



► PITreader

PITreader Firmware Version 02.04.xx

PILZ
THE SPIRIT OF SAFETY

Operating Manual-1004806-EN-18
- Control and signal devices



This document is a translation of 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.

CECE®, CHRE®, CMSE®, INDUSTRIAL PI®, Leansafe®, MYZEL®, PAS4000®, PAS-cal®, PASconfig®, Pilz®, PIT®, PMCprimo®, PMCprotego®, PM Ctendo®, PMD®, PMI®, PNOZ®, Primo®, PSEN®, PSS®, PVIS®, SafetyBUS p®, SafetyEYE®, SafetyNET p®, THE SPIRIT OF SAFETY® are registered and protected trademarks of Pilz GmbH & Co. KG in some countries.



SD means Secure Digital

1	Introduction	8
1.1	Validity of documentation	8
1.2	Using the documentation	8
1.3	Terminology	8
1.4	Definition of symbols	9
2	Safety and Security	10
2.1	Intended use	10
2.1.1	Product	10
2.1.2	Application ranges	10
2.1.3	Application conditions	10
2.1.4	Use of qualified personnel	10
2.1.5	Prerequisites for operation	10
2.1.6	Specific measures for intended use	11
2.1.7	Improper use	11
2.1.8	Third-party manufacturer licence information	11
2.2	Safety regulations	11
2.2.1	Additional documents that apply	11
2.2.2	Safety assessment	11
2.2.3	Warranty and liability	12
2.3	General security information	12
2.4	Security measures	12
2.4.1	Implemented security measures	12
2.4.2	Required external security measures	13
2.4.2.1	Network topology	13
2.4.2.2	Physical manipulation	13
2.4.2.3	Password	13
2.4.2.4	Token	13
2.4.2.5	Transponder	13
2.4.2.6	Network, firewall, virus scanner	14
2.4.2.7	Data, logs, configurations	14
2.4.2.8	Synchronisation	14
2.4.2.9	Updates	14
2.4.2.10	Coding	14
2.4.2.11	Disposal	14
3	Overview	15
3.1	Device features	15
3.2	System overviews with PITreader	16
3.2.1	Access system	16
3.2.2	Systems for safety-related operating mode selection	16
3.2.3	Access system for maintenance safeguarding system Key-in-pocket	16
3.3	Unit views	17
3.3.1	Unit view PITreader Key	17
3.3.2	Unit view PITreader Card	18
3.3.3	Device view PIT gb with PITreader	18
3.3.4	View PITreader transponder key	19
3.3.5	View PITreader transponder card	19
3.3.6	View PITreader transponder sticker	20

4	Function description	21
4.1	Authentication procedure	21
4.2	Authentication modes	22
4.2.1	"Transponder data" authentication mode	22
4.2.1.1	Device groups	22
4.2.2	"External" authentication mode	23
4.2.3	"Permission list" authentication mode	26
4.2.4	"Fixed permission" authentication mode	26
4.3	Authentication types	26
4.3.1	"Basic" authentication type	26
4.3.2	"Single authentication" authentication type	26
4.3.3	"2-person rule" authentication type	27
4.4	Two-factor authentication	29
4.4.1	PIN requirement on the PITreader	29
4.4.2	PIN as a second factor	29
4.4.3	Limiting the number of PIN entry attempts	30
4.4.4	Set and provide a PIN	30
4.5	Transponders	31
4.5.1	Transponders from Pilz	31
4.5.1.1	Permission on a transponder	31
4.5.1.2	Data areas of a transponder	33
4.5.1.3	Evaluation of a transponder's serial number	34
4.5.2	Transponders from third-party manufacturers with selected ISO/IEC standards (without MI-FARE DESFire applications)	34
4.5.3	Transponders from third-party manufacturers with MIFARE DESFire applications	36
4.5.4	Transponder's security ID (SID)	36
4.5.5	Transponder recognition with one PITreader Card	37
4.6	User data	39
4.6.1	System parameters	40
4.7	Coding	41
4.7.1	Basic coding	42
4.7.2	OEM coding	43
4.8	Block list	44
4.9	Real-time clock and operating hours counter	44
4.10	Synchronisation with external data	44
4.11	Modbus/TCP	45
4.11.1	LED control	45
4.11.2	Function codes (Client connections)	46
4.11.3	Modbus/TCP data areas	47
4.11.3.1	Data transfer limits	50
4.12	HTTP(S) connection	51
4.13	24 V I/O port	51
4.14	Connect the base unit to a safe evaluation unit	51
5	Installation and removal	52
5.1	General guidelines for installation and removal	52
5.2	Installation and removal of a PITreader Key	53
5.2.1	Installation of PITreader Key	53

5.2.2	Removal of PITreader Key	56
5.3	Installation and removal of a PITreader Card	57
5.3.1	Installation of PITreader Card	57
5.3.2	Removal of PITreader Card	60
5.3.3	Installation PITreader card holder	60
5.3.4	Attach PITreader transponder sticker	61
5.3.4.1	Application without PITreader card holder	61
5.3.4.2	Application with PITreader card holder	62
5.4	Installation and removal of a PIT gb with PITreader	63
5.5	Dimensions	64
5.5.1	Dimensions of PITreader Key	64
5.5.2	Dimensions of PITreader Card	64
5.5.3	Dimensions of PIT gb with PITreader	64
5.5.4	Dimensions of PITreader transponder key	65
5.5.5	Dimensions of PITreader transponder card	65
5.5.6	Dimensions of PITreader transponder sticker	66
5.5.7	Dimensions PITreader card holder	66
6	Wiring	67
6.1	Base unit without safe evaluation unit (standalone)	67
6.2	Base unit with safe evaluation unit	67
7	Configuration	68
7.1	Web application	68
7.2	Network discovery with Multicast DNS (mDNS)	68
7.3	Network configuration via Multicast protocol	69
7.4	Connect to PITreader	69
7.5	Device user	70
7.6	Manage certificates	71
7.6.1	Managing certificates	71
7.6.2	Incorporate certificate into a public key infrastructure (PKI)	72
7.7	Configure authentication mode	72
7.8	Configure authentication type	73
7.9	Configure two-factor authentication	73
7.9.1	Enable two-factor authentication	73
7.9.2	Write PIN to transponder	73
7.9.3	Enter your PIN for authentication	73
7.10	Location description	73
7.11	Data logging with personal data	74
7.12	Audit trail messages deleted automatically	74
7.13	Set device group	74
7.14	Set basic coding	74
7.15	Set OEM coding	74
7.16	Configure third-party transponder with ISO/IEC standard as RFID protocol	75
7.17	Configure third-party transponders with MIFARE DESFire application	76
7.17.1	Select RFID protocol	77
7.17.2	Store cryptographic keys	78
7.18	Initialise third-party transponder with MIFARE DESFire application	78

7.18.1	Initialise third-party transponder yourself	78
7.18.1.1	The third-party transponder does not require prior authentication with the PICC Master Key in order to create new applications.	79
7.18.1.2	The third-party transponder requires prior authentication with the PICC Master Key in order to create new applications.....	80
7.18.2	Initialise third-party transponder through a third party.....	80
7.18.2.1	Using your own Application Master Keys and Application User Keys.....	80
7.18.2.2	Using Transport Keys.....	81
7.19	Write/program transponder	81
7.19.1	Program permissions	81
7.19.2	Configure the validity of the transponder	82
7.19.3	Teach in transponder to basic coding	82
7.19.4	Teach in transponder to OEM coding	82
7.19.5	Limit transponder to identically coded PITreaders	84
7.19.6	Edit user data values.....	84
7.19.7	Delete user data on transponders.....	84
7.20	Permission list.....	84
7.21	Use block list.....	85
7.22	Configure user data.....	85
7.23	Configuration for PIT Windows Logon	86
7.24	Configure synchronisation monitoring.....	86
7.25	API Clients	87
7.26	Save and restore configuration	87
7.27	Reset to default settings.....	88
7.27.1	Reset via short circuit at the terminals TxD/RxD.....	88
7.27.2	Reset in the web application	88
8	Firmware update	90
9	Commissioning, operation	91
9.1	Position transponder	91
9.1.1	PITreader Key	91
9.1.2	PITreader Card	91
9.1.3	PITreader card holder	92
9.1.3.1	PITreader transponder key	92
9.1.3.2	PITreader transponder card	92
9.1.3.3	PITreader transponder sticker.....	93
9.2	LED indicator.....	93
9.3	Personal data	96
9.3.1	PITreader	96
9.3.2	Transponder.....	96
9.4	Diagnostics.....	96
9.4.1	Statistics.....	97
10	Maintenance and testing	99
11	Decommissioning	100
11.1	Disposal	100

12	Technical details	101
13	Safety characteristic data	104
14	Supplementary data	105
14.1	Radio approvals PITreader Key	105
14.2	Radio approvals PITreader Card	105
14.3	Network data	106
14.4	Overview of permissions	106
15	Order reference	109
15.1	Authentication system PITreader Key	109
15.2	Authentication system PITreader Card	109
15.3	Transponder key	109
15.4	Transponder cards	110
15.5	Transponder sticker	111
15.6	Accessories	112
16	EC declaration of conformity	113
17	UKCA-Declaration of Conformity	114

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

The term "PITreader" includes all RFID authentication systems from PILZ GmbH & Co. KG on which authentication is via a transponder.

The following can be used as transponders, for example:

- ▶ PITreader transponder key
- ▶ PITreader transponder cards
- ▶ PITreader transponder sticker

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 Key

The term "PITreader Key" includes all PITreader product types on which only a PITreader transponder key can be used for authentication. The PITreader transponder key is inserted into the read head for this purpose.

One product type is the PITreader S base unit, for example.

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

PITreader Card

The term "PITreader Card" includes all PITreader product types on which the following transponders can be used for authentication:

- ▶ PITreader transponder card
- ▶ PITreader transponder sticker
- ▶ PITreader transponder key

The PITreader transponder is held in front of the read head for this purpose.

One product type is the PITreader S card unit, for example.

The term "PITreader Card" 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 PITgatebox with PITreader. There are two product types available: PIT gb with PITreader Key and PIT gb with PITreader Card.

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

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.

2 Safety and Security

2.1 Intended use

2.1.1 Product

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

2.1.2 Application ranges

The product is designed for use in an industrial environment.

2.1.3 Application conditions



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.

2.1.4 Use of qualified personnel

Product installation, assembly, programming, commissioning, operation, decommissioning and maintenance may only be carried out by competent persons.

A competent person is a qualified and knowledgeable person who, because of their training, experience and current professional activity, has the specialist knowledge required.

In order to inspect, assess and handle products, devices, systems, plant and machinery, this person must be familiar with the state of the art and the applicable national, European and international laws, regulations, 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 section on "Safety and Security" in this description and
- ▶ Have a good knowledge of the generic and specialist standards applicable to the specific application.

2.1.5 Prerequisites for operation

This document is intended for instruction. Only install and commission the product if you have read and understood this document.

Only approved accessories and approved consumables may be used.

2.1.6 Specific measures for intended use

No specific measures are required for intended use.

2.1.7 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 document.
- ▶ Use of the product outside the technical details (see [Technical Details](#)  101)).

2.1.8 Third-party manufacturer licence information

The product contains open source software, whose terms of use could further limit the product's application area. It is essential that you observe the third-party manufacturer licence information.

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

2.2 Safety regulations

2.2.1 Additional documents that apply

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

- ▶ Operating manual PITreader REST API (1005365)
- ▶ Operating manual PITreader OPC Server UA (1005480)
- ▶ When using a PIT gb with PITreader:
Operating manual PIT gb with PITreader (1005249)
- ▶ When using a safe evaluation unit PIT m4SEU:
Operating manual PIT m4SEU (1004648)
- ▶ For information on the calculation of safety-related characteristic data:
 - System description PITmode flex (1005276)
 - System description PITmode flex visu (1005364)
 - System description for the maintenance safeguarding system Key-in-pocket (1006613)

2.2.2 Safety assessment

Before using the product, a risk assessment is required in accordance with the Machinery Regulation.

Connecting additional units may result in further risks. Take the necessary measures to protect against corruption.

The product as an individual component fulfils the functional safety requirements in accordance with EN/IEC 61508, EN ISO 13849-1/2 and EN IEC 62061. However, this does not guarantee the functional safety of the overall plant/machine. To achieve the relevant safety level of the overall plant/machine's required safety functions, each safety function needs to be considered separately.

It is the responsibility of the user/operator to carry out a risk assessment for their application, in which they consider the impact of assumed errors in the wiring and take appropriate measures to control or avoid these errors.

2.2.3 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 operating 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.).

2.3 General security information

To protect 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.

Carry out a risk assessment in accordance with VDI/VDE 2182 or IEC 62443-3-2 and plan the security measures with care.

If you have any questions about implementation, please contact technical support at support@pilz.com.

You can reach the Pilz Product Security Incident Response Team (PSIRT) at <https://www.pilz.com/psirt>.

With regard to a Pilz product, this is where you can:

- ▶ Report security vulnerabilities and security incidents
- ▶ Ask questions about security vulnerabilities and security incidents
- ▶ View Security Advisories

2.4 Security measures

2.4.1 Implemented security measures

- ▶ The web application is protected against unauthorised access by a password prompt.
- ▶ If a password is changed, you will be prompted to enter the old password for authentication.
- ▶ The password is saved in an encrypted format.
- ▶ 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.

2.4.2 Required external security measures

2.4.2.1 Network topology

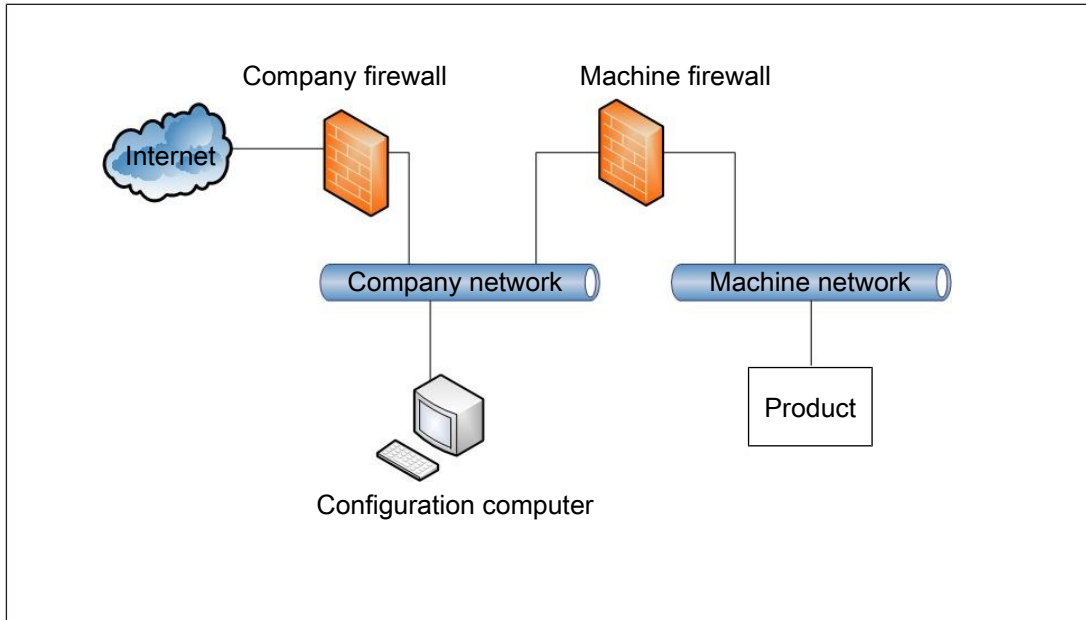


Fig.: Example network topology

2.4.2.2 Physical manipulation

- ▶ The product is not protected from physical manipulation. If protection is inadequate, safety-critical functions may be compromised. The product should therefore be installed in a lockable control cabinet or in a closed 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.

2.4.2.3 Password

- ▶ If necessary, protect the configuration computer and the product from unauthorised use by assigning passwords and taking other appropriate measures.
Ensure that the user logged in to this configuration computer does not have administrator rights.
- ▶ Only use strong passwords and handle them carefully. Be guided by generally accepted guidelines such as NIST 800-63B for example.
- ▶ 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.

2.4.2.4 Token

- ▶ An API token should be handled with the same care as a password.

2.4.2.5 Transponder

- ▶ Keep transponders in a safe place and protect them from unauthorised access.
Inform users of the security risks involved in sharing transponders.

2.4.2.6 Network, firewall, virus scanner

- ▶ The configuration computer that accesses the product should be protected from attacks using a firewall or other appropriate measures.

Use a virus scanner on this configuration computer and keep it up to date.

- ▶ Limit Modbus/TCP connections to the internal machine network. Secure the connection against external networks.
- ▶ Take the [network data](#)  106 into account when carrying out the risk analysis and when defining security measures.
- ▶ Use a firewall or other appropriate measures to protect the product from unauthorised data exchange over the network.

Only allow the data exchange necessary for the application.

Prevent any unnecessary data exchange, e.g. by using a firewall.

2.4.2.7 Data, logs, configurations

- ▶ Log data may contain personal data.

Only save exported logs on storage media that are adequately secure.

- ▶ 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.

2.4.2.8 Synchronisation

- ▶ Synchronising the real-time clock in the product via SNTP does not provide any security mechanisms; for example, spoofing of the configured SNTP Server.

Secure the real-time clock at application level by configuring an appropriate firewall or by using a local time server within the machine network.

2.4.2.9 Updates

- ▶ Install any firmware updates from Pilz as soon as possible.

2.4.2.10 Coding

- ▶ When the product is reset to its factory settings, the coding in the product is also reset. As a result, the product will once again accept transponders that are either uncoded or coded differently.

To ensure correct function, monitor the coding check sum in a higher-level controller, HMI or evaluation unit.

2.4.2.11 Disposal

- ▶ Before disposal, the product must be safely decommissioned. To do this, all the data must be deleted from the product.

- Set the configuration back to its default settings or delete the configuration.
- Switch off the product.

3 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, Product ID 402250) for safe operating mode selection (only with PITreader Key and PITreader Card)

3.1 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

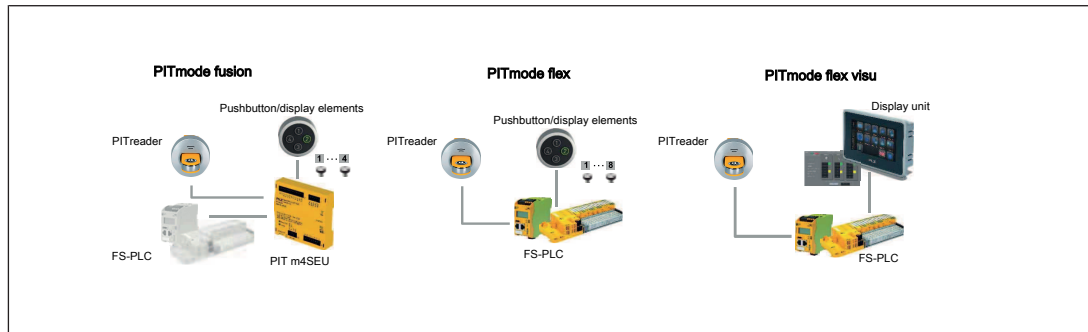
Device feature		PITreader Key	PITreader Card	PIT gb with PITreader Key	PIT gb with PITreader Card
Transponder					
	Transponder key	◆	◆	◆	◆
	Transponder cards	---	◆	---	◆
	Transponder sticker	---	◆	---	◆
PITreader card holder		---	◆	---	◆
Integrated OPC UA Server		PITreader S base unit	PITreader S card unit	PIT gb RLLE y up ETH PIT gb RLLE y down ETH	PIT gb QLLE y up ETH PIT gb QLLE y down ETH
Transponders from third-party manufacturers with MIFARE DES-Fire applications		---		---	
Interface for connecting a PITm4SEU		◆	◆	---	---
Base unit for mounting cutout D22 (diameter 22.3 mm) with anti-rotation device		◆	◆	---	---

3.2 System overviews with PITreader

3.2.1 Access system

The PITreader can be used for authentication on any controller/PLC or HMI.

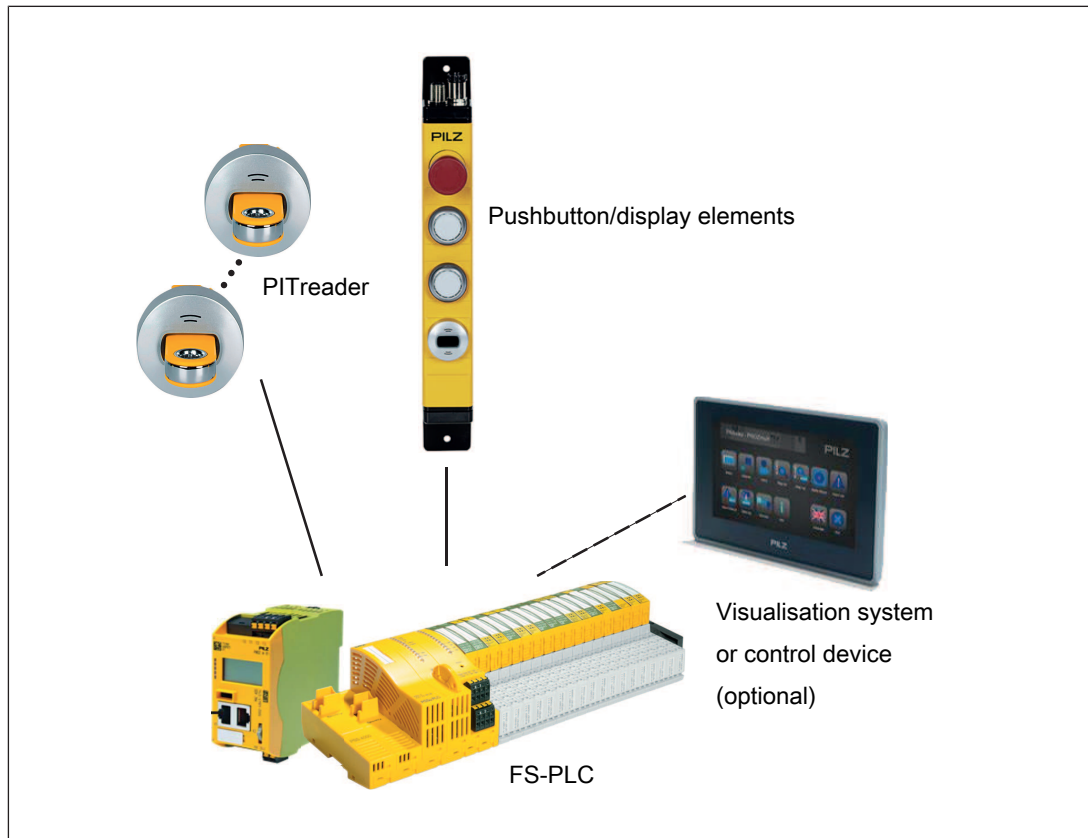
3.2.2 Systems for safety-related operating mode selection



You can find further information for

- ▶ PITmode fusion in the operating manual PIT m4SEU (1004648).
- ▶ PITmode flex in the system description PITmode flex (1005276).
- ▶ PITmode flex visu in the system description PITmode flex visu (1005364).

3.2.3 Access system for maintenance safeguarding system Key-in-pocket



Further information is available in the system description for the maintenance safeguarding system Key-in-pocket (1006613).

3.3 Unit views

3.3.1 Unit view PITreader Key

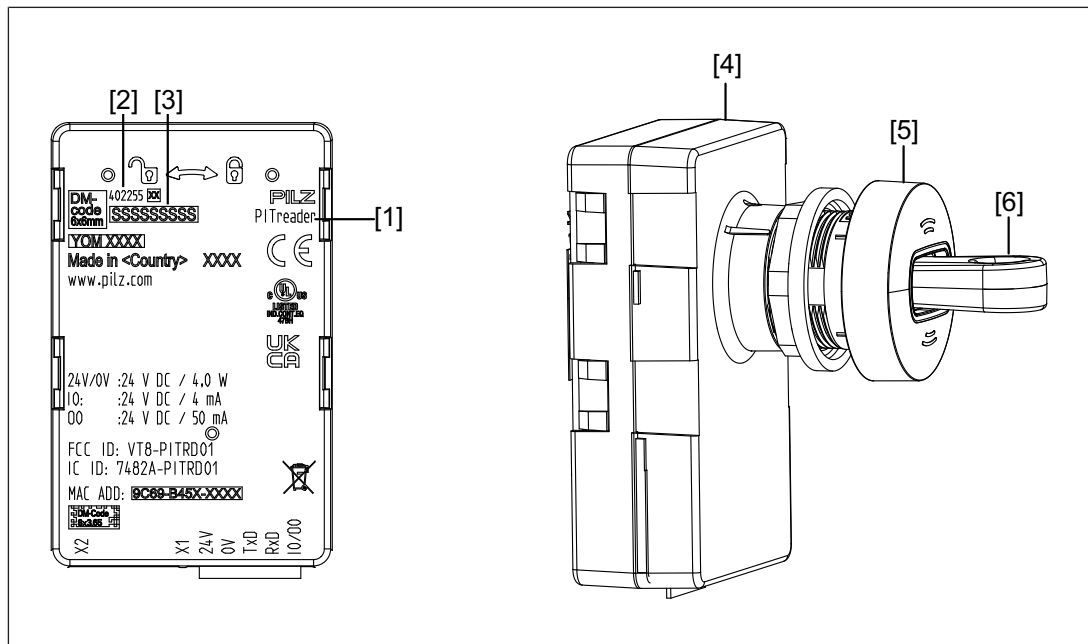


Fig.: Device view of PITreader Key using the PITreader base unit as an example

Legend

- X1 Voltage supply, 24 V input/output and connection of a safe evaluation unit (PIT m4SEU)
- X2 Ethernet interface
- [1] Device name
- [2] Product ID
- [3] Serial number
- [4] Base unit (Product ID 402255 or 402256), including spring-loaded terminal (402307)
- [5] Read head PITreader key Adapter h (Product ID 402308)
(not supplied with the base unit, see also [Order reference \[109\]](#))
- [6] Transponder key (see also [Transponders \[31\]](#) and [Order reference \[109\]](#))

3.3.2 Unit view PITreader Card

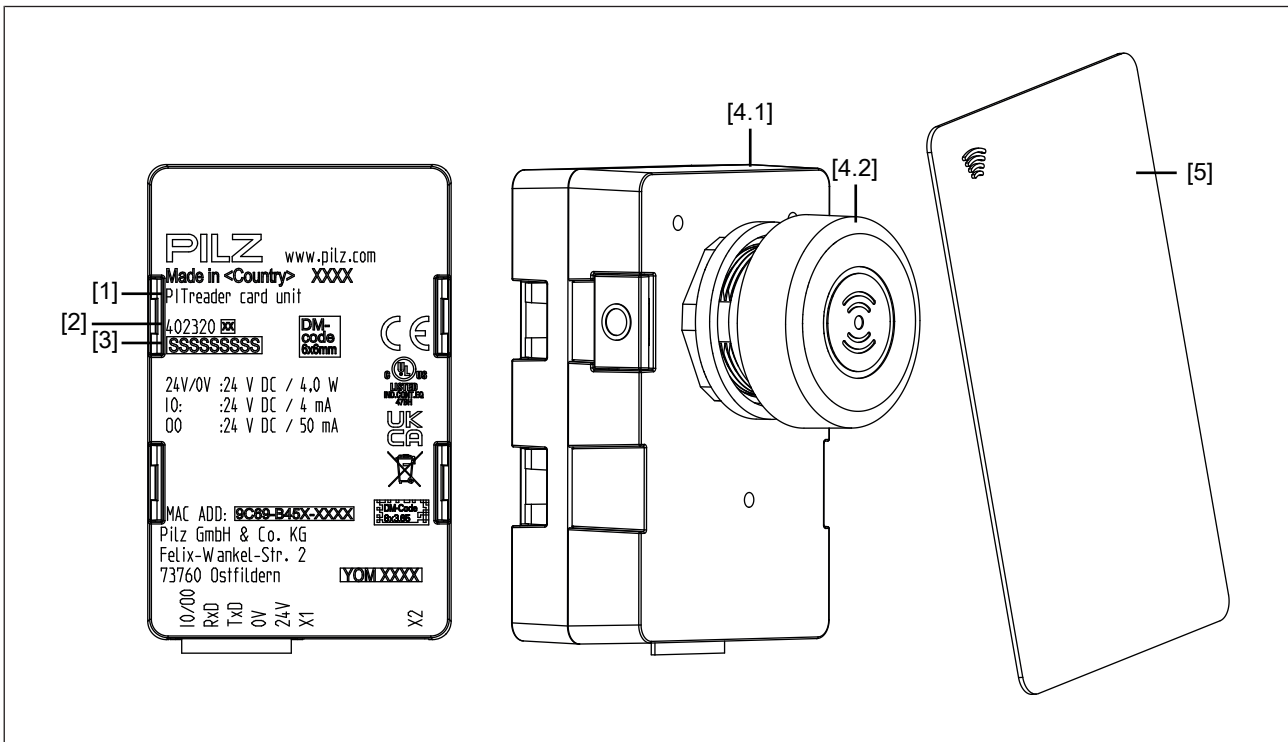


Fig.: Device view of PITreader card with transponder card using the PITreader card unit as an example

Legend

- X1 Voltage supply, 24 V input/output and connection of a safe evaluation unit (PIT m4SEU)
- X2 Ethernet interface
- [1] Device name
- [2] Product ID
- [3] Serial number
- [4.1] Base unit (Product ID 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 \[109\]](#))
- [5] Transponder (in this case transponder card, for example) (see also [Transponders \[31\]](#) and [Order reference \[109\]](#))

3.3.3 Device view PIT gb with PITreader

You will find the necessary information in the operating manual PIT gb with PITreader.

3.3.4 View PITreader transponder key

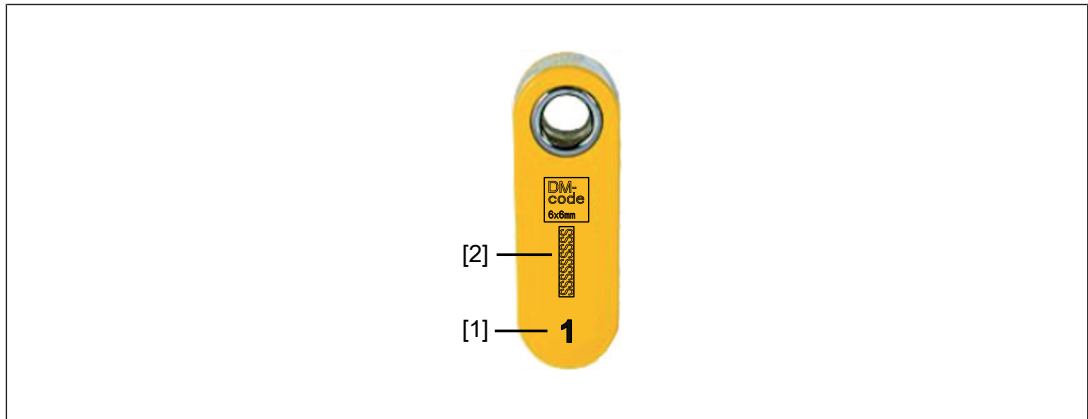


Fig.: Key view, using PITreader key ye 1 as an example

Legend

- [1] Permission
(see also [Permission on a transponder](#) [31] and [Order reference](#) [109])
- [2] Serial number

3.3.5 View PITreader transponder card

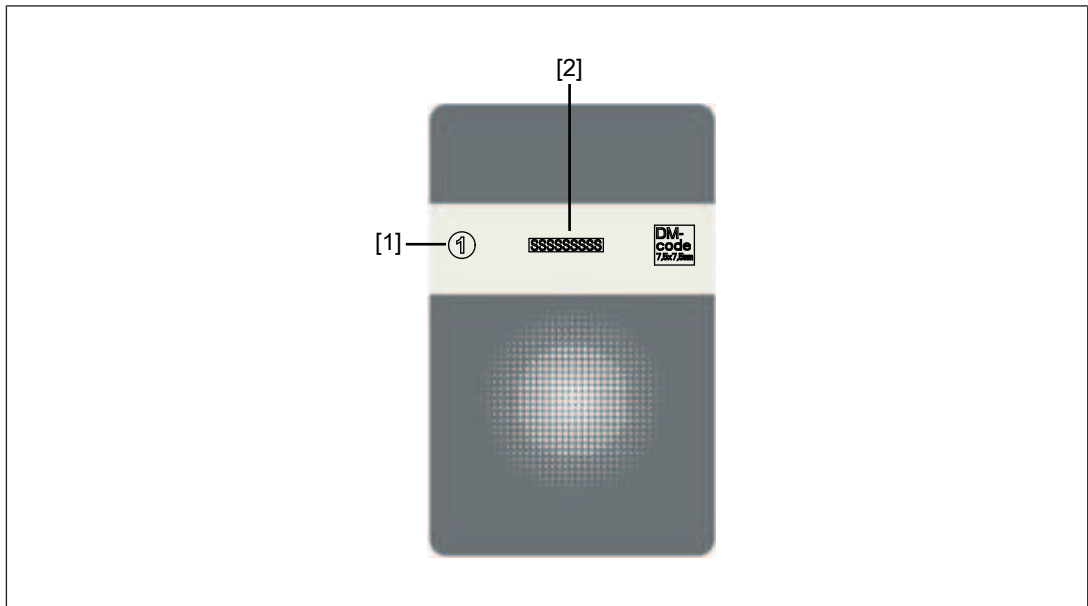


Fig.: Card view, using PITreader card ye 1 as an example

Legend

- [1] Permission
(see also [Permission on a transponder](#) [31] and [Order reference](#) [109])
- [2] Serial number

3.3.6 View PITreader transponder sticker

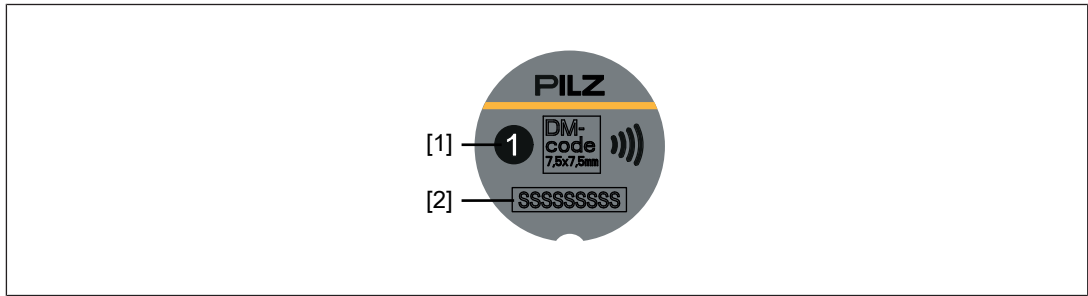


Fig.: Sticker view, using PITreader sticker ye 1 as an example

Legend

- [1] Permission
(see also [Permission on a transponder](#) [📖 31] and [Order reference](#) [📖 109])
- [2] Serial number

4 Function description

4.1 Authentication procedure

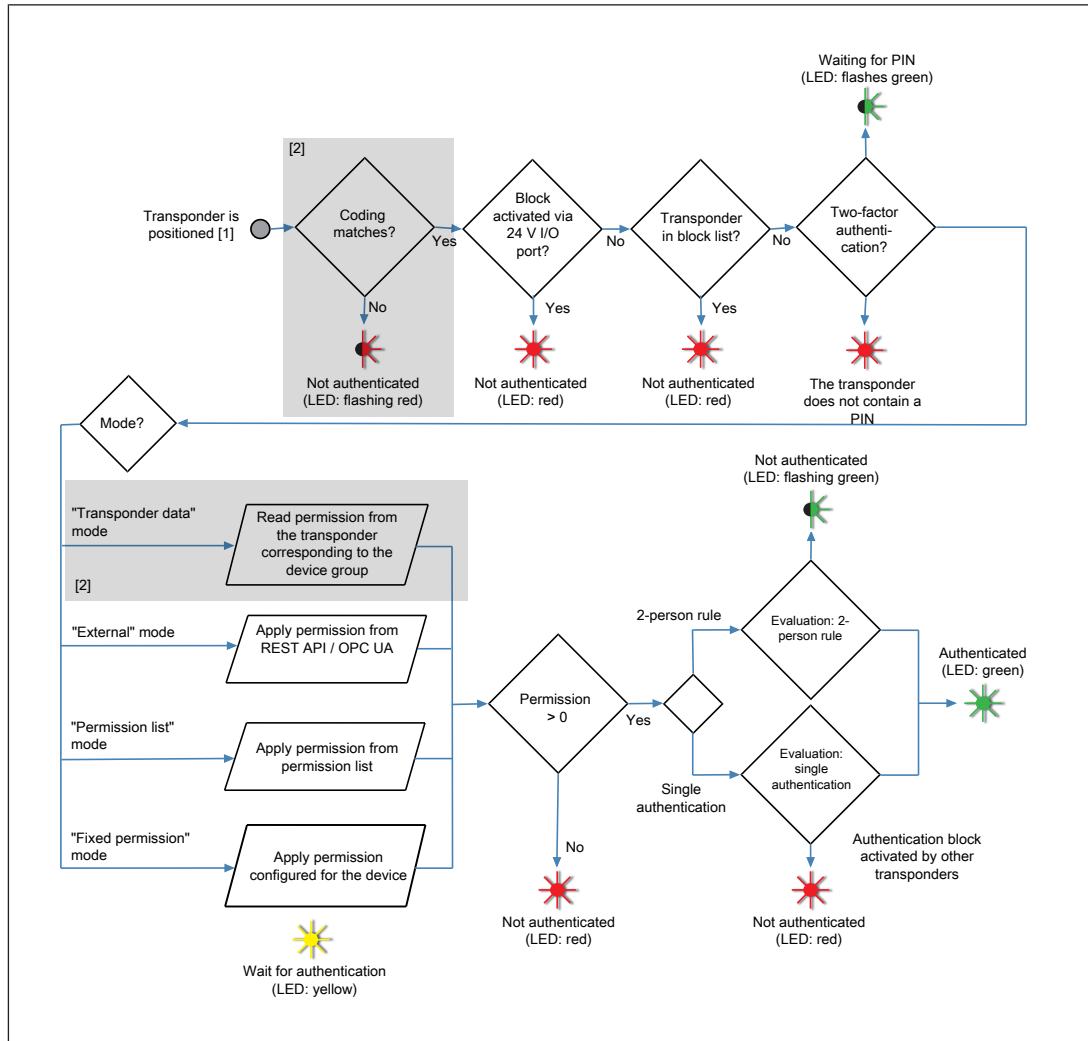


Fig.: Authentication procedure

[1]

Meaning:

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

[2]

The grey marked areas are omitted when the option **Support third-party transponder** is activated and an ISO/IEC standard is selected in the **RFID protocol** dropdown menu.

4.2 Authentication modes

The PITreader supports the following authentication modes:

- ▶ "Transponder data" authentication mode [ 22]
- ▶ "External" authentication mode [ 23]
- ▶ "Permission list" authentication mode [ 26]
- ▶ "Fixed permission" authentication mode [ 26]

"Transponder data" authentication mode is set upon delivery. The authentication mode can be changed in the web application; it is possible to set whether the authentication mode may be overwritten via the REST API (see also [Configure authentication mode](#) [ 72]).

4.2.1 "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](#) [ 44] if they are lost.

On a transponder from Pilz it is possible to store the period for which the transponder is valid. If required, the validity of the transponder can be evaluated in "Transponder data" authentication mode. If the transponder is invalid, the permission "0" is issued, irrespective of the device group. In other words, the transponder is not authenticated.

In order for the validity to be evaluated, the option **Evaluate validity date** must be activated for the PITreader in the web application under **Configuration -> Settings -> Advanced functions**.

4.2.1.1 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; a user then has the same permission on all turning machines, for example (see also [Set device group](#) [ 74]).

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](#) [106].

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](#) [39].

4.2.2

"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)

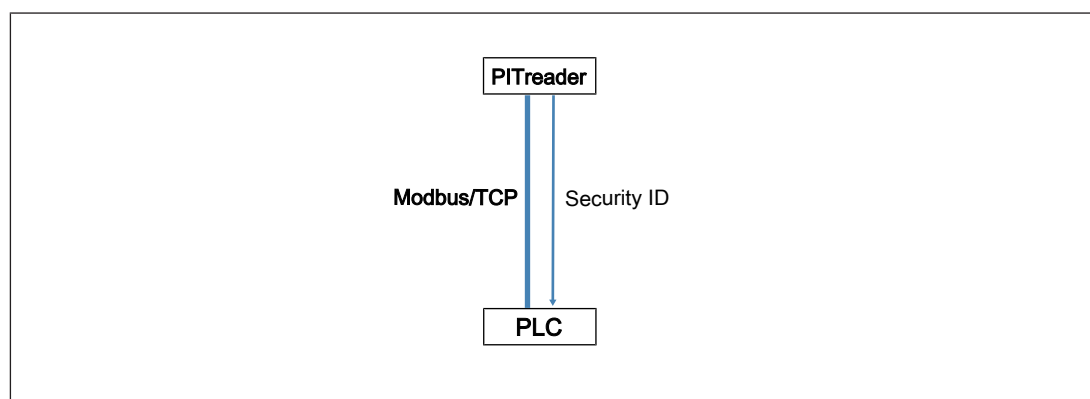


Fig.: External authentication (Modbus/TCP)

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)

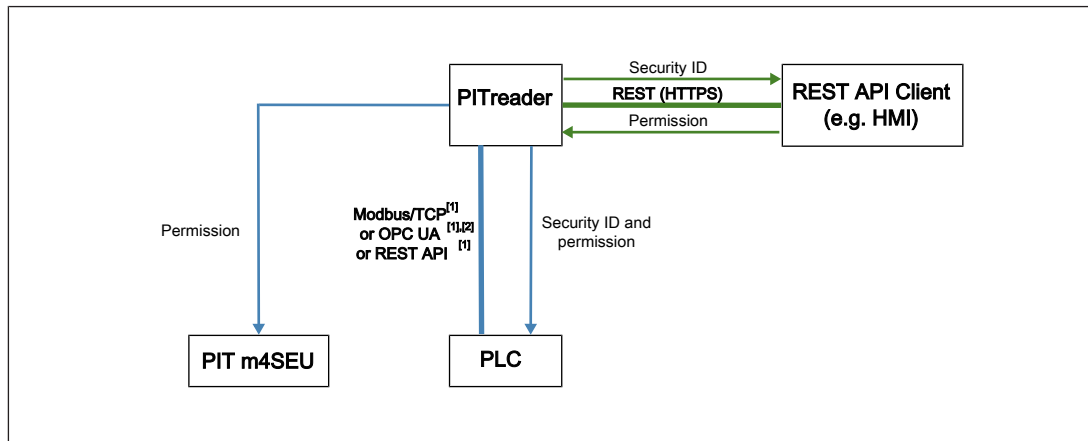


Fig.: External authentication (REST API)

[1] Select a protocol that is supported by the PLC.

[2] Only certain PITreader types are supported.

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 takes place 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)

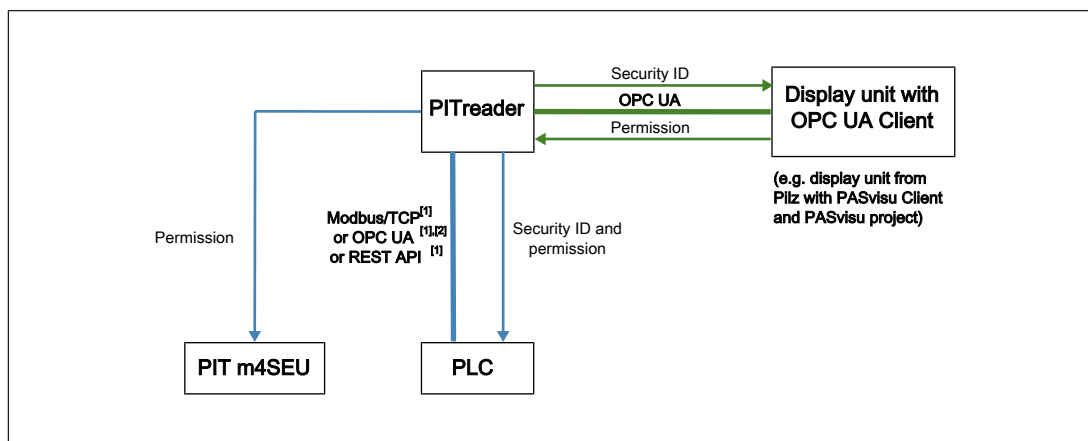


Fig.: External authentication (OPC UA)

[1] Select a protocol that is supported by the PLC.

[2] Only certain PITreader types are supported.

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.

4.2.3 "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](#)  84).

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).

4.2.4 "Fixed permission" authentication mode

In "Fixed permission" authentication mode, each transponder is authenticated and is given a pre-configured permission, with the exception of transponders in the block list. The permission is the same for all transponders.

This authentication mode is particularly suitable for third-party transponders for which an ISO/IEC standard has been selected in the RFID protocol dropdown menu. The PITreader then accepts each transponder and provides the UID and Security ID of the authenticated transponder.

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.

4.3 Authentication types

The PITreader supports the following authentication types:

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

4.3.1 "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](#)  22).

4.3.2 "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.

4.3.3 "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). 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). 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

4.4 Two-factor authentication

Two-factor authentication enhances security when logging into the PITreader via a combination of two factors:

- ▶ Transponder (ownership)
- ▶ PIN (knowledge)

Authentication is only successful if both factors are valid.

Two-factor authentication protects against the illicit sharing, theft and unauthorised use of transponders.

A stolen transponder cannot be used without knowing the correct PIN.

This function does not protect the transponder data from being read or manipulated.

Coding can be used to protect the transponder data.

4.4.1 PIN requirement on the PITreader

The PIN requirement is a property of the PITreader, not the transponder. For each station, therefore, you can specify individually whether a PIN is required. The PIN is only requested locally on the respective PITreader.

Users have the following options:

- ▶ Two-factor authentication not enabled; transponder with or without a PIN

No PIN request.

Authentication is immediate.

- ▶ Two-factor authentication enabled, transponder without a PIN

Authentication is rejected.

A red LED lights up on the PITreader.

- ▶ Two-factor authentication enabled, transponder with PIN

Authentication requires a transponder and the correct PIN.

- ▶ Two-factor authentication enabled, PIN too short

Authentication is rejected.

Example:

The transponder PIN is 4 digits long, but the minimum length set on the PITreader is 6 digits.

4.4.2 PIN as a second factor

A PIN consists of 4 to 6 digits. Only the digits 0 to 9 are permitted.

A minimum PIN length can be configured for each PITreader, ranging from 4 to 6 digits.

If the PIN stored on the transponder is shorter than the configured minimum length, authentication will be rejected.

A PIN can be programmed on to a transponder at any time. This applies regardless of whether two-factor authentication is enabled.

4.4.3 Limiting the number of PIN entry attempts

A maximum of three attempts to enter the PIN are permitted. After three incorrect attempts, the PIN entry will be blocked. The block will be lifted when the transponder is removed and presented again.

The number of attempts is independent of the interface:

- ▶ Web application
- ▶ REST API
- ▶ OPC Server UA

4.4.4 Set and provide a PIN

The PIN can be written and provided via the following interfaces:

- ▶ Web application
- ▶ REST API
- ▶ OPC Server UA

Further information on the REST API and OPC Server UA can be found in the operating manuals for the PITreader REST API (1005365) and PITreader OPC Server UA (1005480).

4.5 Transponders

4.5.1 Transponders from Pilz

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

Transponder application options

Transponder	PITreader Key PIT gb with PITreader Key	PITreader Card PIT gb with PITreader Card
Transponder key	◆	◆
Transponder cards	---	◆
Transponder sticker [1]	---	◆

[1]

Note: A transponder sticker is attached to an existing card (see [Attach PITreader transponder sticker](#) [ 61]).

4.5.1.1 Permission on a transponder

Transponder keys

The transponder keys are available in the following types, with the following permissions (see also [Order reference](#) [ 109]):

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

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 device groups G0 ... G31.

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](#) [ 109]):

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

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 G0 ... G31.

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](#)  109]):

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

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 device groups G0 ... G31.

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

4.5.1.2 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 the transponder (start/end date)

The data area cannot be locked.

► Data area for free (customised) user data

The data area cannot be locked.

Example

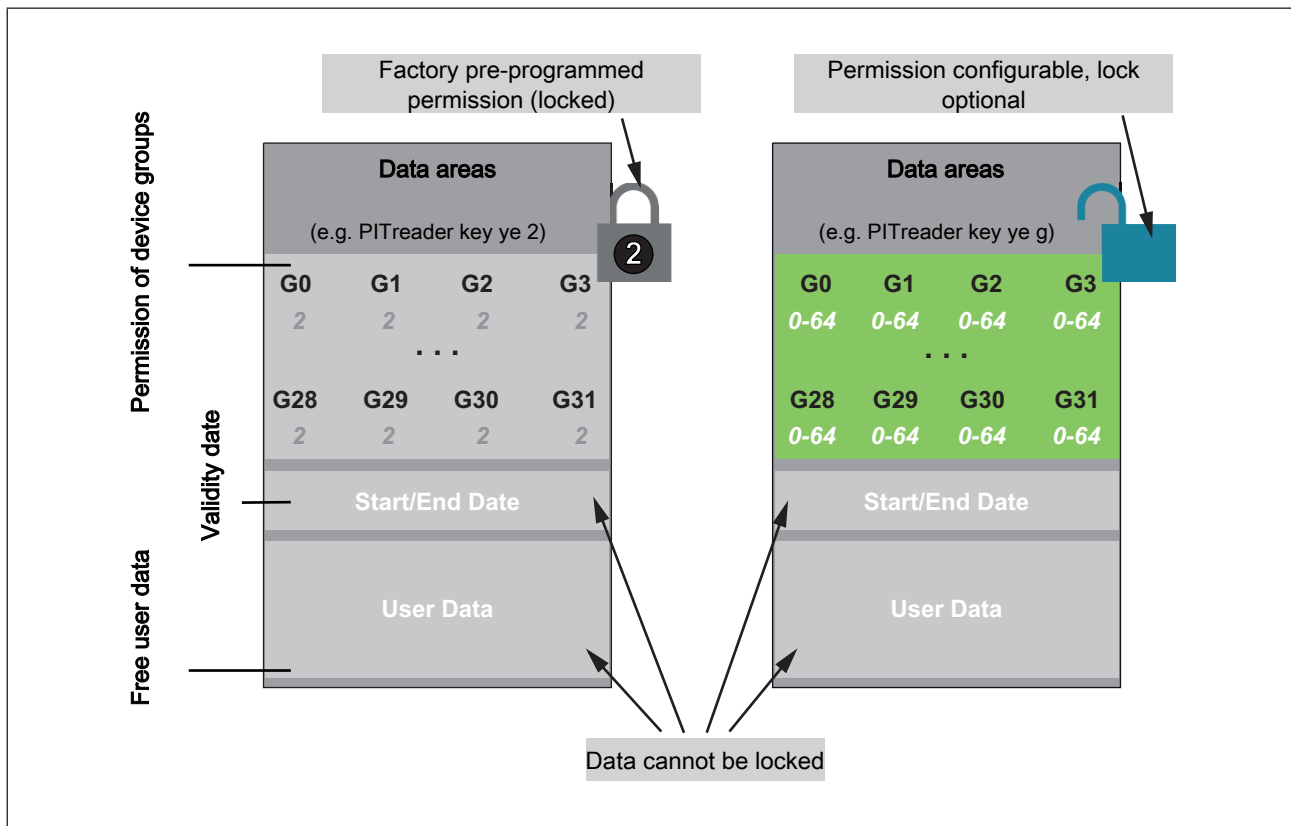


Fig.: Data areas of a transponder, using PITreader key ye 2 and PITreader key ye g as an example

4.5.1.3 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.

4.5.2 Transponders from third-party manufacturers with selected ISO/IEC standards (without MIFARE DESFire applications)

The reader units PITreader S card unit and PIT gb with PITreader Card can read transponders from third-party manufacturers. This is possible, even if no specific PITreader data is stored on the transponders, if they meet one of the following standards:

- ▶ ISO/IEC 14443 Type A
- ▶ ISO/IEC 15693
- ▶ ISO/IEC 18092 (Sony FeliCa)

However, only the ISO standard UID is read from a third-party transponder; this is then used to calculate the transponder's Security ID. No further data can be read or written.

This results in the following restrictions:

- ▶ Various security functions of the PITreader cannot be used, e.g. coding or protected communication via AES key.
- ▶ "Transponder data" authentication mode cannot be used.
- ▶ User data cannot be written to the third-party transponder.
- ▶ The safe evaluation unit PIT m4SEU can be used with some restrictions:
In this configuration, the least significant 3 Bytes of the UID are displayed at the Key-ID interface IDo0 ... IDo3 of the safe evaluation unit PIT m4SEU.
- ▶ Third-party transponders cannot be used in the "Key-in-Pocket" maintenance safeguarding system from Pilz.
- ▶ Two-factor authentication is not possible.

In order for the PITreader to support the third-party transponders, the option **Support third-party transponders** must be activated in the configuration (see [Configure third-party transponder with ISO/IEC standard as RFID protocol](#)  75]).



NOTICE

Possible security vulnerability due to third-party transponders whose identity cannot be determined

The use of third-party transponders is a potential security risk.

If the option **Support third-party transponder** is activated and an **ISO/IEC** standard is selected in the **RFID protocol** dropdown menu, the identity (UID) of the transponder cannot be determined safely. As a result there is no systematic protection against copying transponders or spoofing other transponders.

When carrying out your security risk analysis, consider that using third-party transponders can represent a security vulnerability for cyber threats.



NOTICE

If the option **Support third-party transponder** is activated and the standard **ISO/IEC 14443-A** is selected in the **RFID protocol** dropdown menu, PILZ transponders are treated as third-party transponders. In this case, only the UID is read from Pilz transponders and the same restrictions apply as for third-party transponders, see [Transponders from third-party manufacturers with selected ISO/IEC standards \(without MIFARE DESFire applications\)](#) [ 34]

4.5.3 Transponders from third-party manufacturers with MIFARE DESFire applications

You can use transponders with MIFARE DESFire applications with the following products:

- ▶ PITreader S Card unit
- ▶ PIT gb QLLE y up ETH
- ▶ PIT gb QLLE y down ETH

The following transponders with MIFARE DESFire applications are supported:

- ▶ NXP MIFARE DESFire EV2
- ▶ NXP MIFARE DESFire EV3
- ▶ Legic ATC4096-MP312
- ▶ Legic ATC4096-MP313

With these transponders, all the functions available when using Pilz transponders are available for the PITreader.

In order to use transponders with MIFARE DESFire applications

- ▶ The PITreader data structure must be applied to the transponders.
Technically, this corresponds to your own MIFARE DESFire application. To apply the PITreader data structure, at least 1440 bytes must be free in the transponder memory. Thereafter, the transponders with MIFARE DESFire applications behave like Pilz transponders and support all PITreader functions.
- ▶ AES keys must be stored in the PITreader. These cryptographic keys enable the PITreader to authenticate itself on the transponder. As a result, the PITreader can read and write data to the transponder. Using diversification, an individual AES key can be generated for each transponder.

4.5.4 Transponder's security ID (SID)

A transponder's Security ID (SID) is a unique identifier, which is only valid for this one transponder.

- ▶ Pilz transponders

All Pilz transponders are factory pre-programmed with a Security ID. A transponder's Security ID cannot be changed.

Note: If the option **Support third-party transponders** is activated in the PITreader, the pre-programmed Security ID will not be valid for the Pilz transponders but instead a Security ID, which is calculated in the PITreader from the transponder's UID.

- ▶ Third-party transponders for which ISO/IEC 14443 Type A, ISO/IEC 15693 or ISO/IEC 18092 (FeliCa) has been selected in the **RFID protocol** dropdown menu
The Security ID is calculated in the PITreader from the transponder's UID.

- ▶ Third-party transponders with MIFARE DESFire applications

The Security ID is calculated during initialisation from the transponder's Product ID, serial number and UID. After that, it cannot be changed.

The Security ID is used to uniquely identify a transponder on the PITreader; i.e. a transponder on the PITreader is authenticated 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 OPC 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](#) [85]).

4.5.5

Transponder recognition with one PITreader Card

► Maximum read distance when positioning a transponder

– 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.

– Transponder card or transponder sticker

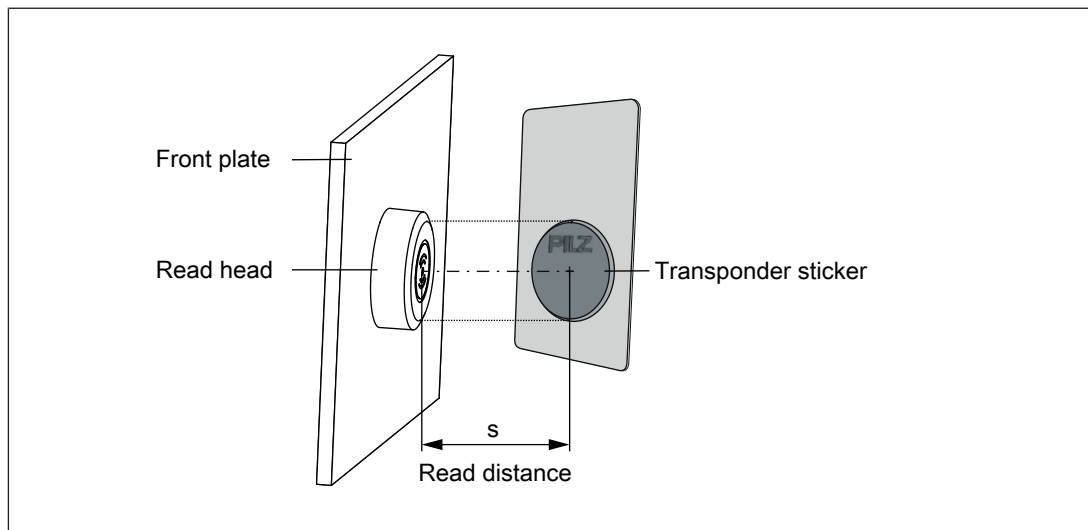
The centre of the transponder should ideally be positioned over the centre of the read head.

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" (see LED indicator).

4.6 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](#)  40]).

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
31	BIT	1 Byte	0 or 1	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 is extended from 0 ... 31 to 0 ... 9999. In order for the groups 32 ... 9999 to be employed, it is absolutely essential that the system parameter with ID 1 is created (see [System parameters](#)  40]).

Details of how to configure the user data are described here: [Configure user data](#)  85]

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 is used for all device groups 0 ... 9999, for which no separate value is configured.

Details of how to write the values for the parameters on a transponder are described here:
[Edit user data values](#)  84]

The user data can be read by 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.

4.6.1 System parameters

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

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

4.7 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](#)  42]
- ▶ [OEM coding](#)  43]

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](#)  84)).

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](#)  74] and [Set OEM coding](#)  74]).

4.7.1 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](#)  43]).

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](#)  74]). 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](#)  82]).

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.

4.7.2 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](#) [82]).

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

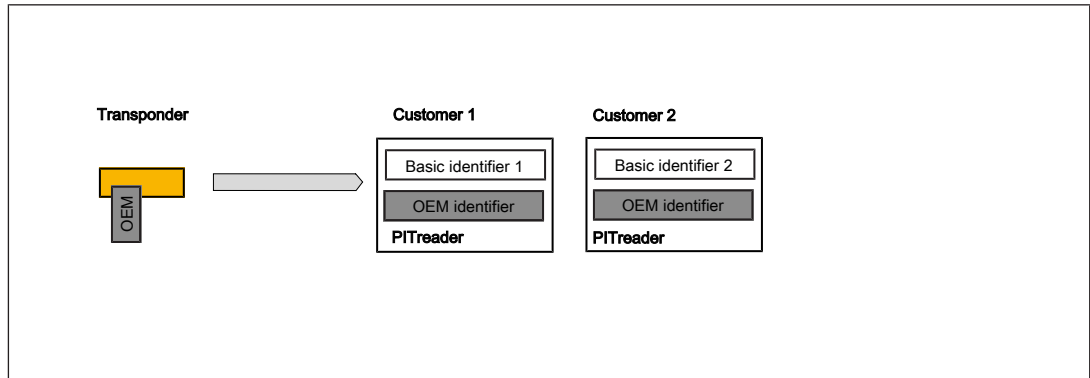


Fig.: OEM coding

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](#) [82].

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](#) [74].

4.8 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 their transponder. It can stop unauthorised persons authenticating themselves on the PITreader.

The block list can contain up to 1000 entries.

The block list can be used in any authentication mode.

See also [Use block list](#)  85].

4.9 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.

4.10 Synchronisation with external data

There is data on the PITreader (e.g. permission list and block list) that can be updated by an external service (e.g. PIT User Authentication Service). The data is maintained in a database and then synchronised with the PITreader by the external service.

This synchronisation can be monitored, to ensure that it actually takes place. A time of 5 minutes to 3 days can be configured; this is called the "Synchronisation timeout". If synchronisation is monitored and synchronisation does not occur within the timeout, then the authentication of transponders is blocked. Transponders cannot be authenticated again until the data has once again been synchronised. Monitoring of synchronisation restarts.

If the PITreader is switched off, the time that has already elapsed is stored and continues running when the PITreader is switched back on. When switching on, if the time until the timeout occurs is less than 10 minutes, then it is automatically set to 10 minutes. As a result, after switching on there is always a time window of 10 minutes available for the initial synchronisation.

When a timeout occurs, the diagnostic list displays the alarm "A synchronisation timeout has occurred." until the data has been synchronised successfully.

Monitoring of synchronisation increases security. A potential attacker can no longer interrupt the connection between the PITreader and external service in order to prevent the data on the PITreader being updated.

Configuration of monitoring (see [Configure synchronisation monitoring](#)  86]).

4.11 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.

4.11.1 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)

4.11.2 Function codes (Client connections)

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

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

4.11.3 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 Product ID (coded) Bits 31 to 24: Product group (0 = empty, 1 = G1) Bits 19 to 0: Product number Examples: PITreader base unit (402255): 0x 00 0 6234F PITreader card unit (402320): 0x 00 0 62390 PIT gb RLLE y up ETH (G1000020): 0x 01 0 00014
3x0003 ... 3x0004	PITreader serial number
3x0005 ... 3x0006	Operating hours counter in minutes
3x0007 ... 3x0008	RTC time stamp, seconds since 01.01.2000 00:00 (UTC)
3x0009	LED colour (see also LED control  45])
3x0010	LED flash mode (see also LED control  45])
3x0011	Diagnostic status (all diagnostic messages are assigned a severity; severity 3 = error, severity 8 = warning, severity 13 = status information)
3x0012	Reserved
3x0013 ... 3x0016	PITreader Product ID (ASCII)
3x0017	PITreader revision (ASCII)
3x0018	Reserved
3x0019	SEU status information (see also operating manual PIT m4SEU, section 5.5) Default value if no SEU is connected: 0x00F0 (decimal: 240)
3x0020 ... 3x0024	Reserved
3x0025 ... 3x0028	Security ID (data from the transponder)
3x0029 ... 3x0030	Reserved
3x0031 ... 3x0032	Permission (code word)

Address	Contents
3x0033	Permission (integer, 0 to 64)
3x0034	Authentication status: ▶ 0 = Not authenticated ▶ 1 = Transponder successfully authenticated ▶ 2 = Waiting for external authentication ▶ 3 = Waiting for PIN
3x0035 ... 3x0036	Product ID (transponder)
3x0037 ... 3x0038	Serial number (transponder) (see also Evaluation of a transponder's serial number [ 34])
3x0039 ... 3x0042	Reserved
3x0043 ... 3x0047	Transponder's UID in accordance with ISO standard (4, 7 or 10 Bytes); the data length is in the register 3x0048
3x0048	Data length of UID (number of bytes)
3x0049 ... 3x0054	Reserved
3x0055 ... 3x0056	Start date from which the transponder is valid; seconds since 01.01.2000 00:00 (UTC)
3x0057 ... 3x0058	End date to which the transponder is valid; seconds since 01.01.2000 00:00 (UTC)
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

Address	Contents
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
3x0119 ... 3x0120	Permission group 30
3x0121 ... 3x0122	Permission group 31
3x0123 ... 3x0158	Reserved
3x0159 ... 3x0166	Check sum for basic coding
3x0167 ... 3x0174	Check sum for OEM coding
3x0175 ... 3x0999	Reserved
3x1000 ... 3x1519	User data (see also information below and User data [39])
3x1520 ... 3x9999	Reserved



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.

4.11.3.1**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 Registers)	
Write data (Word)	FC 06 (Write Single Register)	1 Word
	FC 16 (Write Multiple Registers)	1 ... 123 Words

4.12 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](#)  68] and [Firmware update](#)  90]).

4.13 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](#)  26]).

4.14 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).

5 Installation and removal

5.1 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.

5.2 Installation and removal of a PITreader Key

5.2.1 Installation of PITreader Key

Procedure

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

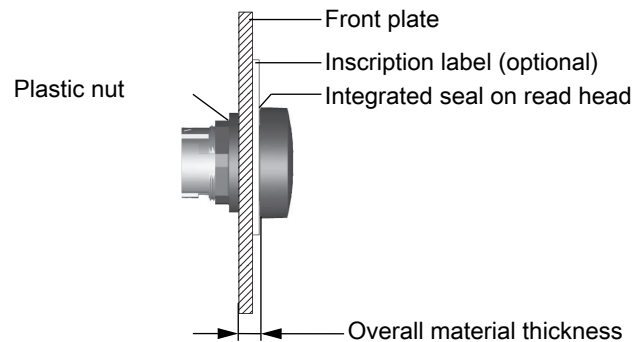
Maximum permitted material thickness:

- 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.:

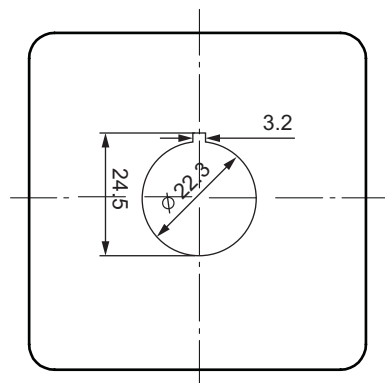
Material thickness_{Maximum} = Material thickness_{Front Plate} + Material thickness_{Optional Materials}

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:



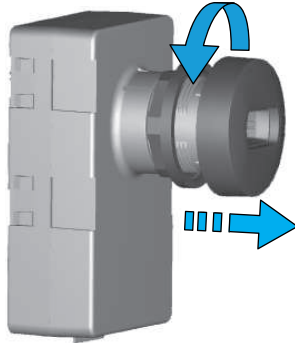
In the example, the recess can be positioned so that the base unit can be installed either with an upward or downward cable outlet.

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:

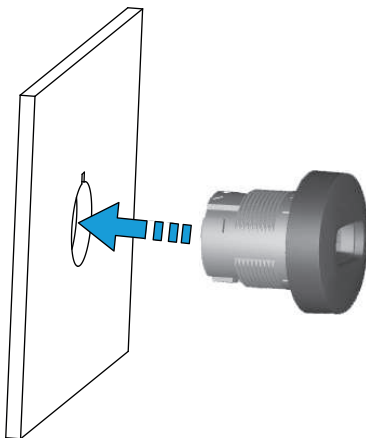
Hold the base unit firmly, rotate the read head 15° anti-clockwise and pull the read head from the base unit.



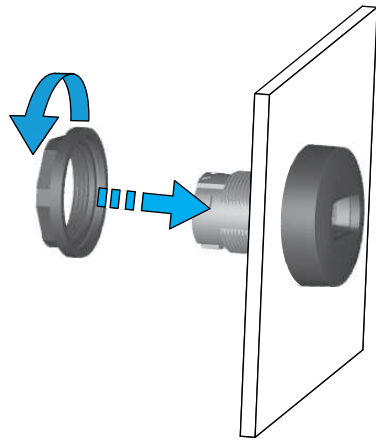
- Remove the plastic nut (M22) from the read head.



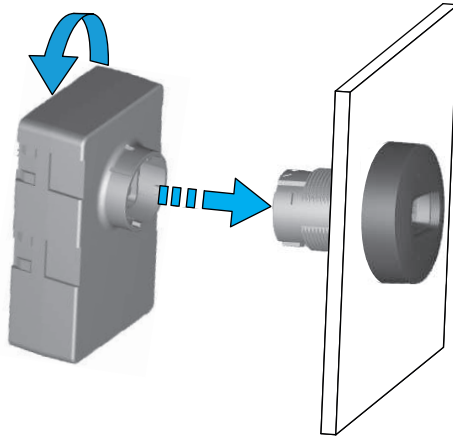
- From the front, insert the read head into the mounting cutout so that the latch is positioned in the recess on the mounting cutout.



- 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 \[📖 109\]](#)).



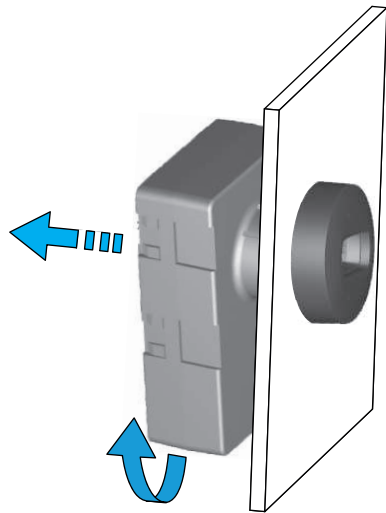
- Connect the base unit to the read head and rotate the base unit 15° clockwise until it locks in position.



5.2.2 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.



5.3 Installation and removal of a PITreader Card

5.3.1 Installation of PITreader Card

Procedure

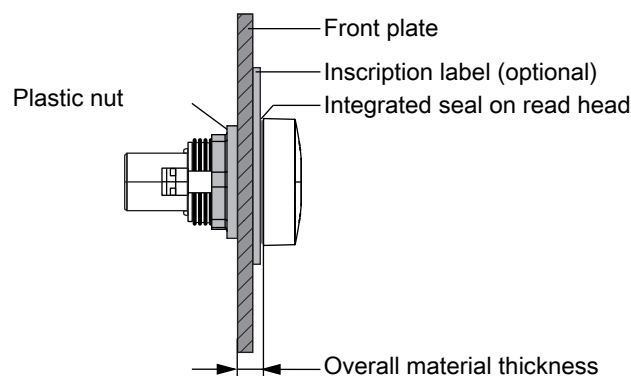
- Install the device in the front panel of a control cabinet or in a control console.

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.:

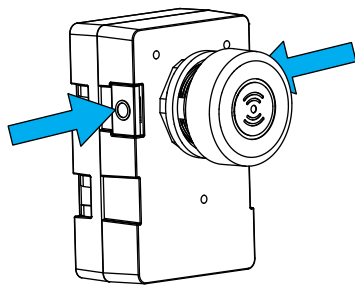
Material thickness_{Maximum} = Material thickness_{Front Plate} + Material thickness_{Optional Materials}

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



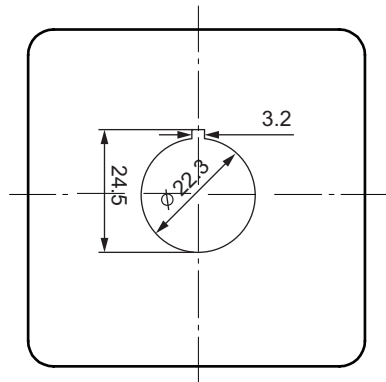
The overall material thickness must not exceed the maximum permitted material thickness.

- 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 (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 card Adapter. The latch provides anti-rotation protection.

Example:



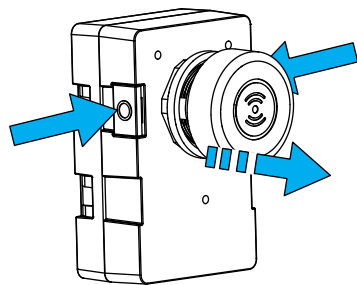
In the example, the position of the recess is such that the cable for the base unit exits upwards.

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.

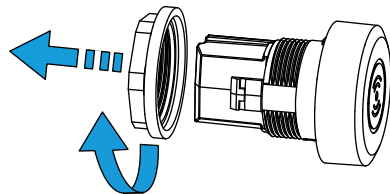
- On your device, if the read head is not installed on the base (e.g. as delivered), you can skip this step.

Otherwise:

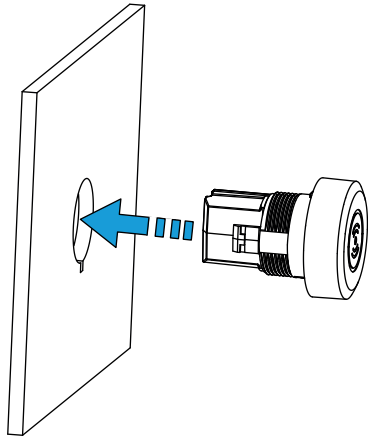
On the sides of the base unit housing, press and hold the two release buttons, then pull the read head from the base unit.



- 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.

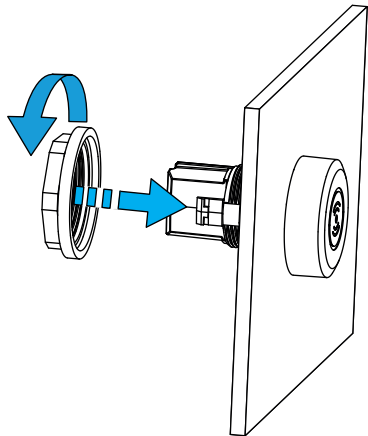


- Align the silicone cap on the read head in the required direction.

Note: After alignment, the latch must be positioned in one of the recesses on the silicone cap.

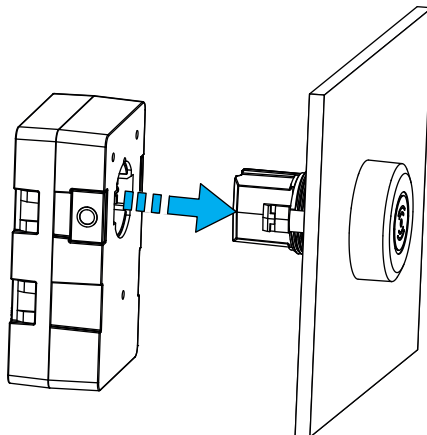
- Use the plastic nut (M22) to secure the read head from the other side.

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 \[📖 109\]](#)).



- Connect the base unit to the read head.

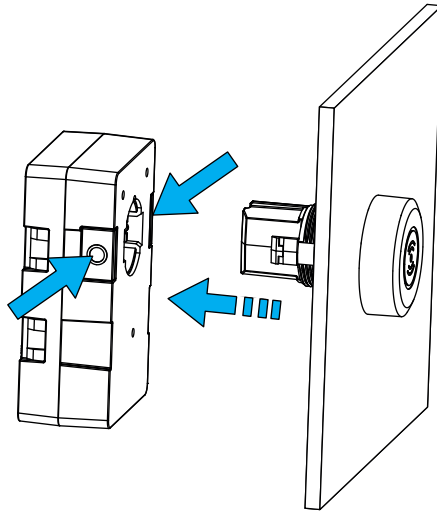
The base unit must lock in position.



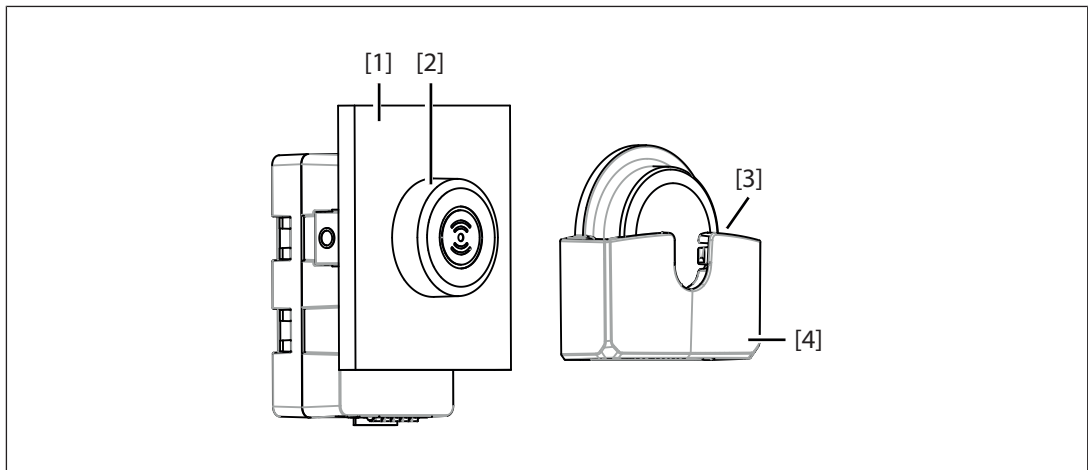
5.3.2 Removal of PITreader Card

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.



5.3.3 Installation PITreader card holder



- ▶ Clean the front plate [1] around the read head [2]. The adhesive position must be smooth and free from dirt, dust and grease.
- ▶ On the PITreader card holder [4], remove the protective film from the adhesive surface. Do not touch the adhesive surface, to ensure that the adhesive function is not compromised.
- ▶ Guide the PITreader card holder [4] so that it is a little above the read head [2]; the opening [3] of the PITreader card holder [4] must face upwards.
- ▶ Align the PITreader card holder [4] horizontally.
- ▶ Guide the PITreader card holder [4] further above the read head [2] until it is on the front plate [1].

- Press the PITreader card holder [4] firmly on to the front plate [1], around the read head [2].

5.3.4 Attach PITreader transponder sticker

The PITreader transponder sticker has a self-adhesive side and can be attached to an existing card, e.g. company ID. The card is then known as the carrier card. This reduces the number of cards required.



NOTICE

Transponder recognition impaired

If the PITreader transponder sticker is attached to a metallic carrier card, the PITreader may not be able to recognise the transponder.

Do not attach the PITreader transponder sticker to a metallic carrier card.



NOTICE

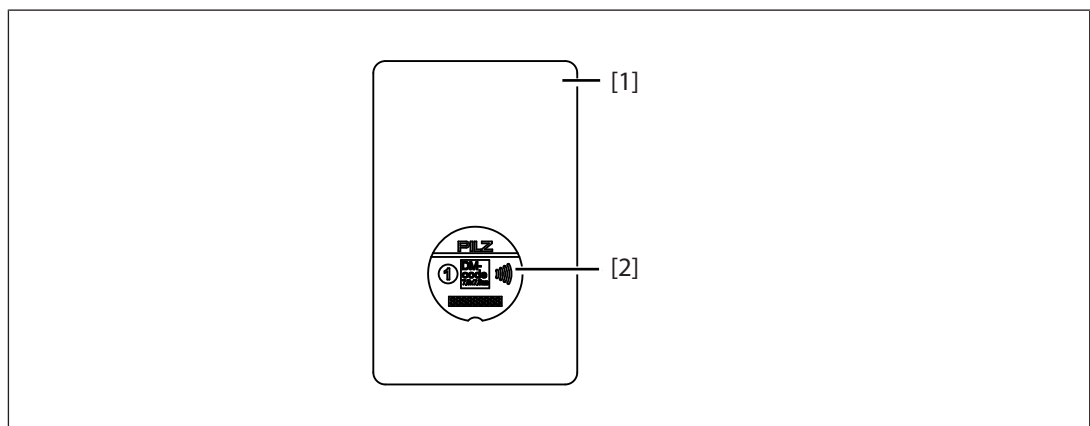
Functional impairment of the carrier card or PITreader transponder sticker

If the PITreader transponder sticker is attached to a functional surface on the carrier card, such as magnetic strips or a chip card contact surface for example, carrier card functions may no longer be available or may be compromised.

The PITreader transponder sticker and the carrier card with RFID function may interfere with each other and, as a result, not all functions may be available.

- Only attach the PITreader transponder sticker to surfaces that have no function. If necessary, use another carrier card.
- After attaching the PITreader transponder sticker, check the functions of the PITreader transponder sticker and carrier card.

5.3.4.1 Application without PITreader card holder



- ▶ Clean the carrier card [1] on which you wish to attach the PITreader transponder sticker [2]. The adhesive position must be free from dirt, dust and grease.
- ▶ On the PITreader transponder sticker [2], remove the protective film from the adhesive surface.
Do not touch the adhesive surface, to ensure that the adhesive function is not compromised.
- ▶ Attach the PITreader transponder sticker [2] to the carrier card [1].

5.3.4.2

Application with PITreader card holder

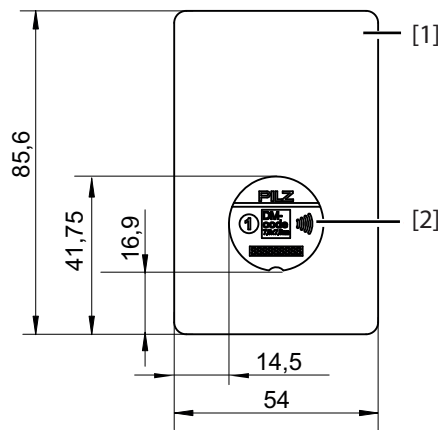


NOTICE

Transponder readability impaired

If the PITreader transponder sticker is not attached at the stipulated adhesive position on the carrier card, the PITreader Card may not be able to recognise the transponder.

- Only attach the PITreader transponder sticker at the stipulated adhesive position.
- Only attach the PITreader transponder sticker to surfaces that have no function. If necessary, use another carrier card.



- ▶ Use a carrier card [1] with the stated dimensions.
- ▶ Clean the carrier card [1] in and around the adhesive position of the PITreader transponder sticker [2].
The adhesive position must be free from dirt, dust and grease.
- ▶ On the PITreader transponder sticker [2], remove the protective film from the adhesive surface.
Do not touch the adhesive surface, to ensure that the adhesive function is not compromised.
- ▶ Attach the PITreader transponder sticker [2] to the adhesive position on the carrier card [1].

5.4 Installation and removal of a PIT gb with PITreader

You will find the necessary information in the operating manual PIT gb with PITreader.

5.5 Dimensions

5.5.1 Dimensions of PITreader Key

Dimensions in mm

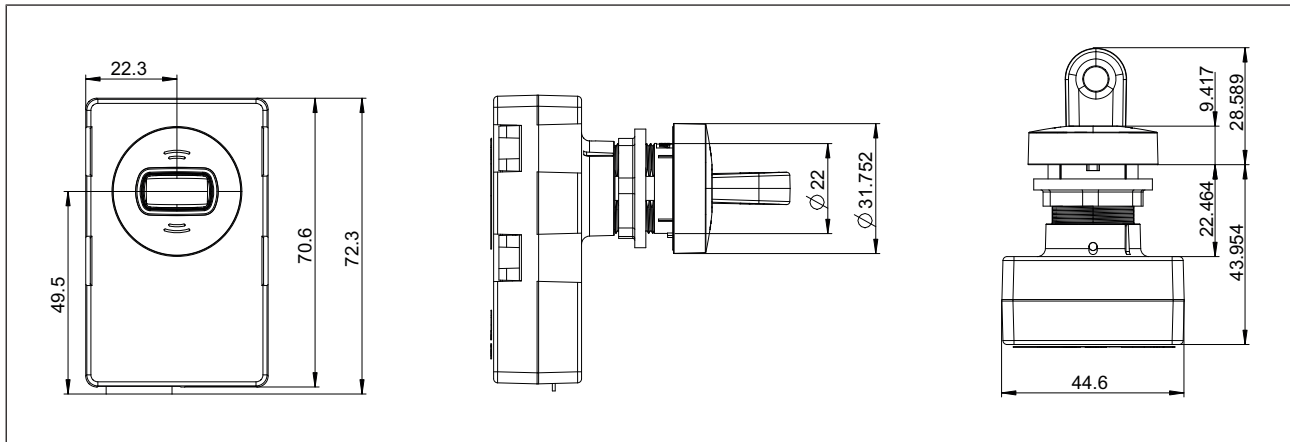


Fig.: Dimensions of a PITreader Key (base unit with spring-loaded terminal, read head PITreader key adapter h and positioned transponder key)

5.5.2 Dimensions of PITreader Card

Dimensions in mm

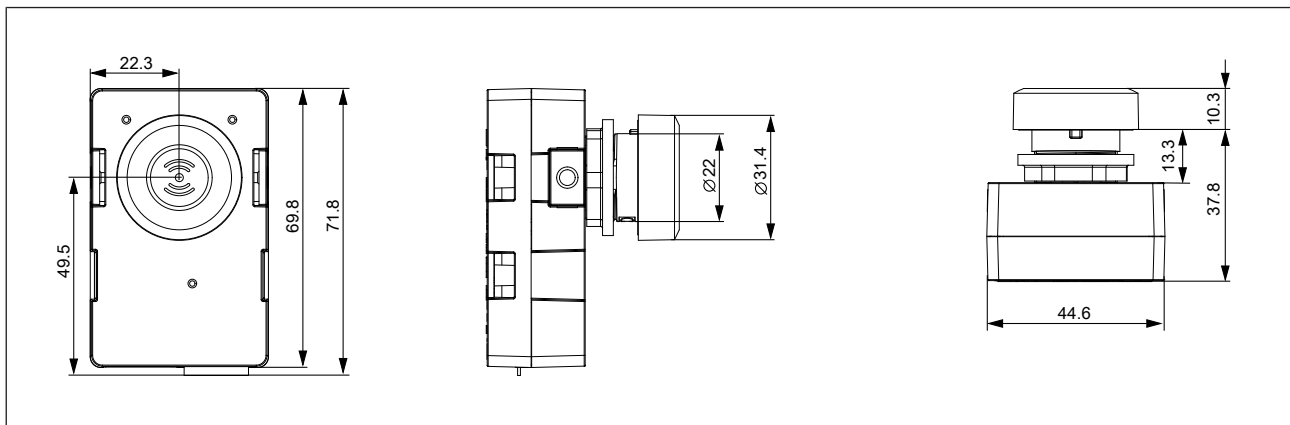


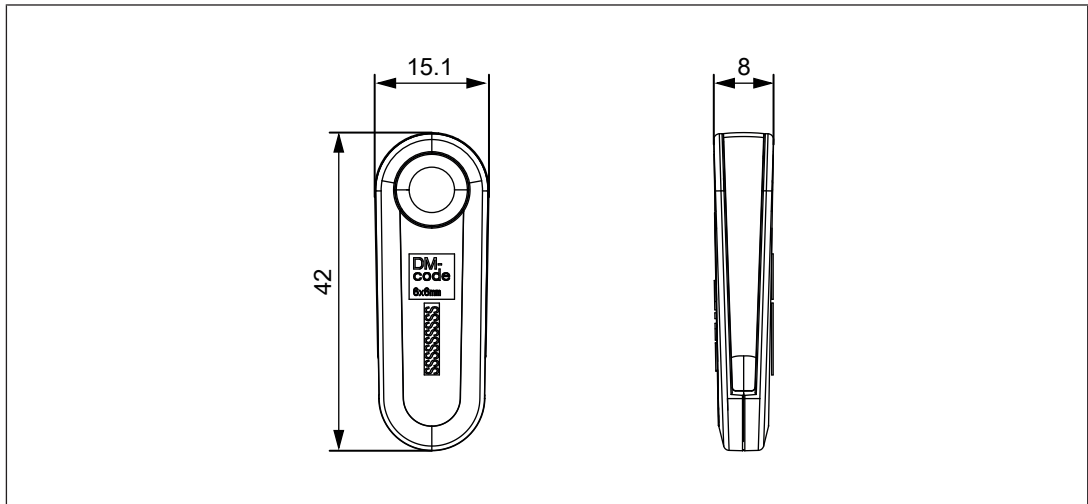
Fig.: Dimensions of a PITreader Card (base unit with spring-loaded terminal and read head PITreader card adapter)

5.5.3 Dimensions of PIT gb with PITreader

You will find the necessary information in the operating manual PIT gb with PITreader.

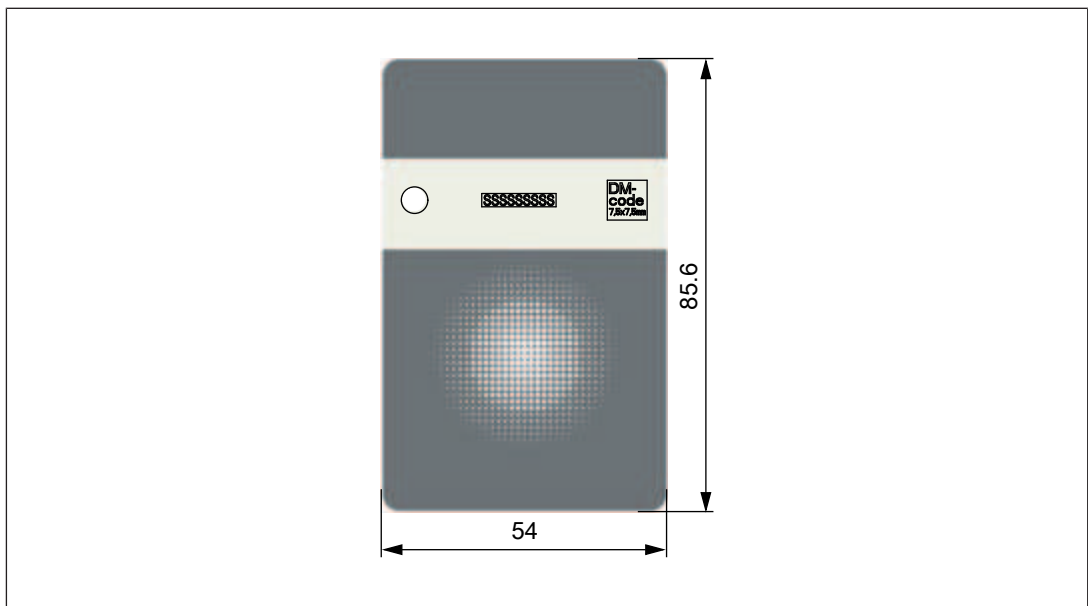
5.5.4 Dimensions of PITreader transponder key

Dimensions in mm



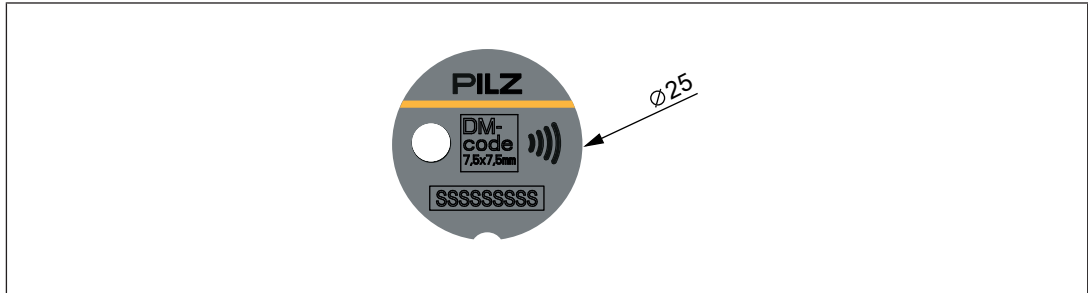
5.5.5 Dimensions of PITreader transponder card

Dimensions in mm



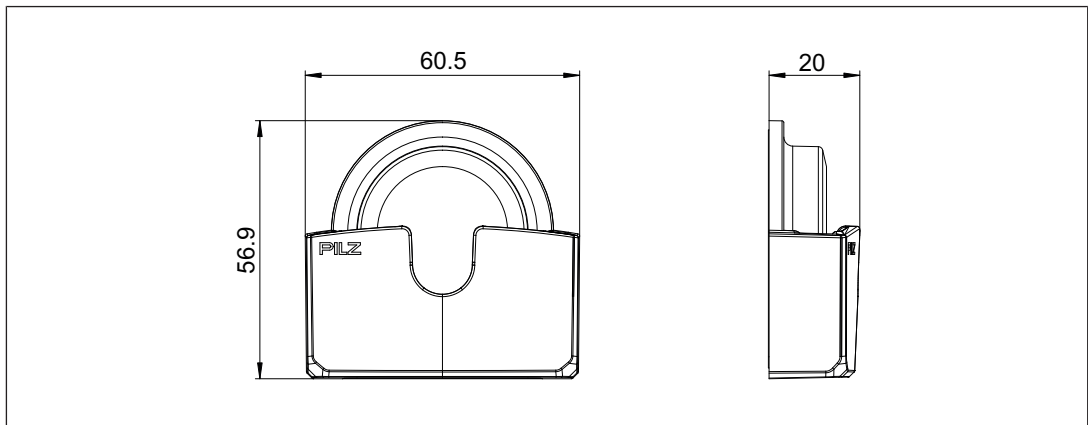
5.5.6 Dimensions of PITreader transponder sticker

Dimensions in mm



5.5.7 Dimensions PITreader card holder

Dimensions in mm



6 Wiring

6.1 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 the PIT gb with PITreader can be found in the operating manual PIT gb with PITreader.

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).

6.2 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.

7 Configuration

7.1 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.

7.2 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-<Product ID>-<Serial number>.local
An individual PITreader can be addressed specifically in a network via the address pilz-<Product ID>-<Serial number>.local.

A Multicast DNS query uses the Multicast Ipv4 group address 224.0.0.251. Multicast DNS queries to a PITreader are made via UDP and 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
- ▶ Product ID
- ▶ 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.

7.3 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. This is possible with the PIT Transponder Manager from Version 01.02.00, for example.

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 default "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.

7.4 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](#)  71).

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](#)  17)).

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).

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.

7.5 Device user

Additional device users can be created in the web application under **Users -> Device users**. 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 with different permissions.

When new device users are created, only those access rights that are necessary should be assigned via the corresponding role. This helps to control security and access to data.

There are 4 roles:

	Administrator	Device manager	Transponder manager	Guest (read access)
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 names	R/W	R/W	R	R
User data configuration	R/W	R/W	R	R

	Administrator	Device manager	Transponder manager	Guest (read access)
Support third-party transponders	R/W	R	R	R
Cryptographic key	R/W	R/W	-	-
Manage device users	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 users with the "Administrator" role
- *** With the exception of users with the "Administrator" role. Only the permitted device configuration settings can be restored (see [Save and restore configuration](#)  87])

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).

7.6 Manage certificates

7.6.1 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 the 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 default 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 transferred to other devices via the function **Save configuration/Restore configuration**.

7.6.2 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 the 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)

7.7 Configure authentication mode

You can configure the authentication mode for the PITreader in the web application under **Configuration -> Settings**. Select either "Transponder data", "External", "Permission list" or "Fixed permission" 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 go to **Configuration -> Settings -> Function** and activate **Allow external overriding**.

If **Allow external overriding** 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.

7.8 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".

7.9 Configure two-factor authentication

7.9.1 Enable two-factor authentication

You can enable two-factor authentication for the respective PITreader in the web application under **Configuration -> Settings**. In this case it will apply to this PITreader only. Select

- ▶ **Two-factor authentication required:** Two-factor authentication is enabled
- ▶ **Minimum PIN length for two-factor authentication:** Set the minimum PIN length to between 4 and 6 digits

7.9.2 Write PIN to transponder

A PIN can be written to a transponder, regardless of whether the connected PITreader requires a PIN as the second factor for authentication.

You can write a PIN to the transponder in the web application under Transponder -> Data. The PIN must be between 4 and 6 digits long.

You can also write the PIN to the transponder using the REST API and OPC Server UA. Further information can be found in the operating manuals for the PITreader REST API (1005365) and the PITreader OPC Server UA (1005480).

7.9.3 Enter your PIN for authentication

The PIN can be provided via the following interfaces:

- ▶ REST API
- ▶ OPC Server UA

To test this, you can also enter the PIN in the web application under **Status -> Authentication**.

7.10 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.

7.11 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**. This function is deactivated in the default configuration.

7.12 Audit trail messages deleted automatically

In the web application, you can specify that audit trail messages are deleted automatically after a configurable number of days.

To do this, select **Configuration -> Settings**. Under **Advanced functions**, set the desired number of days under **Audit trail messages deleted automatically after**.

This function is deactivated in the default configuration.

7.13 Set device group

You can assign a device group to the PITreader in the web application under **Configuration -> Settings** (see also [Device groups \[22\]](#)). 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**, the corresponding name is displayed in the selection list. If no name has been entered, the number of the device group is displayed.

7.14 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 \[41\]](#).

7.15 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](#) [📖 41].

7.16

Configure third-party transponder with ISO/IEC standard as RFID protocol

The reader units PITreader S card unit and PIT gb with PITreader Card also support transponders from third-party manufacturers.

For configuration, go to **Configuration -> Settings ->** in the web application and activate **Support third-party transponders** under **Advanced functions**. The **RFID protocol** dropdown menu appears.

In the dropdown menu **RFID Log**, you can select one or more of the following standards:

- ▶ **ISO/IEC 14443-A**
- ▶ **ISO/IEC 15693**
- ▶ **ISO/IEC 18092 (Sony FeliCa)**

Only transponders that meet the selected standard will be recognised. If transponders with a different RFID protocol are used, the PITreader units will not respond and the LED on the reader unit will continue to light up blue.



NOTICE

If the option **Support third-party transponder** is activated and the standard **ISO/IEC 14443-A** is selected in the **RFID protocol** dropdown menu, PILZ transponders are treated as third-party transponders. In this case, only the UID is read from Pilz transponders and the same restrictions apply as for third-party transponders, see [Transponders from third-party manufacturers with selected ISO/IEC standards \(without MIFARE DESFire applications\)](#) [📖 34]

7.17 Configure third-party transponders with MIFARE DESFire application

The reader units PITreader S card unit and PIT gb with PITreader Card also support transponders from third-party manufacturers.

The cryptographic keys (AES keys) enable the PITreader to authenticate itself on the transponder. As a result, the PITreader can read and write data to the transponder. Using diversification, an individual AES key can be generated for each transponder.

The following cryptographic keys are available	Explanation
Application Master Key Use: always required Diversification: recommended, freely selectable	The Application Master Key is used to protect the PITreader application on the transponder from manipulation and from being overwritten. To do this, the Application Master Key must be set up on the PITreader. This key can then be used to transfer the desired PITreader application to the transponder with MIFARE DESFire applications.
PICC Master Key Use: optional Diversification: must be set to match the configuration of the transponder with the MIFARE DESFire application	The PICC Master Key is required to program the PITreader application on a transponder with MIFARE DESFire applications, when bit 2 of the PICCKeySettings has the value 0. The AES keys and diversification settings specified by the manufacturer or supplier of the transponder with MIFARE DESFire applications must be stored in the PITreader. For this purpose, the PICC Master Key must be stored in the PITreader that is also used to apply the PITreader application to the transponder with MIFARE DESFire applications.
Application User Key Use: optional Diversification: recommended, freely selectable	In normal operation, the PITreaders use the PITreader application via the Application User Key. If your own Application User Key is not stored in the corresponding PITreader, an AES key is used, based on the set basic coding. This eliminates the need to configure your own AES keys for PITreaders that are intended to access transponders with MIFARE DESFire. However, if you have configured your own Application User Key on the initialisation PITreader, this must be stored in all other PITreaders on which the corresponding transponder with MIFARE DESFire is to work.

The following cryptographic keys are available	Explanation
Application Default Key Use: optional Diversification: not supported	The Application Default Key is specified by the manufacturer or supplier of the transponder with MIFARE DESFire applications. If the default value of the Application Default Key on the transponder with MIFARE DESFire is not 0x00..00, the corresponding value must be entered in the initialisation PITreader. This is important so that the transponder can be authenticated by the PITreader.
Transport Key Use: optional Diversification: must be set to match the configuration of the transponder with the MIFARE DESFire application	"Transport Keys" can be used temporarily to enable external third parties to apply the PITreader data structure to the MIFARE DESFire transponder memory. These temporary AES keys can be replaced later with your own AES keys in the PITreader. This ensures security and control over the data structure on the transponder.

Diversification

Diversification is performed in accordance with the procedure for 128-bit AES keys, as described in NXP Application Note AN10922 (Symmetric key diversifications). This procedure is used to guarantee security and authentication between the transponder and the PITreader.

For each AES key, the diversification can be entered in the PITreader web application under **Configuration -> Crypto. key**. This must be stated as hexadecimal encoded bytes, e.g. A1B9.... The placeholder "\$UID" can be used to diversify AES keys for each transponder individually.

During diversification, the placeholder "\$UID" is replaced by the transponder UID in accordance with ISO 14443-A. One example of diversification with a placeholder for "\$UID" would be A1B9F0\$UID03.

7.17.1 Select RFID protocol

For configuration, go to **Configuration -> Settings ->** in the web application and activate **Support third-party transponders** under **Advanced functions**. The **RFID protocol** dropdown menu appears.

In the **RFID protocol** dropdown menu, you can then select the standard **MIFARE DESFire with PITreader data structure**. With this standard, the cryptographic keys and encoding must be stored.

Pilz transponders cannot be used.

Only transponders that meet the selected standard will be recognised. If transponders with a different RFID protocol are used, the PITreader units will not respond and the LED on the reader unit will continue to light up blue.

7.17.2 Store cryptographic keys

To store the cryptographic keys, select **Configuration -> Crypto. Keys** in the web application. The **cryptographic keys** selection menu appears.

Memory space 1 and memory space 2

Under **Memory space 2**, select **Edit**. The **Set cryptographic key** menu appears. In the **Type** dropdown menu for **Memory space 1** and **Memory space 2**, you can then choose between the following cryptographic keys:

- ▶ **Application Master Key**
- ▶ **Application User Key**
- ▶ **PICC Master Key**
- ▶ **Transport Key**

When the cryptographic key is selected:

- ▶ Under **AES key**, enter the corresponding 128-bit AES key: hexadecimal entry of exactly 32 characters, e.g.: C963EC29964DE3399BDE34E478014963
- ▶ Under **Diversification**, enter the corresponding key: hexadecimal entry of maximum 62 characters with AES key placeholder "\$UID", e.g.: A1B9F0\$UID03

Application Default Key

Under **Application Default Key**, select **Edit**. The **Set Application Default Key** menu appears.

- ▶ Under **AES key**, enter the corresponding 128-bit AES key: hexadecimal entry of exactly 32 characters, e.g.: C963EC29964DE3399BDE34E478014963

7.18 Initialise third-party transponder with MIFARE DESFire application

There are 4 options for initialising third-party transponders with MIFARE DESFire application:

- ▶ [Initialise third-party transponder yourself !\[\]\(73a4b87cf9b3bab6f9fecd9ef10139c0_img.jpg\) 78](#)
 - The third-party transponder does not require prior authentication with the PICC Master Key in order to create new applications. [79](#)
 - The third-party transponder requires prior authentication with the PICC Master Key in order to create new applications [80](#)
- ▶ [Initialise third-party transponder through a third party !\[\]\(1dbec70abef03f8a9674bf16008535c5_img.jpg\) 80](#)
 - Using your own Application Master Keys and Application User Keys [80](#)
 - Using Transport Keys [81](#)

7.18.1 Initialise third-party transponder yourself

- ▶ In the RFID protocol, select the standard **MIFARE DESFire with PITreader data structure**, see [Select RFID protocol !\[\]\(566b694a89e8fe2c13eba2407849fa90_img.jpg\) 77](#).
- ▶ Set basic coding and store the necessary cryptographic keys:
 - The third-party transponder does not require prior authentication with the PICC Master Key in order to create new applications. [79](#)

- The third-party transponder requires prior authentication with the PICC Master Key in order to create new applications [80]

- ▶ In the web application, select **Transponder -> Initialisation**.
- ▶ In the Serial number field, enter a unique serial number for the transponder.
- ▶ As an option, you can enter a Product ID for the transponder under Product ID.
- ▶ Position the transponder to be initialised in front of the PITreader read head, see [Position transponder \[91\]](#).
- ▶ Click on the Initialise field below.
The transponder is initialised and can now be programmed, see [Write/program transponder \[81\]](#).

**WARNING!**

Key-in-Pocket system: Possible loss of the safety function if third-party transponders have not been assigned a unique serial number.

If third-party transponders have not been assigned a unique serial number, in some circumstances the Key-in Pocket system cannot evaluate the internal sign-in list correctly. As a result, the Key-in Pocket system might not detect the presence of people in the danger zone.

There is an increased risk of injury or even a threat to life!

- Always assign unique serial numbers when initialising third-party transponders.

Even if transponders with MIFARE DESFire application contain a PITreader application, they can be re-initialised. To do this, the Application Master Key stored in the PITreader must match the Application Master Key from the previous initialisation. During initialisation, all data in the existing PITreader application is reset and the serial number and Product ID are overwritten.

7.18.1.1

The third-party transponder does not require prior authentication with the PICC Master Key in order to create new applications.

PITreader configuration		
	Initialisation PITreader	All other PITreaders
Basic coding	Must be set	Must be set
Cryptographic key	Key 1: Application Master Key (choose your own key, diversification freely selectable)	Key 1: (empty)
	Key 2: (empty)	
	If necessary, enter the appropriate Application Default Key for the transponder.	

- ▶ Set the identifier for basic coding under **Configuration -> Coding**, see [Set basic coding \[74\]](#).

- Store the cryptographic keys listed in the table above, see [Store cryptographic keys](#)  78].

7.18.1.2

The third-party transponder requires prior authentication with the PICC Master Key in order to create new applications

Configuration of the PITreader		
	Initialisation PITreader	All other PITreaders
Basic coding	Must be set	Must be set
Cryptographic key	Key 1: Application Master Key (choose your own key, diversification freely selectable)	Key 1: (empty)
	Key 2: PICC Master Key (appropriate for the transponders, diversification must also be set appropriately)	
	If necessary, enter the appropriate Application Default Key for the transponder.	

- Set the identifier for basic coding under **Configuration -> Coding**, see [Set basic coding](#)  74].
- Store the cryptographic keys listed in the table above, see [Store cryptographic keys](#)  78].

7.18.2

Initialise third-party transponder through a third party

To enable initialisation through a third party, you can request a definition of the PITreader data structure from PILZ. You then have the advantage that you do not have to assign the transponder serial numbers yourself.

This would allow your transponders to be set up in advance with uniform serial numbers.

7.18.2.1

Using your own Application Master Keys and Application User Keys

If you use your own Application Master Key and Application User Key, then you do not need your own initialisation PITreader to set up the transponders with the MIFARE DESFire application.

However, all PITreaders on which the transponders are used must then be set up with the appropriate "Application User Key".

Configuration of the PITreader	
	All PITreaders
Basic coding	Must not be set
Cryptographic key	Key 1: Application User Key (setting in accordance with the data agreed with third parties)
	Key 2: (empty)

- Store the cryptographic keys listed in the table above, see [Store cryptographic keys](#)  78].

7.18.2.2 Using Transport Keys

Temporary Transport Keys can be used to avoid having to set up your own Application User Key on all PITreaders. To do this you need your own initialisation PITreader, on which an Application Master Key and Transport Key are set up.

The Transport Keys are replaced by your own keys as soon as the transponder is recognised by an initialisation PITreader configured with an Application Master Key and corresponding Transport Key. The Transport Keys are replaced by your own Application User Keys.

Configuration of the PITreader		
	Initialisation PITreader	All other PITreaders
Basic coding	Must be set	Must be set
Cryptographic key	Key 1: Application Master Key (choose your own key, diversification freely selectable)	Key 1: (empty)
	Key 2: Transport Key (setting in accordance with the data agreed with third parties)	

- ▶ Set the identifier for basic coding under Configuration -> Coding, see [Set basic coding](#) [74].
- ▶ Store the cryptographic keys listed in the table above, see [Store cryptographic keys](#) [78].
- ▶ Position all transponders with MIFARE DESFire application on the initialisation PITreader. The Transport Key is replaced by the Application User Key.

7.19 Write/program transponder

7.19.1 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.

7.19.2 Configure the validity of the transponder



INFORMATION

The validity date of transponders can only be evaluated in "Transponder data" authentication mode.

You can limit the validity of transponders to a certain time period. To do this go to **Configuration -> Settings -> Advanced functions**, activate **Evaluate validity date** and set the valid time zone. The selected time zone is only used to evaluate the validity date. Under **Transponder -> Permissions** 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").

7.19.3 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.

7.19.4 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:

PITreader

Configuration Coding

Coding

Basic coding

Status Not set

Identifier myOEM_Code

Comment

Set coding

OEM coding

Status Not set

Identifier

Comment

Set coding

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.

7.19.5 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**.

7.19.6 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 \[85\]](#)). 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.

7.19.7 Delete user data on transponders

- ▶ In the web application, select **Transponder -> User data**.
- ▶ Select **Delete user data on transponder**.

7.20 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 \[106\]](#)).
- ▶ 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.
- ▶ The permission list can contain up to 1000 entries.

See also ["Permission list" authentication mode](#)  26].

7.21 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.
- ▶ The block list can contain up to 1000 entries.

See also [Block list](#)  44].

7.22 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.

7.23

Configuration for PIT Windows Logon

In order to use PIT Windows Logon, a PIT Windows Logon Key must be written/programmed on the transponder. You can use the PIT Windows Logon Key from the PIT Windows Logon software or from the PITreader.

Write/program the PIT Windows Logon Key to the transponder via the PITreader:

In the web application, select **Configuration -> Crypto Key**, then **PIT Windows Logon Key**.

Enter a PIT Windows Logon Key here and secure it with a password.

The PIT Windows Logon Key can then be written/programmed to the transponder:

In the web application, select **Transponder -> Crypto Key**, then **Program transponder**.

In the Password field, enter the pre-assigned password for the PIT Windows Logon Key and click on **Program**.

To check whether a PIT Windows Logon Key is stored on the transponder and if so which one: In the web application, select **Transponder -> Crypto Key** and click on **Update** under **Cryptographic keys on transponder**.

Write/program the PIT Windows Logon Key to the transponder using the PIT Windows Logon software:

Information can be found in the operating manual PIT Windows Logon (1007324).

7.24

Configure synchronisation monitoring

Synchronisation with external data can be monitored (see [Synchronisation with external data](#) [44]).

To do this, in the web application go to **Configuration -> Settings -> Advanced functions**, activate **Synchronisation monitoring** and enter the maximum interval between two synchronisations (5 minutes to 3 days) under **Synchronisation timeout**.

7.25 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".

7.26 Save and restore configuration

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

The saving and storing of the configuration is dependent on the role of the user.

Users with the "Administrator" role:

- ▶ Configuration saved by a user with the "Administrator" role:
 - The administrator may save all available data.
 - The saved list of device users contains all device users.
- ▶ Configuration restored by a user with the "Administrator" role:
 - The administrator may restore all the data that's available in the backup file.
 - If the backup file contains a list of the device users and the list contains at least one user with the name "Admin", the role "Administrator" and the authentication "Name/password", then all users are imported. They will replace the existing users on the device.
 - If the backup file contains a list of the device users and the list contains no users with the role "Administrator", then the existing users on the device with the role "Administrator" are retained. Users with the roles "Device manager", "Transponder Manager" and "Guest" are replaced by the users in the backup file.

Users with the "Device manager" role:

- ▶ Configuration saved by a user with the "Device manager" role:
 - Device managers may only save the data to which they have read and write access. See [Device user](#)  70].
 - The saved list of device users contains all device users, but not users with the role "Administrator".
- ▶ Configuration restored by a user with the "Device manager" role:
 - Device managers may only restore the data to which they have read and write access. See [Device user](#)  70].

- If the backup file contains a list of the device users and the list contains users with the role "Administrator", then these are ignored. The existing users on the device with the "Administrator" role are retained. Users with the roles "Device manager", "Transponder Manager" and "Guest" are replaced by the users in the backup file.

7.27 Reset to default settings

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

7.27.1 Reset via short circuit at the terminals TxD/RxD

In the event of a short circuit at the terminals TxD/RxD, all the data on the PITreader is reset to its factory default settings (including the basic coding); only the diagnostic log is retained.

Follow the instructions below:

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



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.

- ▶ 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 PIT gb with PITreader to the factory default settings can be found in the operating manual PIT gb with PITreader.

7.27.2 Reset in the web application

- ▶ In the **Maintenance** menu, under **Factory reset**, select **Reset to factory default settings**.
The selection menu appears.
- ▶ In the **Reset to factory default settings** selection menu, select which data is to be reset:
 - **Device configuration**
 - **Diagnostic log**

- *Names of device groups*
 - *Configuration of user data*
 - *Permission list*
 - *Transponder block list*
- Click on the **Reset** field below.
A corresponding display appears as confirmation.

8 Firmware update

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

An update package can be downloaded to the product from the download area on the Pilz website. There are two different file extensions:

- ▶ .fw
- ▶ .fwu

The PITreader web application shows which update package with which file extension should be used for your product.



NOTICE

Update the firmware regularly to obtain security-related updates.

From firmware version 02.02.01 it is also possible to install an older firmware version, in which case please note:

- ▶ Guidelines regarding support for the hardware/firmware versions can be found in the "Product Modifications" description for PITreader.
- ▶ Should the PITreader not function correctly after a downgrade, reset the PITreader to the factory default setting (see [Reset to default settings](#) [ 88]).
- ▶ Pilz only offers support for the current firmware version.
- ▶ Pilz only monitors the current firmware version for security weaknesses.

9 Commissioning, operation

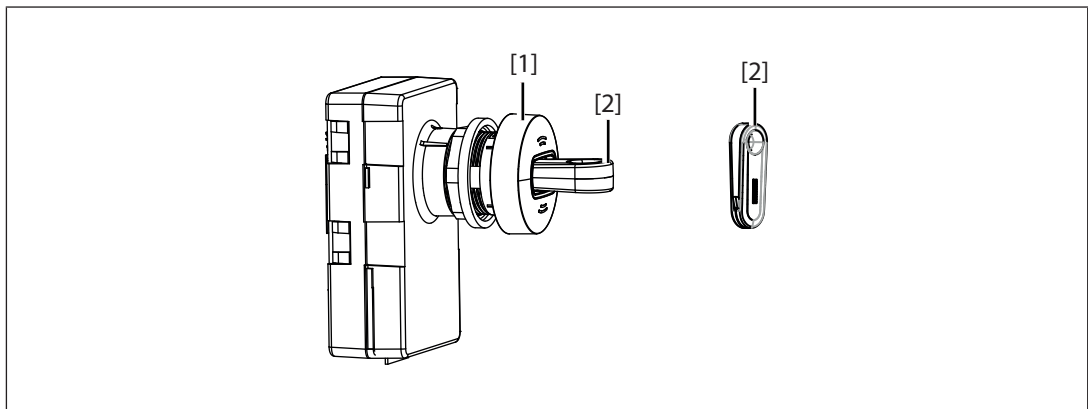
Prerequisites

- ▶ PITreader is installed correctly.
- ▶ PITreader is wired correctly.
- ▶ PITreader is configured correctly.
- ▶ The PITreader firmware has been updated.
- ▶ You have read the chapter on Safety and Security and complied with the requirements.

9.1 Position transponder

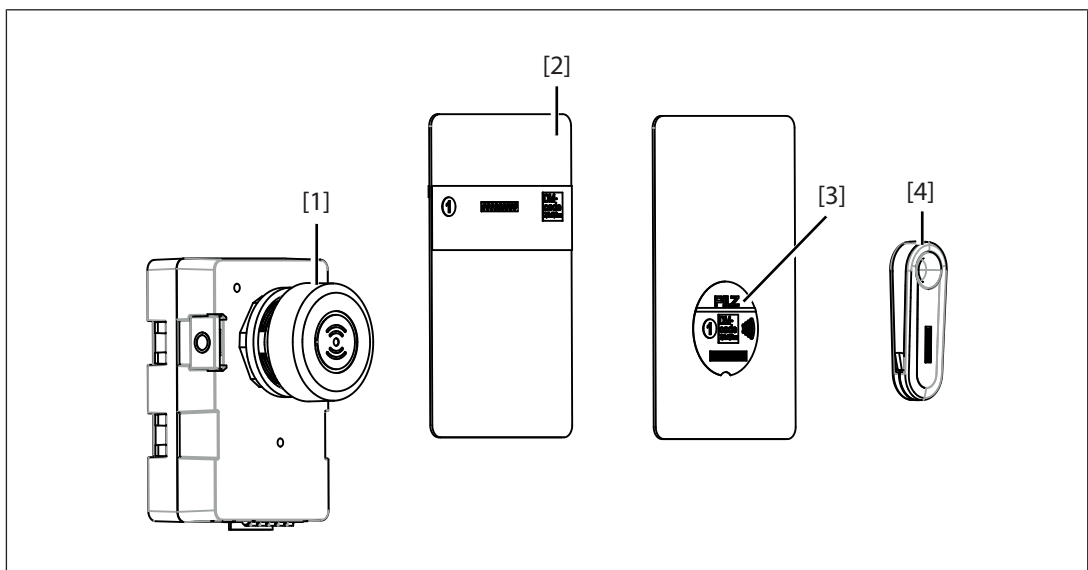
The Pilz transponders are described below. Some transponders from third-party manufacturers may also be used. Further information can be found under [Transponders from third-party manufacturers with selected ISO/IEC standards \(without MIFARE DESFire applications\)](#) [ 34].

9.1.1 PITreader Key



- ▶ Guide the PITreader transponder key [2] into the read head [1], as far as it will go.

9.1.2 PITreader Card

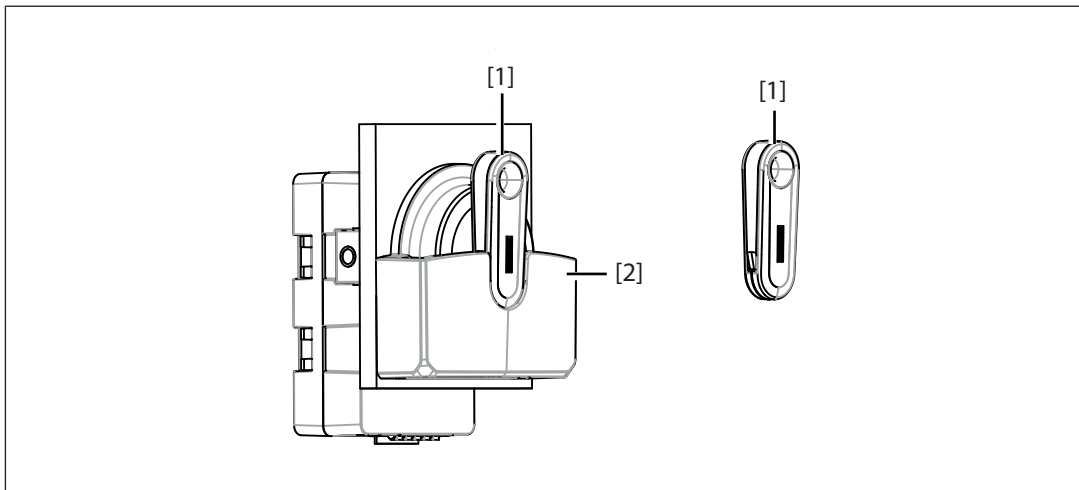


- Hold the PITreader transponder card [2], PITreader transponder sticker [3] or PITreader transponder key [4] in front of the read head [1].

9.1.3 PITreader card holder

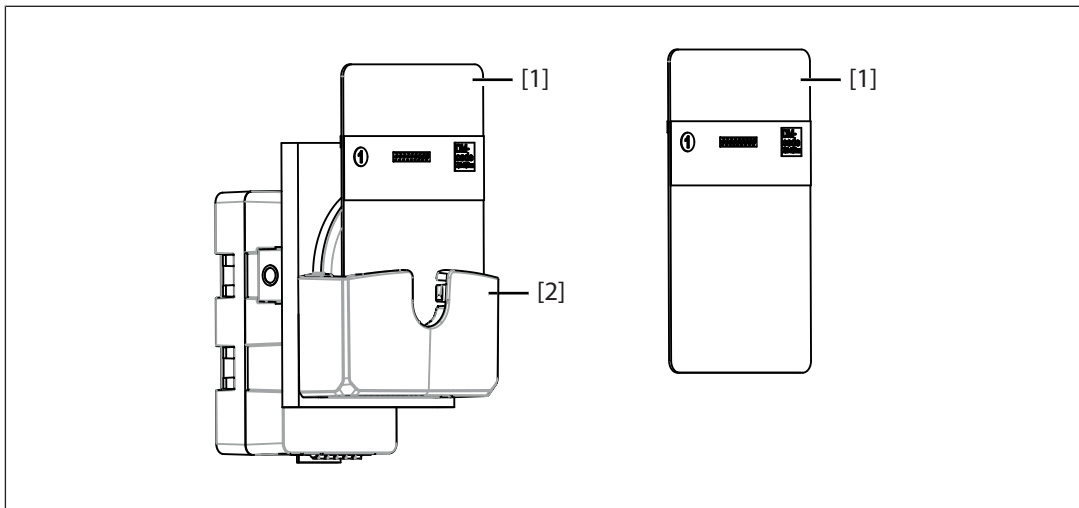
You can use suitable transponders in the PITreader card holder, or also just hold them in front of the read head.

9.1.3.1 PITreader transponder key



- Guide the PITreader transponder key [1] into the PITreader card holder [2] from above, until it locks in position.

9.1.3.2 PITreader transponder card

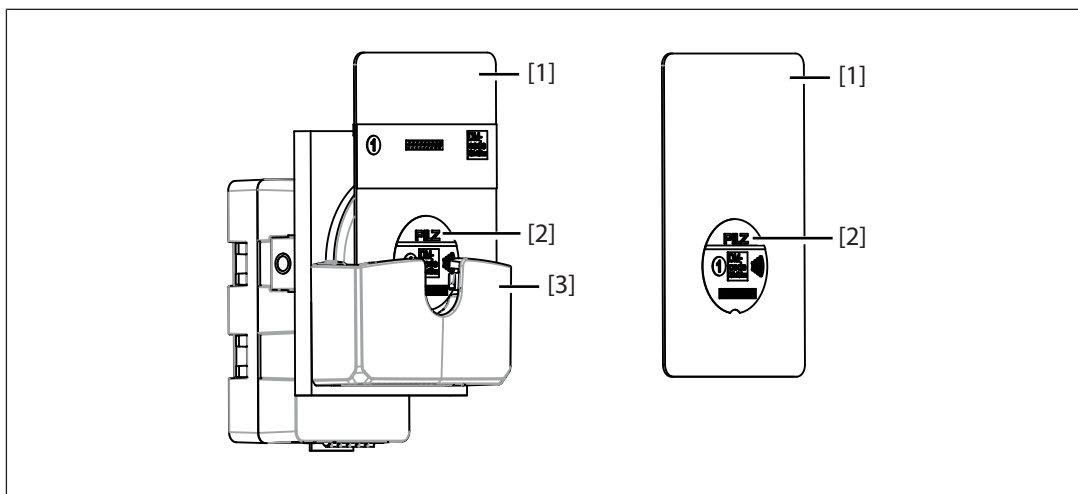


Ensure that only one PITreader transponder card [1] is inserted at a time.

- Guide the PITreader transponder card [1] into the PITreader card holder [2] from above, as far as it will go.

9.1.3.3

PITreader transponder sticker



- Guide the carrier card [1] with the attached PITreader transponder sticker [2] into the PITreader card holder [3] from above, as far as it will go.

9.2

LED indicator

Legend



LED on



LED flashes

Colour	Status	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 Network configuration via Multicast protocol [69]).
Green		Transponder has been recognised as valid.

Colour	Status	Meaning
Green		2-person rule, possible reasons: ▶ The authentication process was started with the first transponder. ▶ 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. Two-factor authentication: ▶ The transponder is valid; a valid PIN must also be entered for authentication.
Red		Transponder has been recognised as invalid Possible reasons: ▶ Transponder in the read area: Authentication is denied (e.g. permission = 0). ▶ No transponder in the read area: Authentication on the device is blocked (e.g. via 24 V I/O port or single authentication). You'll find further information in the web application under Status -> Authentication

Colour	Status	Meaning
Red		Error ► Possible reasons (PITreader Card only): – A transponder from Pilz was not clearly recognised. – Several transponders from Pilz are recognised. – At least one transponder from a third-party manufacturer is recognised. Possible remedies: – Remove transponder from the read area – Position exactly one transponder from Pilz in the read area. Note: Once the fault has been rectified, the fault indicator is deactivated automatically. ► Other reasons (all PITreaders): e.g. hardware error, configuration error, invalid or uncoded transponder, etc. Possible remedies in the event of a configuration error and when the device is no longer accessible under the set IP address: – Try to open the web application with the default IP address or – Reset the device to its factory default settings.

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

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

See also [Reset to default settings](#)  88].

9.3 Personal data

Personal data can be recorded, stored and processed in PITreaders and transponders.

9.3.1 PITreader

Personal data is stored in the PITreader via the web application under

- ▶ **User -> Device user**, see [Device user](#)  70].
- ▶ **Diagnostics -> Log**, see [Data logging with personal data](#)  74].

You can delete all personal data by resetting the configuration to its factory default settings, see [Reset to default settings](#)  88].

9.3.2 Transponder

User data is also stored on the transponder. For information on how to delete user data, see [Delete user data on transponders](#)  84].

9.4 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.

- ▶ 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](#)  97].

9.4.1 Statistics

Various settings for the statistical evaluations can be made in the web application under **Diagnostics -> 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 -> Advanced functions**. 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

Only those permissions that have been used at least once for a successful authentication are listed in the table under **Authenticated permission**.

Statistical values for a permission:

– **Permission**

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

– **Number**

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.

10 Maintenance and testing

It is not necessary to perform maintenance work on the product in normal operation.

- ▶ Please return any faulty product to Pilz.

11 Decommissioning

PITreader and transponders may contain personal data.

- ▶ In the PITreader, reset the configuration to the factory default settings, see [Reset to default settings](#) [ 88].
- ▶ Delete the data on the transponders, see [Delete user data on transponders](#) [ 84].

11.1 Disposal

- ▶ When decommissioning, please comply with local regulations regarding the disposal of electronic devices, such as the Electrical and Electronic Equipment Act.

12 Technical details

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

The technical details of the PITreader base unit (Product ID 402255) and the technical details of the PITreader S base unit (Product ID 402256) are identical.

The technical details of the PITreader card unit (Product ID 402320) and the technical details of the PITreader S card unit (Product ID 402321) are identical.

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

Ethernet interface	402255	402320
Transmission rate	10/100 Mbit/s	10/100 Mbit/s
Times	402255	402320
Supply interruption before de-energisation	10 ms	10 ms
Environmental data	402255	402320
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 SL	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
Mechanical data	402255	402320
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. fixing screws torque settings	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 mm², 24 - 14 AWG	0,2 - 1,5 mm², 24 - 14 AWG
Spring-loaded terminals: Terminal points per connection	1	1

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

Note:

The technical details for the PIT gb with PITreader can be found in the operating manual PIT gb with PITreader.

13 Safety characteristic data

Information on calculating the safety-related characteristic data can be found - depending on the product - in the

- ▶ System description PITmode flex (1005276).
- ▶ System description PITmode flex visu (1005364).
- ▶ System description for the maintenance safeguarding system Key-in-pocket (1006613).
- ▶ Operating manual PIT m4SEU (1004648).

14 Supplementary data

14.1 Radio approvals PITreader Key

FCC/IC approval

USA/Canada

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

FCC/IC-Requirements:

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

Operation is subject to the following two conditions:

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

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

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

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

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

14.2 Radio approvals PITreader Card

FCC/IC approval

USA/Canada

FCC ID: VT8- PITRD11
IC: 7482A- PITRD11

FCC/IC-Requirements:

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

Operation is subject to the following two conditions:

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

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

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

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

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

14.3 Network data

Protocol	Direction [*]	Transport protocol (IP version)	Port no.	Can be deactivated	Time-critical	Description
HTTP	In	TCP	1 ... 65535 Default: 80	Yes	No	Web application: Communication with a browser. Browser is always redirected to HTTPS
HTTPS	in	TCP	1 ... 65535 Default: 443	No	No	Web application: Secured communication with a browser. Transport protection by TLSv1.2. Access to the web application via user name and password. The web server is authenticated via an X.509 certificate.
Modbus TCP	in	TCP	1 ... 65535 Default: 502	Yes Default: inactive	No	Modbus/TCP Server
NTP	Out	UDP	1 ... 65535 Default: 123	Yes Default: inactive	No	SNTP-Client
OPC UA	in	TCP	4840	Yes Default: inactive	No	PITreader OPC Server UA
mDNS	in	UDP	5353	Yes	No	Network discovery with Multicast DNS (224.0.0.251)
Multicast configuration	in	UDP	7075	Yes	No	Network configuration via Multicast protocol (239.255.0.12)

*

in: the communication partner starts communication with the device.

out: the device starts communication with the communication partner.

14.4 Overview of permissions

Permission	Code	
	Hexadecimal	Decimal
0	0x00000000	0
1	0x000001ff	511
2	0x00003e0f	15887

Permission	Code	
	Hexadecimal	Decimal
3	0x00003ff0	16368
4	0x0001c633	116275
5	0x0001c7cc	116684
6	0x0001f83c	129084
7	0x0001f9c3	129475
8	0x00064a55	412245
9	0x00064baa	412586
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

Permission	Code	
	Hexadecimal	Decimal
39	0x0031b5a9	3257769
40	0x0036063f	3540543
41	0x003607c0	3540928
42	0x00363830	3553328
43	0x003639cf	3553743
44	0x0037c00c	3653644
45	0x0037c1f3	3654131
46	0x0037fe03	3669507
47	0x0037fffc	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

15 Order reference

15.1 Authentication system PITreader Key

Product type	Features	Product ID
PITreader base unit	RFID authentication system Contents: Base unit, connector [402307] Required accessories: PITreader key adapter	402255
PITreader S base unit	RFID authentication system with extended function range, Contents: Base unit, connector [402307] Required accessories: PITreader key adapter	402256
PITreader key Adapter h	1x PITreader key adapter horizontal + 1x nut for PITreader base unit	402308

15.2 Authentication system PITreader Card

Product type	Features	Product ID
PITreader card unit	RFID authentication system for cards, stickers & keys Contents: Base unit, connector [402307], PITreader card Adapter	402320
PITreader S card unit	RFID authentication system for cards, stickers & keys, with advanced function range Contents: Base unit, connector [402307], PITreader card Adapter	402321

15.3 Transponder key

Product type	Features	Product ID
PITreader key ye g	Transponder key for authentication system PITreader, permissions freely configurable Colour: yellow Material: plastic	402260
PITreader key ye g bk	Generic transponder key for authentication system PITreader, permissions freely configurable Colour: black Material: plastic	402260BK
PITreader key ye g bl	Generic transponder key for authentication system PITreader, permissions freely configurable Colour: blue Material: plastic	402260BL
PITreader key ye g gn	Generic transponder key for authentication system PITreader, permissions freely configurable Colour: green Material: plastic	402260GN
PITreader key ye g rd	Generic transponder key for authentication system PITreader, permissions freely configurable Colour: red Material: plastic	402260RD

Product type	Features	Product ID
PITreader key ye g wt	Generic transponder key for authentication system PITreader, permissions freely configurable Colour: white Material: plastic	402260WT
PITreader key ye g ye	Generic transponder key for authentication system PITreader, permissions freely configurable Colour: light yellow Material: plastic	402260YE
PITreader key ye 1	Transponder key for authentication system PITreader, permission for operating mode 1 Colour: yellow Material: plastic	402261
PITreader key ye 2	Transponder key for authentication system PITreader, permission for operating mode 1 and 2 Colour: yellow Material: plastic	402262
PITreader key ye 3	Transponder key for authentication system PITreader, permission for operating mode 1, 2 and 3 Colour: yellow Material: plastic	402263
PITreader key ye 4	Transponder key for authentication system PITreader, permission for operating mode 1, 2, 3 and 4 Colour: yellow Material: plastic	402264
PITreader key ye 5	Transponder key for authentication system PITreader, permission for operating mode 1, 2, 3, 4 and 5 Colour: yellow 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) Colour: yellow Material: plastic	402269

15.4 Transponder cards

Product type	Features	Product ID
PITreader card ye g	Transponder card for authentication system PITreader Card, permissions freely configurable Colour: yellow Material: plastic	402330
PITreader card ye 1	Transponder card for authentication system PITreader Card, permission for operating mode 1 Colour: yellow Material: plastic	402331
PITreader card ye 2	Transponder card for authentication system PITreader Card, permission for operating mode 1 and 2 Colour: yellow Material: plastic	402332

Product type	Features	Product ID
PITreader card ye 3	Transponder card for authentication system PITreader Card, permission for operating mode 1, 2 and 3 Colour: yellow Material: plastic	402333
PITreader card ye 4	Transponder card for authentication system PITreader Card, permission for operating mode 1, 2, 3 and 4 Colour: yellow Material: plastic	402334
PITreader card ye 5	Transponder card for authentication system PITreader Card, permission for operating mode 1, 2, 3, 4 and 5 Colour: yellow 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) Colour: yellow Material: plastic	402339

15.5 Transponder sticker

Product type	Features	Product ID
PITreader sticker ye g	Transponder sticker for authentication system PITreader Card, permissions freely configurable Colour: yellow Material: plastic	402340
PITreader sticker ye 1	Transponder sticker for authentication system PITreader Card, permission for operating mode 1 Colour: yellow Material: plastic	402341
PITreader sticker ye 2	Transponder sticker for authentication system PITreader Card, permission for operating mode 1 and 2 Colour: yellow Material: plastic	402342
PITreader sticker ye 3	Transponder sticker for authentication system PITreader Card, permission for operating mode 1, 2 and 3 Colour: yellow Material: plastic	402343
PITreader sticker ye 4	Transponder sticker for authentication system PITreader Card, permission for operating mode 1, 2, 3 and 4 Colour: yellow Material: plastic	402344
PITreader sticker ye 5	Transponder sticker for authentication system PITreader Card, permission for operating mode 1, 2, 3, 4 and 5 Colour: yellow 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) Colour: yellow Material: plastic	402349

15.6 Accessories

Product type	Features	Product ID
PIT es wrench	Installation wrench for PIT es pushbutton	400222
PITreader card holder	Plastic holder for PITreader (S) card [402320/21] for transponder cards and transponder keys as an optional accessory	402323

16 **EC declaration of conformity**

This product/these products meet(s) 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.

Representative: Pilz GmbH & Co. KG, Felix-Wankel-Str. 2, 73760 Ostfildern, Germany

17 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.

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

Support

Technical support is available from Pilz round the clock.

Americas

Brazil

+55 11 97569-2804

Canada

+1 888 315 7459

Mexico

+52 55 5572 1300

USA (toll-free)

+1 877-PILZUSA (745-9872)

Asia

China

+86 400-088-3566

Japan

+81 45 471-2281

South Korea

+82 31 778 3390

Australia and Oceania

Australia

+61 3 95600621

New Zealand

+64 9 6345350

Europe

Austria

+43 1 7986263-444

Belgium, Luxembourg

+32 9 3217570

France

+33 3 88104003

Germany

+49 711 3409-444

Ireland

+353 21 4804983

Italy, Malta

+39 0362 1826711

Scandinavia

+45 74436332

Spain

+34 938497433

Switzerland

+41 62 88979-32

The Netherlands

+31 347 320477

Türkiye

+90 216 5775552

United Kingdom

+44 1536 460866

You can reach our international hotline on:

+49 711 3409-222

support@pilz.com

Reporting security vulnerabilities or security incidents

If you would like to report a security vulnerability or a security incident in connection with a Pilz product, please contact our **Pilz Product Security Incident Response Team (PSIRT)**.

You can reach us at: www.pilz.com/psirt

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



www.pilz.com/facebook



www.pilz.com/linkedin



www.pilz.com/xing



www.pilz.com/youtube



CECE, CHRE, CMSE®, IndustrialPI®, Leansafe®, MYZEL®, PAS4000®, PAScale®, PASconfig®, Pilz®, PIR®, PMCPrimo®, PMCProtego®, PMCTendo®, PMD®, PMV®, PNOZ®, Primo®, PSN®, PSS®, PVS®, PVS®, PVS®, SafetyBUS p®, SafetyNET p®, THE SPIRIT OF SAFETY® are registered and protected trademarks of Pilz GmbH & Co. KG in some countries. We would point out that product features may vary from the details stated in this document, depending on the status at the time of publication and the scope of the equipment. We accept no responsibility for the validity, accuracy and entirety of the text and graphics presented in this information. Please contact our Technical Support if you have any questions.

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

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

PILZ
THE SPIRIT OF SAFETY