                    | <b>402255</b>   | <b>402320</b>   |
| Overall performance ext. loading, semiconductor | <b>1,2 W</b>  | <b>1,2 W</b>  |
| Number  | <b>1</b>  | <b>1</b>  |
| Switching current per output                    | <b>50 mA</b>  | <b>50 mA</b>  |
| Galvanic isolation                              | <b>No</b>   | <b>No</b>   |
| Short circuit-proof                             | <b>yes</b>  | <b>yes</b>  |
| <b>Ethernet interface</b>                       | <b>402255</b>   | <b>402320</b>   |
| Number  | <b>1</b>  | <b>1</b>  |
| IP address, factory setting                     | <b>192.168.0.12</b>                                     | <b>192.168.0.12</b>   |
| Connection type                                 | <b>RJ45</b>   | <b>RJ45</b>   |
| Transmission rate                               | <b>10/100 Mbit/s</b>                                    | <b>10/100 Mbit/s</b>  |



| <b>Times</b>  | <b>402255</b>                           | <b>402320</b>                           |
|---|---|---|
| Supply interruption before de-energisation  | 10 ms                                   | 10 ms                                   |
| <b>Environmental data</b>   | <b>402255</b>                           | <b>402320</b>                           |
| Ambient temperature   |   |   |
| In accordance with the standard   | EN 60068-2-14                           | EN 60068-2-14                           |
| Temperature range   | -30 - 55 °C                             | -30 - 55 °C                             |
| Storage temperature   |   |   |
| In accordance with the standard   | EN 60068-2-1/-2                         | EN 60068-2-1/-2                         |
| Temperature range   | -30 - 70 °C                             | -30 - 70 °C                             |
| Climatic suitability  |   |   |
| In accordance with the standard   | EN 60068-2-78                           | EN 60068-2-78                           |
| Humidity  | 93 % r. h. at 40 °C                     | 93 % r. h. at 40 °C                     |
| Max. operating height above sea level   | 2000 m                                  | 2000 m                                  |
| EMC   | EN 301489-1 V2.1.1                      | EN 301489-1 V2.1.1                      |
| MTBF  | 36 years                                | 36 years                                |
| Vibration   |   |   |
| In accordance with the standard   | EN 60068-2-6                            | EN 60068-2-6                            |
| Frequency   | 5 - 8,4 Hz, 8,4 - 150 Hz                | 5 - 8,4 Hz, 8,4 - 150 Hz                |
| Amplitude   | 3,5 mm                                  | 3,5 mm                                  |
| Acceleration  | max. 1g                                 | max. 1g                                 |
| Shock stress  |   |   |
| In accordance with the standard   | EN 60068-2-27                           | EN 60068-2-27                           |
| Acceleration  | 15g                                     | 15g                                     |
| Duration  | 11 ms                                   | 11 ms                                   |
| Protection type   |   |   |
| In accordance with the standard   | EN 60529                                | EN 60529                                |
| Housing   | IP20                                    | IP20                                    |
| Front   | IP65/IP67                               | IP65/IP67                               |
| Mounting area (e.g. control cabinet)  | ≥ IP54                                  | ≥ IP54                                  |
| <b>Mechanical data</b>  | <b>402255</b>                           | <b>402320</b>                           |
| Mounting position   | Any                                     | Any                                     |
| Material  |   |   |
| Bottom  | PC                                      | PC                                      |
| Front   | PC                                      | PC                                      |
| Connection type   | Spring-loaded terminal, plug-in         | Spring-loaded terminal, plug-in         |
| Mounting type   | plug-in                                 | plug-in                                 |
| Max. torque setting for fixing screws   | 1,3 - 2,1 Nm                            | 1,3 - 2,1 Nm                            |
| Conductor cross section with spring-loaded terminals: Flexible with/without crimp connector | 0,2 - 1,5 mm <sup>2</sup> , 24 - 14 AWG | 0,2 - 1,5 mm <sup>2</sup> , 24 - 14 AWG |
| Spring-loaded terminals: Terminal points per connection                                     | 1                                       | 1                                       |

| <b>Mechanical data</b>                        | <b>402255</b> | <b>402320</b> |
|---|---------------|---------------|
| Stripping length with spring-loaded terminals | <b>8 mm</b>   | <b>8 mm</b>   |
| Dimensions                                    |               |               |
| Height  | <b>54 mm</b>  | <b>49 mm</b>  |
| Width   | <b>72 mm</b>  | <b>72 mm</b>  |
| Depth   | <b>45 mm</b>  | <b>45 mm</b>  |
| Weight  | <b>47 g</b>   | <b>62 g</b>   |

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

Note:

The technical details of the pushbutton unit PIT gb RLLE y ETH can be found in the operating manual PIT gb RLLE y ETH.

preliminary

## 13 Supplementary data

### 13.1 Radio approvals PITreader Key

#### FCC/IC approval

|   |
|---|
| <p><b>USA/Canada</b></p> <p><b>FC</b> FCC ID: VT8- PITRD01<br/>IC: 7482A- PITRD01</p> <p><u>FCC/IC-Requirements:</u><br/>This product complies with Part 15 of the FCC Rules and with Industry Canada licence-exempt RSS standards.<br/>Operation is subject to the following two conditions:<br/>1) this product may not cause harmful interference, and<br/>2) this product must accept any interference received, including interference that may cause undesired operation.</p> <p>Changes or modifications made to this product not expressly approved by Pilz may void the FCC authorization to operate this equipment.</p> <p>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.</p> <p>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:<br/>(1) le produit ne doit pas produire de brouillage, et<br/>(2) l'utilisateur de le produit doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.</p> |
|---|

### 13.2 Radio approvals PITreader Card

#### FCC/IC approval

|   |
|---|
| <p><b>USA/Canada</b></p> <p><b>FC</b> FCC ID: VT8- PITRD11<br/>IC: 7482A- PITRD11</p> <p><u>FCC/IC-Requirements:</u><br/>This product complies with Part 15 of the FCC Rules and with Industry Canada licence-exempt RSS standards.<br/>Operation is subject to the following two conditions:<br/>1) this product may not cause harmful interference, and<br/>2) this product must accept any interference received, including interference that may cause undesired operation.</p> <p>Changes or modifications made to this product not expressly approved by Pilz may void the FCC authorization to operate this equipment.</p> <p>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.</p> <p>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:<br/>(1) le produit ne doit pas produire de brouillage, et<br/>(2) l'utilisateur de le produit doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.</p> |
|---|

### 13.3 Network data

| Protocol                | Direction [*] | Transport protocol | Port no.                    | Can be deactivated       | Description   |
|-------------------------|---------------|--------------------|-----------------------------|--------------------------|---|
| HTTP                    | In            | TCP                | 1 ... 65535<br>Default: 80  | Yes                      | <b>Web application:</b><br>Browser is always forwarded to HTTPS   |
| HTTPS                   | In            | TCP                | 1 ... 65535<br>Default: 443 | No                       | <b>Web application:</b><br>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<br>Default: 502 | Yes<br>Default: Inactive | <b>Modbus/TCP Server</b>  |
| NTP                     | Out           | UDP                | 1 ... 65535<br>Default: 123 | Yes<br>Default: Inactive | <b>SNTP Client</b>  |
| OPC UA                  | In            | TCP                | 4840                        | Yes<br>Default: Inactive | <b>PITreader OPC Server UA</b>  |
| mDNS                    | In            | UDP                | 5353                        | Yes                      | <b>Network discovery with Multicast DNS</b><br>(224.0.0.251)  |
| Multicast configuration | In            | UDP                | 7075                        | Yes                      | <b>Network configuration via Multicast protocol</b><br>(239.255.0.12)   |

[\*]

**in:** The communication partner starts communication with the device.

**out:** The device starts communication with the communication partner.

### 13.4 Overview of permissions

| Permission | Code        |         |
|------------|-------------|---------|
|            | Hexadecimal | Decimal |
| 0          | 0x00000000  | 0       |
| 1          | 0x000001ff  | 511     |
| 2          | 0x00003e0f  | 15887   |
| 3          | 0x00003ff0  | 16368   |
| 4          | 0x0001c633  | 116275  |
| 5          | 0x0001c7cc  | 116684  |
| 6          | 0x0001f83c  | 129084  |
| 7          | 0x0001f9c3  | 129475  |
| 8          | 0x00064a55  | 412245  |
| 9          | 0x00064baa  | 412586  |

| Permission | Code        |         |
|------------|-------------|---------|
|            | Hexadecimal | Decimal |
| 10         | 0x0006745a  | 423002  |
| 11         | 0x000675a5  | 423333  |
| 12         | 0x00078c66  | 494694  |
| 13         | 0x00078d99  | 495001  |
| 14         | 0x0007b269  | 504425  |
| 15         | 0x0007b396  | 504726  |
| 16         | 0x000a94aa  | 693418  |
| 17         | 0x000a9555  | 693589  |
| 18         | 0x000aaaa5  | 699045  |
| 19         | 0x000aab5a  | 699226  |
| 20         | 0x000b5299  | 742041  |
| 21         | 0x000b5366  | 742246  |
| 22         | 0x000b6c96  | 748694  |
| 23         | 0x000b6d69  | 748905  |
| 24         | 0x000cdeff  | 843519  |
| 25         | 0x000cdf00  | 843520  |
| 26         | 0x000ce0f0  | 844016  |
| 27         | 0x000ce10f  | 844047  |
| 28         | 0x000d18cc  | 858316  |
| 29         | 0x000d1933  | 858419  |
| 30         | 0x000d26c3  | 861891  |
| 31         | 0x000d273c  | 862012  |
| 32         | 0x00304c6a  | 3165290 |
| 33         | 0x00304d95  | 3165589 |
| 34         | 0x00307265  | 3175013 |
| 35         | 0x0030739a  | 3175322 |
| 36         | 0x00318a59  | 3246681 |
| 37         | 0x00318ba6  | 3247014 |
| 38         | 0x0031b456  | 3257430 |
| 39         | 0x0031b5a9  | 3257769 |
| 40         | 0x0036063f  | 3540543 |
| 41         | 0x003607c0  | 3540928 |
| 42         | 0x00363830  | 3553328 |
| 43         | 0x003639cf  | 3553743 |
| 44         | 0x0037c00c  | 3653644 |
| 45         | 0x0037c1f3  | 3654131 |

| Permission | Code        |          |
|------------|-------------|----------|
|            | Hexadecimal | Decimal  |
| 46         | 0x0037fe03  | 3669507  |
| 47         | 0x0037ffc   | 3670012  |
| 48         | 0x003ad8c0  | 3856576  |
| 49         | 0x003ad93f  | 3856703  |
| 50         | 0x003ae6cf  | 3860175  |
| 51         | 0x003ae730  | 3860272  |
| 52         | 0x003b1ef3  | 3874547  |
| 53         | 0x003b1f0c  | 3874572  |
| 54         | 0x003b20fc  | 3875068  |
| 55         | 0x003b2103  | 3875075  |
| 56         | 0x003c9295  | 3969685  |
| 57         | 0x003c936a  | 3969898  |
| 58         | 0x003cac9a  | 3976346  |
| 59         | 0x003cad65  | 3976549  |
| 60         | 0x003d54a6  | 4019366  |
| 61         | 0x003d5559  | 4019545  |
| 62         | 0x003d6aa9  | 4025001  |
| 63         | 0x003d6b56  | 4025174  |
| 64         | 0x00c04e98  | 12603032 |

## 14 Order reference

### 14.1 Authentication system PITreader Key

| Product type            | Features   | Order no. |
|-------------------------|--|-----------|
| PITreader base unit     | RFID authentication system<br>Contents: Base unit, connector [402307]<br>Required accessories: PITreader key Adapter h                               | 402255    |
| PITreader S base unit   | RFID authentication system with advanced function range,<br>Contents: Base unit, connector [402307]<br>Required accessories: PITreader key Adapter h | 402256    |
| PITreader key Adapter h | 1x PITreader key adapter horizontal + 1x nut for PITreader base unit   | 402308    |

### 14.2 Authentication system PITreader Card

| Product type          | Features   | Order no. |
|-----------------------|--|-----------|
| PITreader card unit   | RFID authentication system for cards, stickers & keys<br>Contents: Base unit, connector [402307], PITreader card Adapter                               | 402320    |
| PITreader S card unit | RFID authentication system for cards, stickers & keys, with advanced function range<br>Contents: Base unit, connector [402307], PITreader card Adapter | 402321    |

### 14.3 Transponder key

| Product type          | Features   | Order no. |
|-----------------------|--|-----------|
| PITreader key ye g    | Transponder key for authentication system PITreader, permissions freely configurable<br>Colour: yellow<br>Material: plastic        | 402260    |
| PITreader key ye g bk | Generic transponder key for authentication system PITreader, permissions freely configurable<br>Colour: black<br>Material: plastic | 402260BK  |
| PITreader key ye g bl | Generic transponder key for authentication system PITreader, permissions freely configurable<br>Colour: blue<br>Material: plastic  | 402260BL  |
| PITreader key ye g gn | Generic transponder key for authentication system PITreader, permissions freely configurable<br>Colour: green<br>Material: plastic | 402260GN  |
| PITreader key ye g rd | Generic transponder key for authentication system PITreader, permissions freely configurable<br>Colour: red<br>Material: plastic   | 402260RD  |

| Product type               | Features   | Order no. |
|----------------------------|--|-----------|
| PITreader key ye g wt      | Generic transponder key for authentication system PITreader, permissions freely configurable<br>Colour: white<br>Material: plastic                   | 402260WT  |
| PITreader key ye g ye      | Generic transponder key for authentication system PITreader, permissions freely configurable<br>Colour: light yellow<br>Material: plastic            | 402260YE  |
| PITreader key ye 1         | Transponder key for authentication system PITreader, permission for operating mode 1<br>Colour: yellow<br>Material: plastic                          | 402261    |
| PITreader key ye 2         | Transponder key for authentication system PITreader, permission for operating mode 1 and 2<br>Colour: yellow<br>Material: plastic                    | 402262    |
| PITreader key ye 3         | Transponder key for authentication system PITreader, permission for operating mode 1, 2 and 3<br>Colour: yellow<br>Material: plastic                 | 402263    |
| PITreader key ye 4         | Transponder key for authentication system PITreader, permission for operating mode 1, 2, 3 and 4<br>Colour: yellow<br>Material: plastic              | 402264    |
| PITreader key ye 5         | Transponder key for authentication system PITreader, permission for operating mode 1, 2, 3, 4 and 5<br>Colour: yellow<br>Material: plastic           | 402265    |
| PITreader key ye 5 service | Transponder key for authentication system PITreader, permission for operating mode 1, 2, 3, 4 and 5 (Service)<br>Colour: yellow<br>Material: plastic | 402269    |

#### 14.4 Transponder cards

| Product type        | Features  | Order no. |
|---------------------|---|-----------|
| PITreader card ye g | Transponder card for authentication system PITreader Card, permissions freely configurable<br>Colour: yellow<br>Material: plastic       | 402330    |
| PITreader card ye 1 | Transponder card for authentication system PITreader Card, permission for operating mode 1<br>Colour: yellow<br>Material: plastic       | 402331    |
| PITreader card ye 2 | Transponder card for authentication system PITreader Card, permission for operating mode 1 and 2<br>Colour: yellow<br>Material: plastic | 402332    |



| Product type                | Features   | Order no. |
|-----------------------------|--|-----------|
| PITreader card ye 3         | Transponder card for authentication system PITreader Card, permission for operating mode 1, 2 and 3<br>Colour: yellow<br>Material: plastic                 | 402333    |
| PITreader card ye 4         | Transponder card for authentication system PITreader Card, permission for operating mode 1, 2, 3 and 4<br>Colour: yellow<br>Material: plastic              | 402334    |
| PITreader card ye 5         | Transponder card for authentication system PITreader Card, permission for operating mode 1, 2, 3, 4 and 5<br>Colour: yellow<br>Material: plastic           | 402335    |
| PITreader card ye 5 service | Transponder card for authentication system PITreader Card, permission for operating mode 1, 2, 3, 4 and 5 (Service)<br>Colour: yellow<br>Material: plastic | 402339    |

## 14.5 Transponder sticker

| Product type                   | Features  | Order no. |
|--------------------------------|---|-----------|
| PITreader sticker ye g         | Transponder sticker for authentication system PITreader Card, permissions freely configurable<br>Colour: yellow<br>Material: plastic                          | 402340    |
| PITreader sticker ye 1         | Transponder sticker for authentication system PITreader Card, permission for operating mode 1<br>Colour: yellow<br>Material: plastic                          | 402341    |
| PITreader sticker ye 2         | Transponder sticker for authentication system PITreader Card, permission for operating mode 1 and 2<br>Colour: yellow<br>Material: plastic                    | 402342    |
| PITreader sticker ye 3         | Transponder sticker for authentication system PITreader Card, permission for operating mode 1, 2 and 3<br>Colour: yellow<br>Material: plastic                 | 402343    |
| PITreader sticker ye 4         | Transponder sticker for authentication system PITreader Card, permission for operating mode 1, 2, 3 and 4<br>Colour: yellow<br>Material: plastic              | 402344    |
| PITreader sticker ye 5         | Transponder sticker for authentication system PITreader Card, permission for operating mode 1, 2, 3, 4 and 5<br>Colour: yellow<br>Material: plastic           | 402345    |
| PITreader sticker ye 5 service | Transponder sticker for authentication system PITreader Card, permission for operating mode 1, 2, 3, 4 and 5 (Service)<br>Colour: yellow<br>Material: plastic | 402349    |

## 14.6 Accessories

| Product type  | Features                                  | Order no. |
|---------------|---|-----------|
| PIT es wrench | Installation wrench for PIT es pushbutton | 400222    |

preliminary

## 15 **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](http://www.pilz.com/downloads).

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

preliminary

## 16 UKCA-Declaration of Conformity

This product(s) complies with following UK legislation: Radio Equipment Regulations 2017

The complete UKCA Declaration of Conformity is available on the Internet at [www.pilz.com/downloads](http://www.pilz.com/downloads).

Representative: Pilz Automation Technology, Pilz House, Little Colliers Field,  
Corby, Northamptonshire, NN18 8TJ United Kingdom, eMail: [mail@pilz.co.uk](mailto:mail@pilz.co.uk)

preliminary

