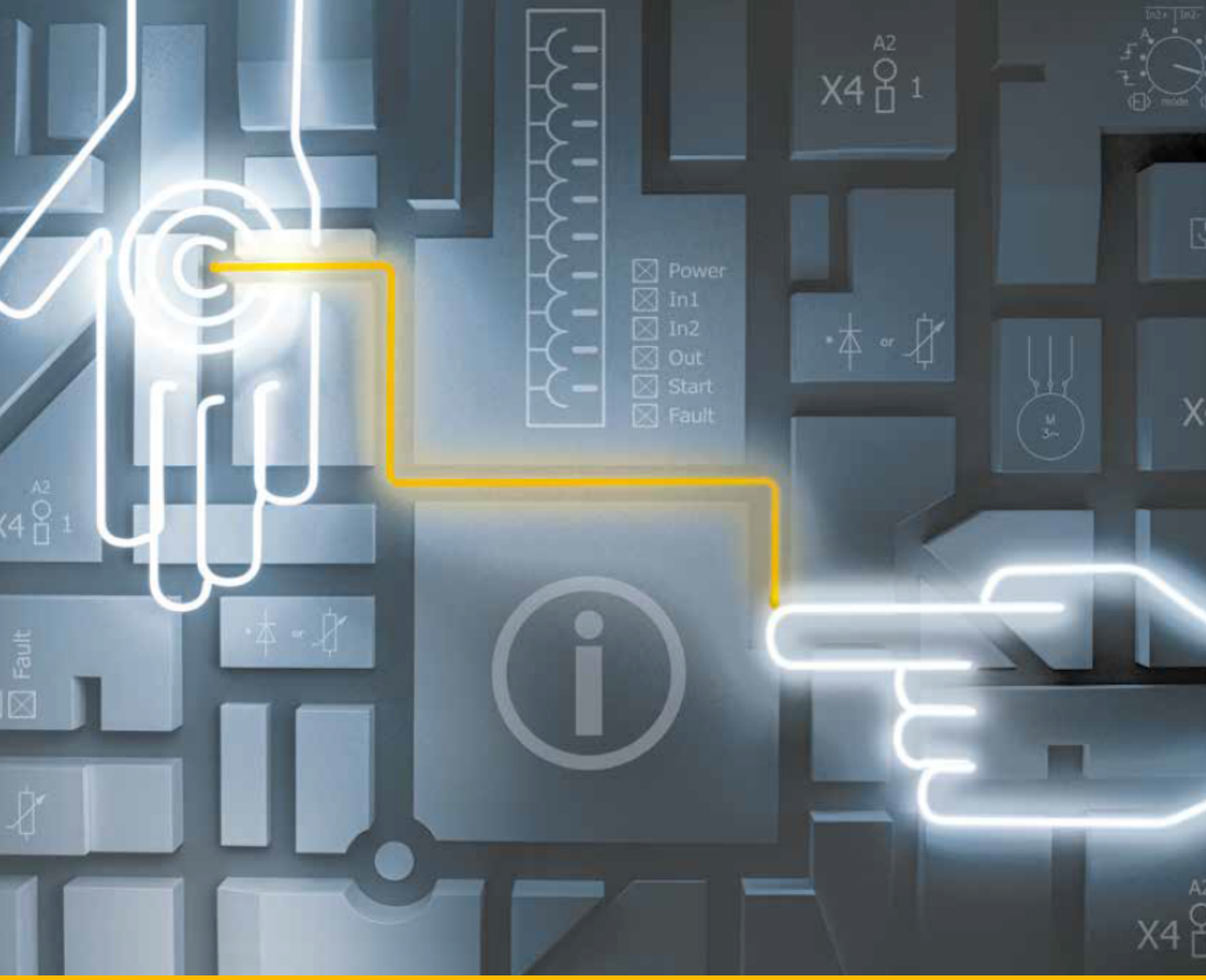


PITreader
PITreader Firmware-Version 02.03.xx

PILZ
THE SPIRIT OF SAFETY

Bedienungsanleitung-1004806-DE-17
- Befehls- und Meldegeräte




Dieses Dokument ist das Originaldokument.

Wo unvermeidbar, wurde aus Gründen der besseren Lesbarkeit die männliche Sprachform bei der Formulierung dieses Dokuments gewählt. Es wird versichert, dass alle Personen diskriminierungsfrei und gleichberechtigt betrachtet werden.

1 Einführung

1.1 Gültigkeit der Dokumentation

Die Dokumentation ist gültig für das Produkt PITreader. Sie gilt, bis eine neue Dokumentation erscheint.

Diese Bedienungsanleitung erläutert die Funktionsweise und den Betrieb, beschreibt die Montage und gibt Hinweise zum Anschluss des Produkts.

1.2 Nutzung der Dokumentation

Dieses Dokument dient der Instruktion. Installieren und nehmen Sie das Produkt nur dann in Betrieb, wenn Sie dieses Dokument gelesen und verstanden haben. Bewahren Sie das Dokument für die künftige Verwendung auf.

1.3 Verwendete Begriffe

PITreader

Unter der Bezeichnung "PITreader" sind alle RFID-Authentifizierungssysteme der PILZ GmbH & Co. KG zusammengefasst, bei denen die Authentifizierung über einen Transponder erfolgt.

Als Transponder können z. B. verwendet werden:

- PITreader Transponder-Schlüssel
- PITreader Transponder-Karten
- PITreader Transponder-Sticker

Die Bezeichnung "PITreader" wird immer dann verwendet, wenn die Beschreibung für alle Produktvarianten gültig ist.

Beachten Sie: Die Produkte der Produktfamilie PSEN cs fallen NICHT unter die Bezeichnung PITreader.

PITreader Key

Unter der Bezeichnung "PITreader Key" sind alle Produktvarianten des PITreaders zusammengefasst, bei denen ausschließlich ein PITreader Transponder-Schlüssel zur Authentifizierung verwendet werden kann. Dazu wird der PITreader Transponder-Schlüssel in den Lesekopf eingesteckt.

Eine Produktvariante ist z. B. PITreader S base unit.

Die Bezeichnung "PITreader Key" wird immer dann verwendet, wenn die Beschreibung ausschließlich für diese Produktvarianten gültig ist.

PITreader Card

Unter der Bezeichnung "PITreader Card" sind alle Produktvarianten des PITreaders zusammengefasst, bei denen folgende Transponder zur Authentifizierung verwendet werden können:

- PITreader Transponder-Karte
- PITreader Transponder-Sticker

- PITreader Transponder-Schlüssel

Dazu wird der PITreader Transponder vor den Lesekopf gehalten.

Eine Produktvariante ist z. B. PITreader S card unit.

Die Bezeichnung "PITreader Card" wird immer dann verwendet, wenn die Beschreibung ausschließlich für diese Produktvarianten gültig ist.

PIT gb mit PITreader

Unter der Bezeichnung "PIT gb mit PITreader " sind alle Produktvarianten der PITgatebox mit PITreader zusammengefasst, hier gibt es die beiden Produktvarianten PIT gb mit PITreader Key und PIT gb mit PITreader Card.

Die Bezeichnung "PIT gb mit PITreader " wird immer dann verwendet, wenn die Beschreibung ausschließlich für diese Produktvarianten gültig ist.

1.4 Zeichenerklärung

Besonders wichtige Informationen sind wie folgt gekennzeichnet:

GEFAHR!

Beachten Sie diesen Hinweis unbedingt! Er warnt Sie vor unmittelbar drohenden Gefahren, die schwerste Körperverletzungen und Tod verursachen können, und weist auf entsprechende Vorsichtsmaßnahmen hin.

WARNUNG!

Beachten Sie diesen Hinweis unbedingt! Er warnt Sie vor gefährlichen Situationen, die schwerste Körperverletzungen und Tod verursachen können, und weist auf entsprechende Vorsichtsmaßnahmen hin.

ACHTUNG!

weist auf eine Gefahrenquelle hin, die leichte oder geringfügige Verletzungen sowie Sachschaden zur Folge haben kann, und informiert über entsprechende Vorsichtsmaßnahmen.

WICHTIG

beschreibt Situationen, durch die das Produkt oder Geräte in dessen Umgebung beschädigt werden können, und gibt entsprechende Vorsichtsmaßnahmen an. Der Hinweis kennzeichnet außerdem besonders wichtige Textstellen.

INFO

liefert Anwendungstipps und informiert über Besonderheiten.

2 Übersicht

Das Produkt kann mit den folgenden externen Komponenten/Systemen eingesetzt werden:

- Transponder zur Authentifizierung
- Web-Anwendung auf einem PC zur Konfiguration
- Bedienterminal (HMI) zur Authentifizierung
- Sicherheitssteuerung (FS-PLC) zur sicheren Betriebsartenwahl oder Authentifizierung
- Sichere Auswerteeinheit (z. B. PIT m4SEU, Artikelnummer 402250) zur sicheren Betriebsartenwahl (nur bei PITreader Key und PITreader Card)

2.1 Gerätemerkmale

- System zur Authentifizierung und Autorisierung an Steuerungssystemen
- Die Authentifizierung erfolgt über Transponder (Transponder-Karten, Transponder-Sticker und/oder Transponder-Schlüssel)
- Konfigurierbar über eine Web-Anwendung
- Ethernet-Schnittstelle für Modbus/TCP
- LED zur Anzeige des Gerätezustands

Unterscheidungsmerkmale

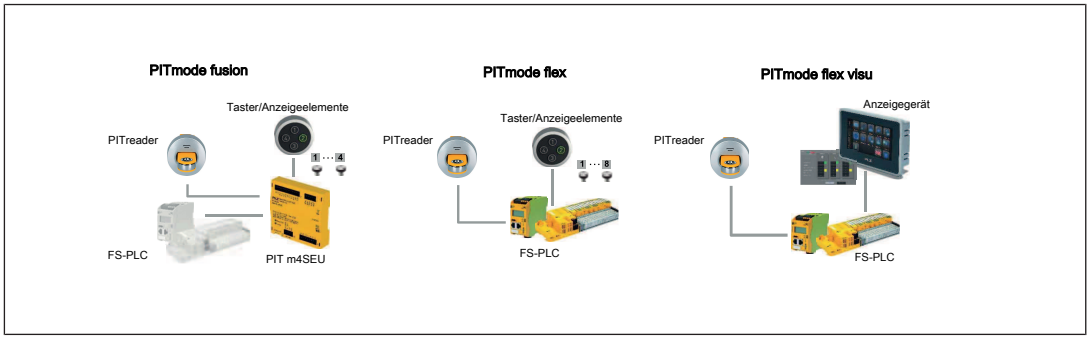
Gerätemerkmal	PITreader Key	PITreader Card	PIT gb mit PITreader Key	PIT gb mit PITreader Card
Transponder				
Transponder-Schlüssel	♦	♦	♦	♦
Transponder-Karten	---	♦	---	♦
Transponder-Sticker	---	♦	---	♦
PITreader card holder	---	♦	---	♦
Integrierter OPC UA-Server	PITreader S base unit	PITreader S card 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
Transponder von Fremdherstellern mit MIFARE DESFire-Anwendungen	---		---	
Schnittstelle für den Anschluss einer PIT-m4SEU	♦	♦	---	---
Basiseinheit für Einbauöffnung D22 (Durchmesser 22,3 mm) mit Verdrehsicherung	♦	♦	---	---

2.2 Systemübersichten mit PITreader

2.2.1 Zugangssystem

Der PITreader kann zur Authentifizierung an einer beliebigen Steuerung/SPS oder einem HMI eingesetzt werden.

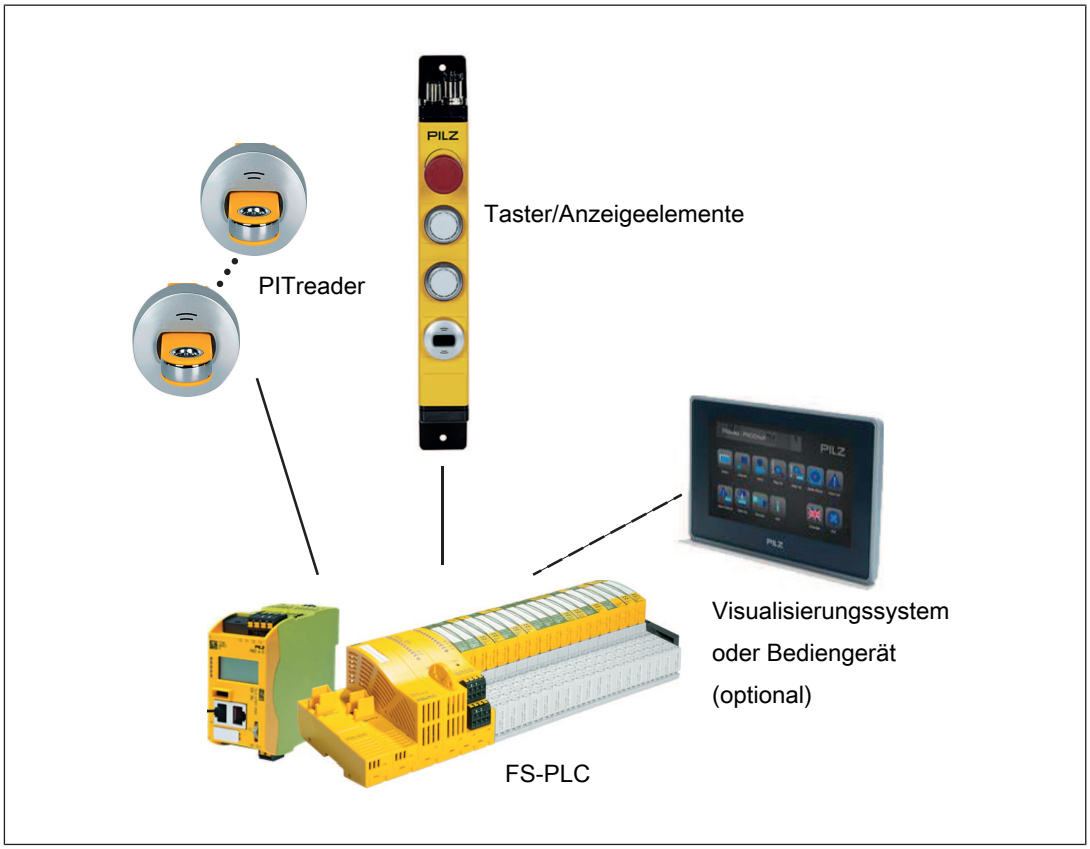
2.2.2 Systeme zur sicherheitsgerichteten Betriebsartenwahl



Weitere Informationen finden Sie für

- PITmode fusion in der Bedienungsanleitung PIT m4SEU (1004648).
- PITmode flex in der Systembeschreibung PITmode flex (1005276).
- PITmode flex visu in der Systembeschreibung PITmode flex visu (1005364).

2.2.3 Zugangssystem für die Wartungssicherung Key-in-pocket



Weitere Informationen finden Sie in der Systembeschreibung Wartungssicherung Key-in-pocket (1006613.

2.3 Geräteansichten

2.3.1 Geräteansicht PITreader Key

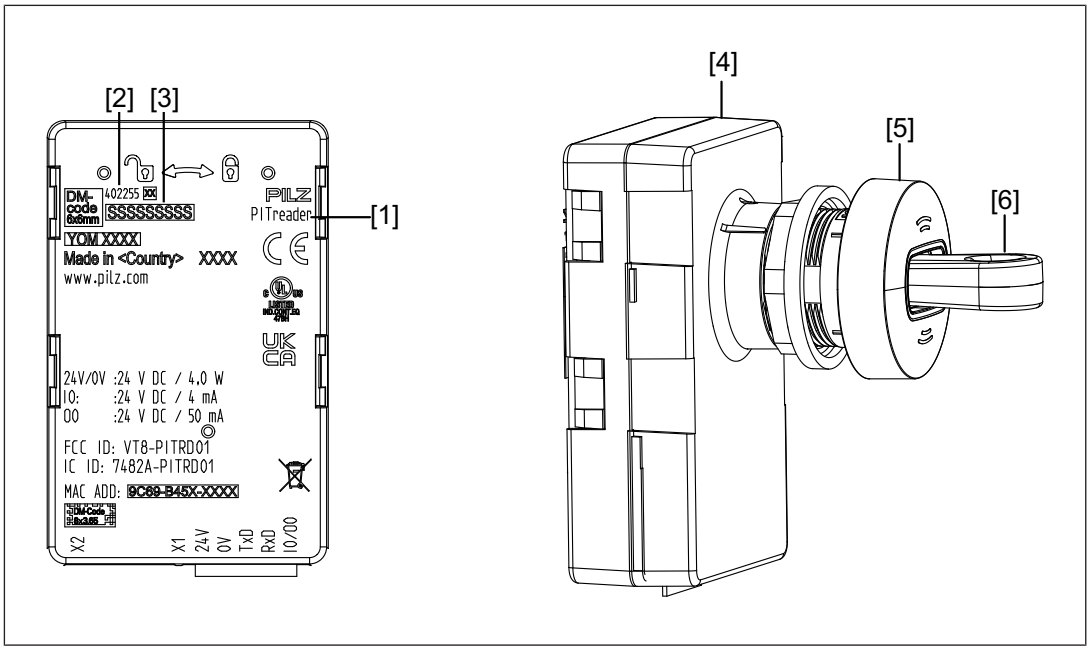


Abb.: Geräteansicht PITreader Key am Beispiel PITreader base unit

Legende

X1 Spannungsversorgung, 24 V Ein-/Ausgang und Anschluss einer sicheren Auswerteeinheit (PIT m4SEU)

X2 Ethernet-Schnittstelle

[1] Gerätebezeichnung

[2] Artikelnummer

[3] Seriennummer

[4] Basiseinheit (Artikelnummer 402255 oder 402256), inklusive Federkraftklemme (402307)

[5] Lesekopf PITreader key Adapter h (Artikelnummer 402308)

(nicht im Lieferumfang der Basiseinheit enthalten, siehe auch Bestelldaten [111])

[6] Transponder-Schlüssel (siehe auch Transponder [29] und Bestelldaten [111])

2.3.2 Geräteansicht PITreader Card

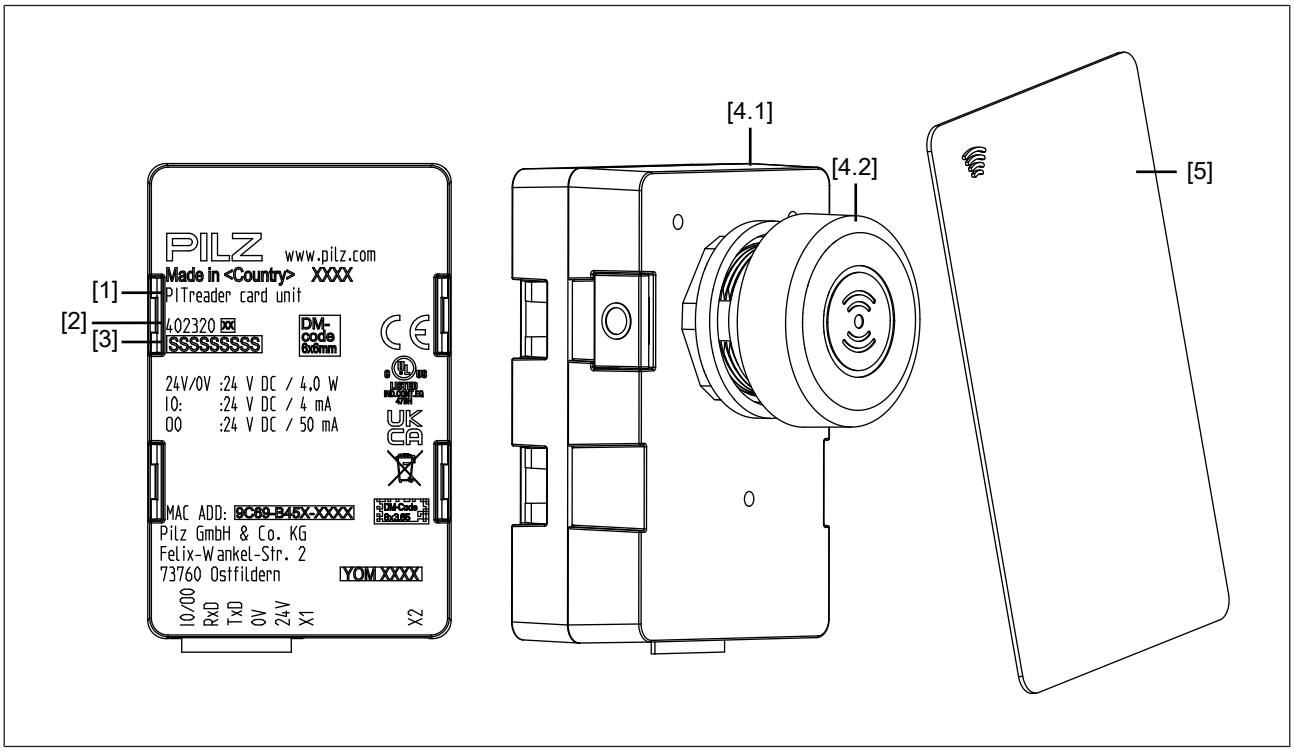


Abb.: Geräteansicht PITreader Card mit Transponder-Karte am Beispiel PITreader card unit

Legende

X1 Spannungsversorgung, 24 V Ein-/Ausgang und Anschluss einer sicheren Auswerteeinheit (PIT m4SEU)

X2 Ethernet-Schnittstelle

[1] Gerätebezeichnung

[2] Artikelnummer

[3] Seriennummer

[4.1] Basiseinheit (Artikelnummer 402320 oder 402321), inklusive Federkraftklemme (402307)

[4.2] Lesekopf mit Silikonkappe PITreader card cap
(im Lieferumfang der Basiseinheit enthalten, siehe auch Bestelldaten [📖 111])

[5] Transponder (hier z. B. Transponder-Karte)
(siehe auch Transponder [📖 29] und Bestelldaten [📖 111])

2.3.3 Geräteansicht PIT gb mit PITreader

Sie finden die erforderlichen Informationen in der Bedienungsanleitung PIT gb mit PITreader.

2.3.4 Ansicht PITreader Transponder-Schlüssel

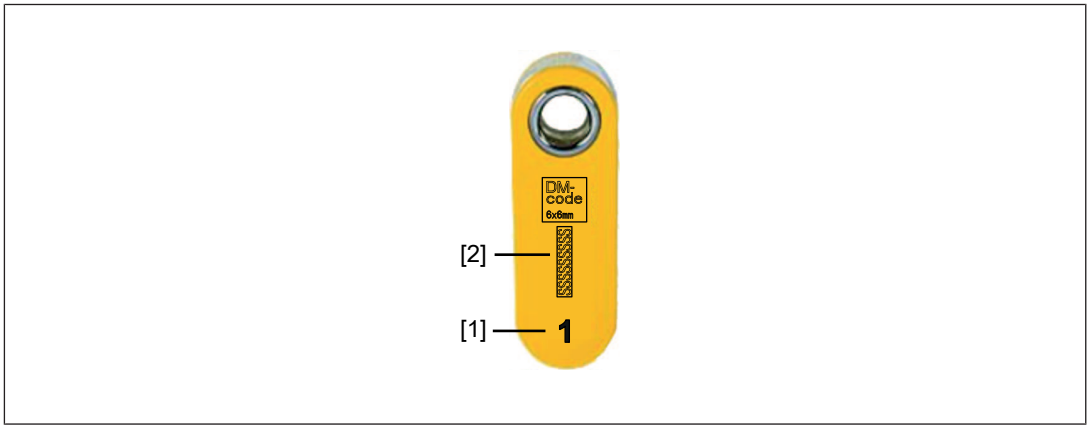


Abb.: Schlüsselansicht am Beispiel PITreader key ye 1

Legende

[1] Berechtigung
(siehe auch Berechtigung eines Transponders [📖 29] und Bestelldaten [📖 111])

[2] Seriennummer

2.3.5 Ansicht PITreader Transponder-Karte

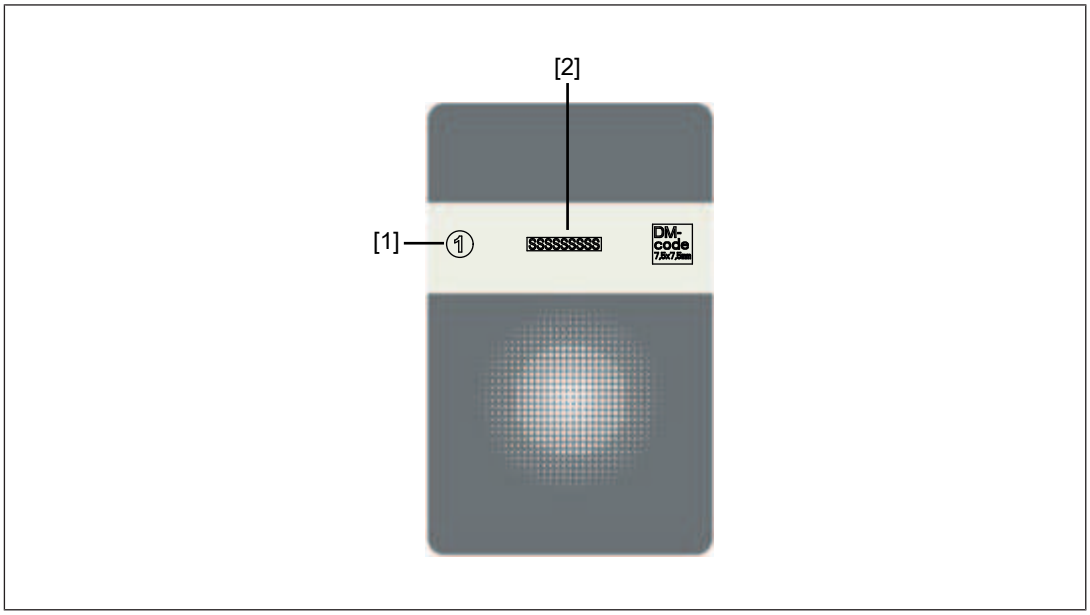


Abb.: Kartenansicht am Beispiel PITreader card ye 1

Legende

[1] Berechtigung
(siehe auch Berechtigung eines Transponders [📖 29] und Bestelldaten [📖 111])

[2] Seriennummer

2.3.6 Ansicht PITreader Transponder-Sticker

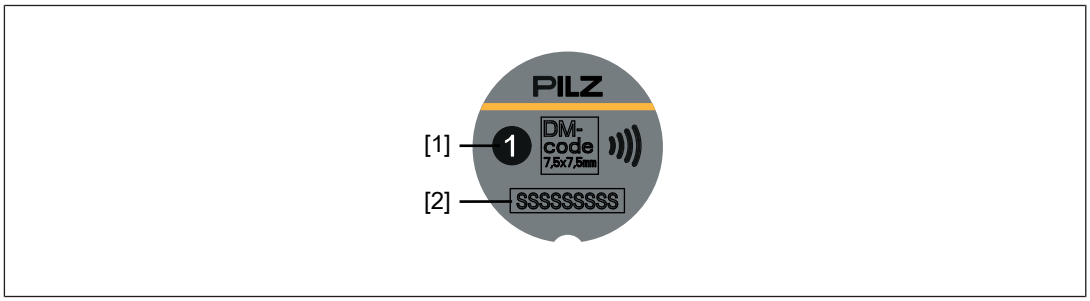


Abb.: Sticker-Ansicht am Beispiel PITreader sticker ye 1

Legende

[1] Berechtigung
(siehe auch Berechtigung eines Transponders [29] und Bestelldaten [111])

[2] Seriennummer

3 Sicherheit

3.1 Bestimmungsgemäße Verwendung

Der PITreader ist ein System zur Authentifizierung und Autorisierung an Steuerungssystemen. Die Authentifizierung erfolgt über RFID-Transponder.

Das Produkt ist für die Anwendung in der Industrieumgebung bestimmt.

Nicht bestimmungsgemäße Verwendung

Als nicht bestimmungsgemäß gilt insbesondere:

- jegliche bauliche, technische oder elektrische Veränderung des Produkts,
- ein Einsatz des Produkts außerhalb der Bereiche, die in dieser Bedienungsanleitung beschrieben sind,
- ein von den technischen Daten (siehe Technische Daten [📖 103]) abweichender Einsatz des Produkts.

WICHTIG

EMV-gerechte elektrische Installation

Das Produkt ist für die Anwendung in der Industrieumgebung bestimmt. Das Produkt kann bei Installation in anderen Umgebungen Funkstörungen verursachen. Ergreifen Sie bei der Installation in anderen Umgebungen Maßnahmen, um die für den jeweiligen Installationsort gültigen Normen und Richtlinien bezüglich Funkstörungen einzuhalten.

3.1.1 Fremdhersteller-Lizenzinformationen

Im Produkt ist Open Source-Software enthalten, deren Nutzungsbedingungen den Einsatzbereich des Produkts zusätzlich einschränken können. Bitte beachten Sie unbedingt die Fremdhersteller-Lizenzinformationen.

Nähere Informationen erhalten Sie, indem Sie in der Web-Anwendung des PITreader das Menü ***Support -> Rechtliche Informationen anzeigen*** aufrufen.

3.2 Sicherheitsvorschriften

3.2.1 Zusätzlich geltende Dokumente

Lesen und beachten Sie auch folgende Dokumente:

- Bedienungsanleitung PITreader REST API (1005365)
- Bedienungsanleitung PITreader OPC Server UA (1005480)
- Bei Verwendung einer PIT gb mit PITreader:
  Bedienungsanleitung PIT gb mit PITreader (1005249)
- Bei Verwendung einer sicheren Auswerteeinheit PIT m4SEU:
  Bedienungsanleitung PIT m4SEU (1004648)

- Für Informationen zur Berechnung von sicherheitstechnischen Kenndaten:
  - Systembeschreibung PITmode flex (1005276)
  - Systembeschreibung PITmode flex visu (1005364)
  - Systembeschreibung Wartungssicherung Key-in-pocket (1006613)

3.2.2 Qualifikation des Personals

Aufstellung, Montage, Programmierung, Inbetriebnahme, Betrieb, Außerbetriebnahme und Wartung der Produkte dürfen nur von hierzu befähigten Personen vorgenommen werden.

Eine befähigte Person ist eine qualifizierte und sachkundige Person, die durch ihre Berufsausbildung, ihre Berufserfahrung und ihre zeitnahe berufliche Tätigkeit über die erforderlichen Fachkenntnisse verfügt. Um Produkte, Geräte, Systeme, Maschinen und Anlagen prüfen, beurteilen und handhaben zu können, muss diese Person Kenntnisse über den Stand der Technik und die zutreffenden nationalen, europäischen und internationalen Gesetze, Richtlinien und Normen haben.

Der Betreiber ist außerdem verpflichtet, nur Personen einzusetzen, die

- mit den grundlegenden Vorschriften zur Arbeitssicherheit und Unfallverhütung vertraut sind,
- den Abschnitt Sicherheit in dieser Beschreibung gelesen und verstanden haben und
- mit den für die spezielle Anwendung geltenden Grund- und Fachnormen vertraut sind.

3.2.3 Gewährleistung und Haftung

Gewährleistungs- und Haftungsansprüche gehen verloren, wenn

- das Produkt nicht bestimmungsgemäß verwendet wurde,
- die Schäden auf Nichtbeachtung der Bedienungsanleitung zurückzuführen sind,
- das Betreiberpersonal nicht ordnungsgemäß ausgebildet ist,
- oder Veränderungen irgendeiner Art vorgenommen wurden (z. B. Austauschen von Bauteilen auf den Leiterplatten, Lötarbeiten usw).

4 Security

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht.
Führen Sie eine Risikoanalyse gemäß VDI/VDE 2182 oder IEC 62443-3-2 durch und planen Sie die Security-Maßnahmen sorgfältig. Lassen Sie sich ggf. durch den Pilz Customer Support beraten.

4.1 Implementierte Security-Maßnahmen

- Die Web-Anwendung ist durch Kennwortabfrage vor unbefugtem Zugriff geschützt.
- Das Kennwort wird verschlüsselt gespeichert.
- Bei der Änderung eines Kennworts wird das alte Kennwort zur Authentifizierung abgefragt.
- Abwehr von CSRF-Angriffen (Cross-Site-Request-Forgery) durch eindeutige Zuordnung einer Sitzung zu einem Token.
- Ein Anwender wird bei Inaktivität nach 15 Minuten Sitzungsdauer automatisch von der Web-Anwendung abgemeldet.

4.2 Erforderliche Security-Maßnahmen

- Das Produkt ist nicht geschützt vor physischer Manipulation. Wir empfehlen deshalb, das Produkt in einem abschließbaren Schaltschrank oder einem Bedienpanel zu montieren. Eine sichere Auswerteeinheit PIT m4SEU darf nur über die Klemmen TxD/RxD im Inneren eines Schaltschrankes oder Bedienpanels verbunden werden.
- Der Konfigurationsrechner, der auf das Produkt zugreift, muss durch eine Firewall oder andere geeignete Maßnahmen gegen Angriffe geschützt werden. Es wird empfohlen, einen Virenscanner auf diesem Konfigurationsrechner einzusetzen und diesen regelmäßig zu aktualisieren.
- Schützen Sie den Konfigurationsrechner und gegebenenfalls das Produkt vor unbefugter Benutzung durch die Vergabe von Kennwörtern und gegebenenfalls weitere Maßnahmen. Es wird zusätzlich empfohlen, dass der an diesem Konfigurationsrechner angemeldete Anwender nicht die Administrator-Rechte besitzt.
- Schützen Sie das Produkt vor unbefugtem Datenaustausch über das Netzwerk, indem Sie eine Firewall verwenden oder andere geeignete Maßnahmen vorsehen. Erlauben Sie ausschließlich den Datenaustausch, der für die Anwendung erforderlich ist. Jeglicher Datenaustausch, der für die Anwendung nicht erforderlich ist, muss durch die Firewall verhindert werden.
- Vergeben Sie ausschließlich starke Kennwörter und handhaben Sie die Kennwörter sorgfältig. Orientieren Sie sich an allgemein anerkannten Richtlinien wie beispielsweise der NIST 800-63b.
- Beschränken Sie Modbus/TCP-Verbindungen auf das maschineninterne Netzwerk. Sichern Sie die Verbindung gegenüber externen Netzwerken ab.
- Behandeln Sie einen API-Token mit derselben Sorgfalt wie ein Kennwort. Sie finden Anforderungen an Kennwörter in der Bedienungsanleitung des PITreaders.

- Installieren Sie zeitnah Firmware-Updates, die von Pilz für das Produkt zur Verfügung gestellt werden.
- Bewahren Sie die Transponder an einem sicheren Ort auf und schützen Sie sie vor unbefugten Zugriffen. Weisen Sie die Anwender auf die Sicherheitsrisiken durch die Weitergabe von Transpondern hin.
- Bei einem Werksreset wird auch die Codierung im Gerät zurückgesetzt. Dadurch werden an diesem Gerät wieder nicht oder anders codierte Transponder akzeptiert. Wir empfehlen deshalb, in einer übergelagerten Steuerung, einer HMI oder Auswerteeinheit die Prüfsumme der Codierung zu überwachen.
- Protokolldaten können personenbezogene Daten enthalten. Legen Sie exportierte Protokolle nur auf einem ausreichend gesicherten Speichermedium ab.
- Bei einem Netzwerkscan über Multicast DNS kann die Seriennummer des Produkts auch ohne Authentifizierung ausgelesen werden. Vergeben Sie in der Web-Anwendung unbedingt ein eigenes Kennwort, das vom Default-Kennwort abweicht.
- Die Synchronisation der Echtzeituhr im Gerät über SNTP enthält keine Security-Mechanismen zur Absicherung gegen Angriffe durch Unberechtigte (z. B. Spoofing des konfigurierten SNTP-Servers). Sichern Sie die Echtzeituhr im Gerät applikationsseitig durch eine entsprechende Firewall-Konfiguration oder die Nutzung eines eigenen lokalen Zeitservers innerhalb des Maschinennetzwerks ab.
- Die Konfigurations-Sicherungsdatei eines Produkts enthält Informationen zur Authentifizierung am Produkt. Legen Sie die Sicherungsdatei nur auf einem ausreichend gesicherten Speichermedium ab.
- Vor der Entsorgung muss das Produkt sicher außer Betrieb gesetzt werden. Dazu müssen alle Daten vom Gerät gelöscht werden.
  - Setzen Sie die Konfiguration auf Werkseinstellungen zurück oder löschen Sie die Konfiguration.
  - Schalten Sie das Produkt aus.

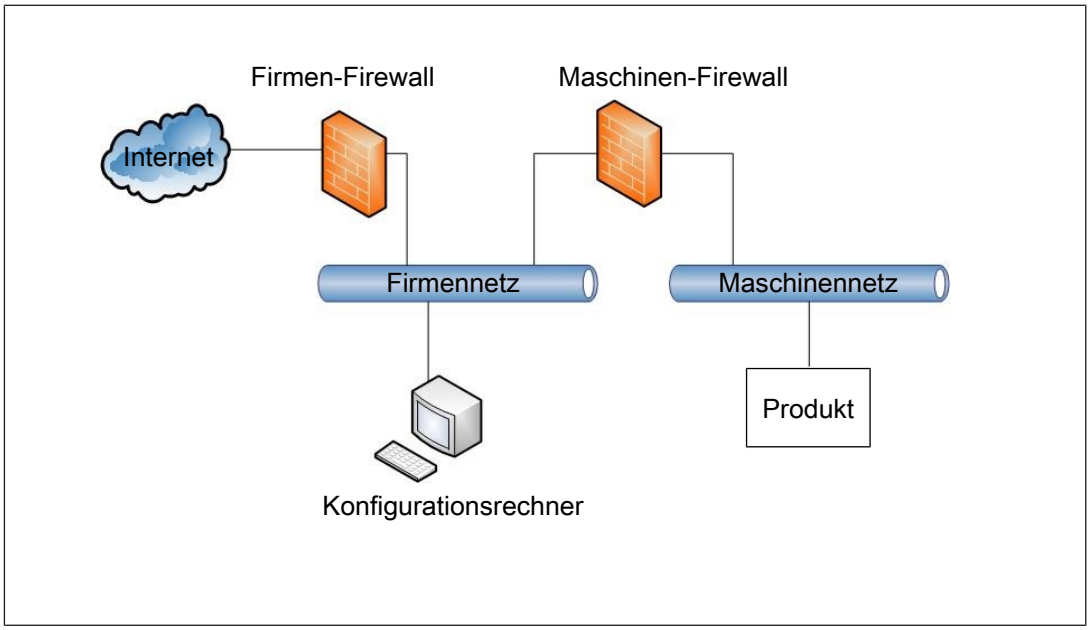


Abb.: Beispiel Netzwerktopologie

- Beachten Sie die Netzwerkdaten [📖 108] für die Risikoanalyse und die Security-Maßnahmen.

5 Funktionsbeschreibung

5.1 Ablauf der Authentifizierung

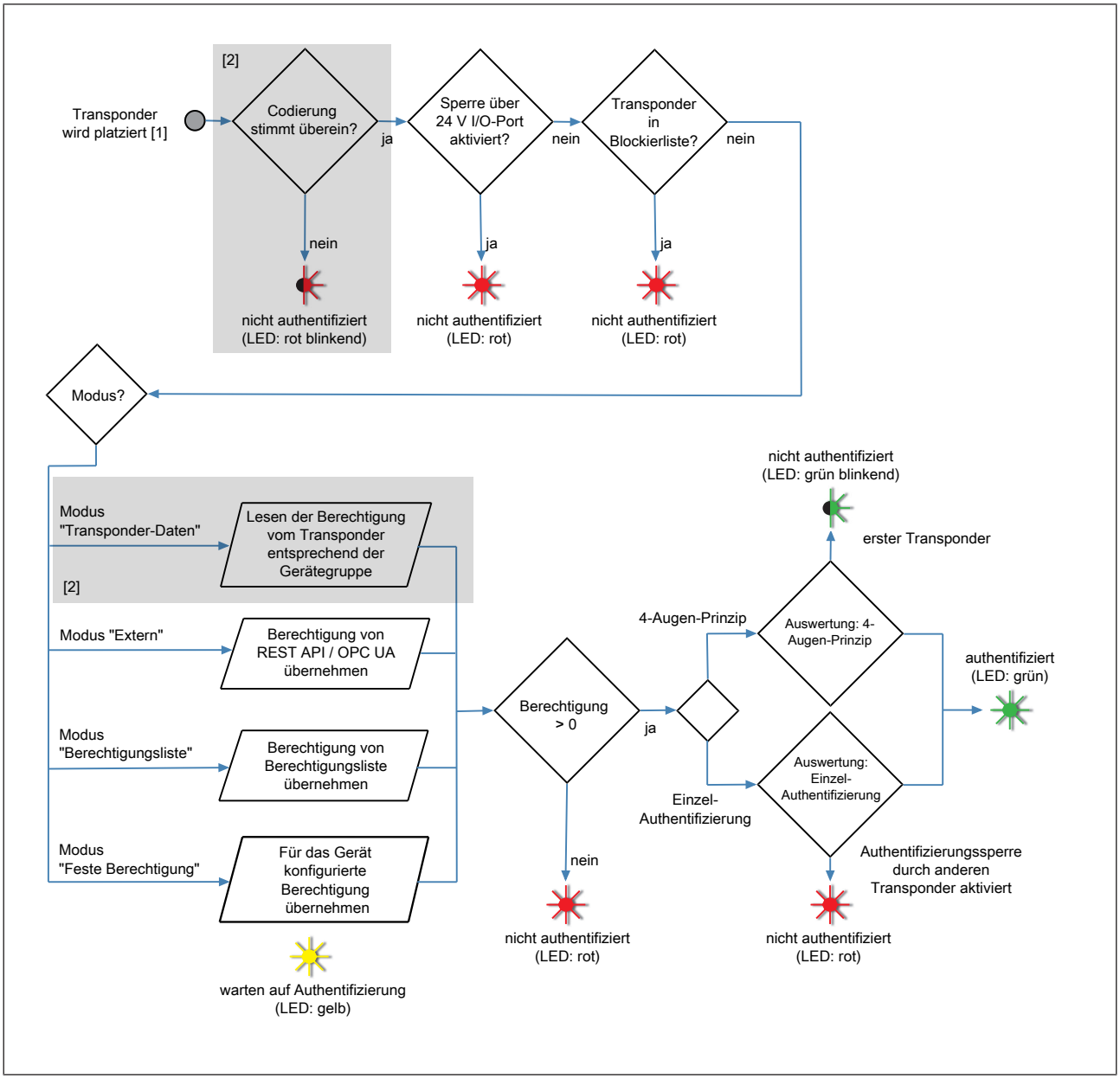


Abb.: Ablauf der Authentifizierung

[1]

Bedeutung:

- PITreader Key: Der Transponder wird in den Lesekopf gesteckt.
- PITreader Card: Der Transponder wird an den Lesekopf gehalten.

[2]

Die grau markierten Bereiche entfallen, wenn die Option ***Fremdtransponder unterstützen*** aktiviert ist und im Dropdown-Menü ***RFID-Protokoll*** ein ISO/IEC Standard gewählt ist.

5.2 Authentifizierungsmodi

Der PITreader unterstützt folgende Authentifizierungsmodi:

- Authentifizierungsmodus "Transponder-Daten" [22]
- Authentifizierungsmodus "Extern" [23]
- Authentifizierungsmodus "Berechtigungsliste" [26]
- Authentifizierungsmodus "Feste Berechtigung" [26]

Im Auslieferungszustand ist der Authentifizierungsmodus "Transponder-Daten" eingestellt. Der Authentifizierungsmodus kann in der Web-Anwendung geändert werden und es kann eingestellt werden, ob der Authentifizierungsmodus über die REST API überschrieben werden darf (siehe auch Authentifizierungsmodus konfigurieren [71]).

5.2.1 Authentifizierungsmodus "Transponder-Daten"

Im Authentifizierungsmodus "Transponder-Daten" kann sich ein Anwender durch das Platzieren eines Transponders im Lesebereich des PITreader an einer sicheren Auswerteeinheit (z. B. PIT m4SEU) und dem verbundenen Steuerungssystem authentifizieren. Die Authentifizierung erfolgt anhand der auf dem Transponder gespeicherten Berechtigungen.

Über eine sichere Auswerteeinheit (z. B. PIT m4SEU) kann eine sichere Betriebsartenwahl durchgeführt werden (nur bei PITreader Key und PITreader Card).

Eine Steuerung (PLC, HMI) kann über Modbus/TCP den zum aktuellen Zeitpunkt authentifizierten Transponder auslesen.

INFO

Beachten Sie, dass im Authentifizierungsmodus "Transponder-Daten" die Authentifizierung allein vom Besitz des Transponders abhängt. Der Verlust eines Transponders kann daher zu einem Security-Risiko führen.
Wir empfehlen Ihnen, die Security-IDs aller herausgegebenen Transponder in eine Liste einzutragen, um diese bei Verlust in die Blockierliste [42] übernehmen zu können.

Auf einem Transponder von Pilz kann gespeichert werden, in welchem Zeitraum der Transponder gültig ist. Wenn gewünscht, kann im Authentifizierungsmodus "Transponderdaten" die Gültigkeit des Transponders ausgewertet werden. Wenn der Transponder ungültig ist, wird unabhängig von der Gerätegruppe die Berechtigung "0" ausgegeben. D. h. der Transponder wird nicht authentifiziert.
Damit die Gültigkeit ausgewertet wird, muss für den PITreader in der Web-Anwendung unter ***Konfiguration -> Einstellungen -> Erweiterte Funktionen*** die Option ***Gültigkeitsdatum auswerten*** aktiviert werden.

5.2.1.1 Gerätegruppen

Es gibt 32 auswählbare Gerätegruppen, G0 bis G31.

In einer Gerätegruppe werden PITreader zusammengefasst. Ein Anwender (ein Transponder) hat an allen PITreader-Geräten einer Gruppe dieselbe Berechtigung. Ein anderer Anwender kann eine andere Berechtigung haben. Gerätegruppen können z. B. für einen Maschinentyp genutzt werden, ein Anwender hat dann z. B. an allen Drehmaschinen dieselbe Berechtigung (siehe auch Gerätegruppe einstellen [72]).

Pro Gerätegruppe kann auf einem Transponder eine Berechtigung gespeichert werden. Jede Gerätegruppe kann bis zu 65 unterschiedliche Berechtigungen haben.

- 0: keine Berechtigung
- 1 bis 64: Berechtigung 1 bis 64

Bei einer Berechtigung kann es sich z. B. um die Freischaltung von Funktionen handeln, die abhängig vom Ausbildungsgrad vergeben werden können.

Berechtigungen sind Codewörter zur fehlersicheren Übertragung mit einer garantierten minimalen Hamming-Distanz. Eine Übersicht der Codewörter für die Berechtigungen finden Sie im Abschnitt Übersicht der Berechtigungen [109].

Im PITreader ist immer nur eine Berechtigung gültig. Zusätzliche Berechtigungen, die auf dem Transponder gespeichert sind, können über die Modbus/TCP-Schnittstelle des PITreader abgerufen und ggf. für kundenspezifische Zwecke verwendet werden.

INFO

Durch die Verwendung der Anwenderdaten kann die Anzahl der Gerätegruppen auf mehr als 32 erweitert werden. Ein PITreader kann der Gerätegruppe 0 ... 9999 zugeordnet werden. Auf einem Transponder können die Berechtigungen für die Gerätegruppen 0 ... 31 gespeichert werden und zusätzlich für maximal 48 weitere Gerätegruppen im Bereich 32 ... 9999. Siehe Anwenderdaten [37].

5.2.2 Authentifizierungsmodus "Extern"

Im Authentifizierungsmodus "Extern" kann sich ein Anwender durch das Platzieren eines Transponders im Lesebereich des PITreader am verbundenen Steuerungssystem oder auf dem HMI authentifizieren.
Es stehen folgende Verbindungsmöglichkeiten zur Verfügung:

Externe Authentifizierung (Modbus/TCP)

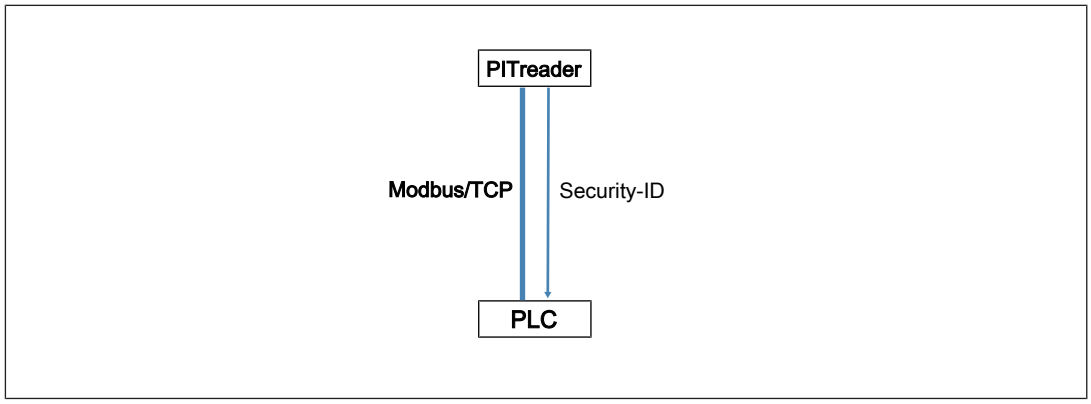


Abb.: Externe Authentifizierung (Modbus/TCP)

Der PITreader stellt die Daten des Transponders über die Modbus/TCP-Verbindung zur Verfügung.
Mithilfe einer Berechtigungsdatenbank (auf der PLC) und der Daten des Transponders (z. B. die Security-ID) kann die Berechtigung für den Anwender ermittelt werden. Die Authentifizierung erfolgt extern (auf der PLC).
Innerhalb des PITreader erfolgt keine Authentifizierung und die Geräte-LED leuchtet bei platziertem Transponder gelb.
Zur Anzeige des extern ermittelten Authentifizierungszustands über die Geräte-LED können Farbe und Blinkmodus über die Modbus/TCP-Schnittstelle überschrieben werden.

Beachten Sie: Im Authentifizierungsmodus "Extern" über Modbus/TCP kann **KEINE** sichere Auswerteeinheit (z. B. PIT m4SEU) eingesetzt werden.

Externe Authentifizierung (REST API)

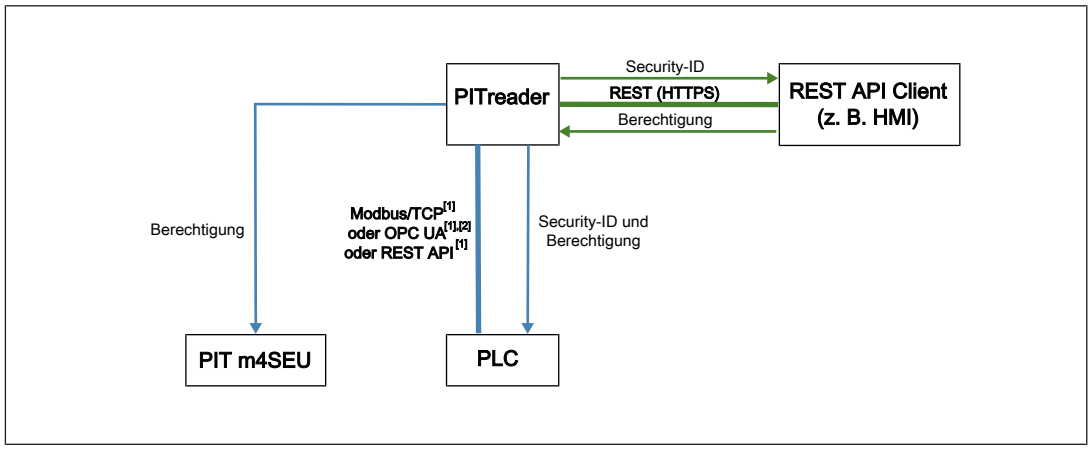


Abb.: Externe Authentifizierung (REST API)

[1] Ein Protokoll wählen, das von der PLC unterstützt wird.

[2] Es werden nur bestimmte PITreader-Varianten unterstützt.

Mithilfe einer Berechtigungsdatenbank auf dem REST API Client (z. B. HMI) und der Daten des Transponders (z. B. Security-ID) kann die Berechtigung für den Anwender ermittelt werden.
Die Authentifizierung erfolgt auf dem REST API Client. Die Information über den Authentifi-

zierungsstatus wird vom PITreader übernommen und an die Steuerung und die sichere Auswerteeinheit (z. B. PIT m4SEU) weitergeleitet. Der extern ermittelte Authentifizierungsstatus wird über die Geräte-LED des PITreader angezeigt.

Externe Authentifizierung (OPC UA)

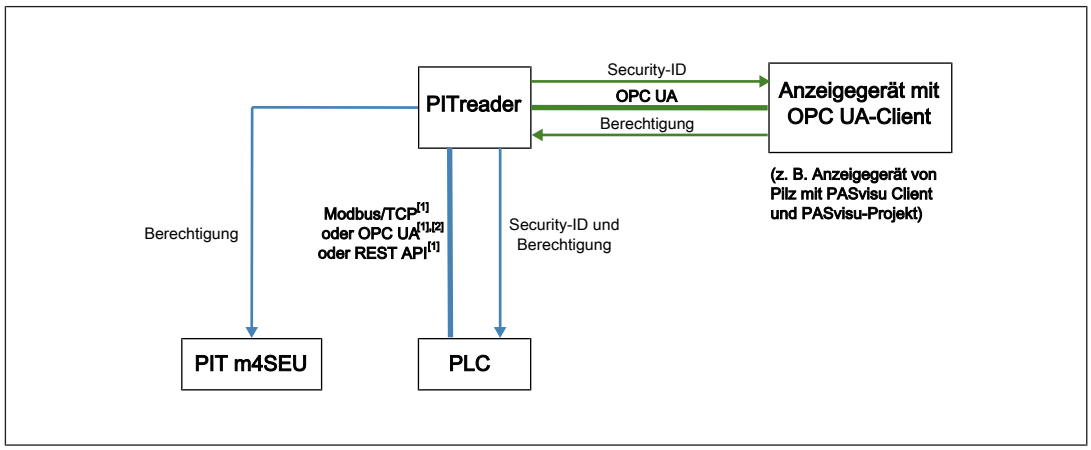


Abb.: Externe Authentifizierung (OPC UA)

[1] Ein Protokoll wählen, das von der PLC unterstützt wird.

[2] Es werden nur bestimmte PITreader-Varianten unterstützt.

Mithilfe einer Berechtigungsdatenbank auf dem OPC UA-Client (z. B. Anzeigegerät) und der Daten des Transponders (z. B. Security-ID) kann die Berechtigung für den Anwender ermittelt werden.

Die Authentifizierung erfolgt auf dem OPC UA-Client. Die Information über den Authentifizierungsstatus wird vom PITreader übernommen und an die Steuerung und die sichere Auswerteeinheit (z. B. PIT m4SEU) weitergeleitet. Der extern ermittelte Authentifizierungsstatus wird über die Geräte-LED des PITreader angezeigt.

5.2.3 Authentifizierungsmodus "Berechtigungsliste"

Im Authentifizierungsmodus "Berechtigungsliste" werden zur Authentifizierung die auf dem Transponder gespeicherte Security-ID und die in der Berechtigungsliste hinterlegten Informationen ausgewertet (siehe auch Berechtigungsliste [84]).

Eine Steuerung (PLC, HMI) kann über Modbus/TCP den zum aktuellen Zeitpunkt authentifizierten Transponder auslesen.

Ein externes Gerät (z. B. HMI) kann über einen HTTP(S)-basierten Webservice-Aufruf den zum aktuellen Zeitpunkt authentifizierten Benutzer auslesen.

Über eine sichere Auswerteeinheit (z. B. PIT m4SEU) kann eine sichere Betriebsartenwahl durchgeführt werden (nur bei PITreader Key und PITreader Card).

5.2.4 Authentifizierungsmodus "Feste Berechtigung"

Im Authentifizierungsmodus "Feste Berechtigung" wird jeder Transponder, mit Ausnahme der Transponder in der Blockierliste, authentifiziert und erhält eine vorkonfigurierte Berechtigung. Die Berechtigung ist für alle Transponder gleich.

Dieser Authentifizierungsmodus eignet sich besonders für Fremdtransponder, bei denen im Dropdown-Menü RFID-Protokoll ein ISO/IEC Standard gewählt wurde. Der PITreader akzeptiert dann jeden Transponder und stellt die UID und die Security-ID des authentifizierten Transponders zur Verfügung.

Eine Steuerung (PLC, HMI) kann über Modbus/TCP den zum aktuellen Zeitpunkt authentifizierten Transponder auslesen.

Ein externes Gerät (z. B. HMI) kann über einen HTTP(S)-basierten Webservice-Aufruf den zum aktuellen Zeitpunkt authentifizierten Benutzer auslesen.

5.3 Authentifizierungstypen

Der PITreader unterstützt folgende Authentifizierungstypen:

- Basis
- Einzelauthentifizierung
- 4-Augen-Prinzip

5.3.1 Authentifizierungstyp "Basis"

Der Authentifizierungstyp "Basis" umfasst die Authentifizierungsmodi "Transponder-Daten", "Extern" und "Berechtigungsliste" mit allen ihren Funktionen und Möglichkeiten (siehe Authentifizierungsmodi [22]).

5.3.2 Authentifizierungstyp "Einzelauthentifizierung"

Der Authentifizierungstyp "Einzelauthentifizierung" umfasst alle Funktionen und Möglichkeiten des Authentifizierungstyps "Basis". Darüber hinaus erhält der Anwender spezielle Rechte, wenn "Einzelauthentifizierung" konfiguriert ist. Der Anwender kann sich mit seinem Transponder an einem Gerät anmelden, um eine Authentifizierungssperre für alle anderen Transponder zu aktivieren. Die Authentifizierungssperre bleibt aktiviert, bis die Abmeldung mit demselben Transponder erfolgt. Bei aktiver Authentifizierungssperre leuchtet die Geräte-LED rot.

- Authentifizierungssperre aktivieren:

  Durch das Platzieren des Transponders am PITreader erfolgt die Anmeldung für Einzelauthentifizierung. Mit der Anmeldung wird für alle anderen Transponder eine Authentifizierungssperre aktiviert. Wird der Transponder entfernt, dann bleibt die Authentifizierungssperre aktiviert.

- Authentifizierungssperre deaktivieren:

  Die Authentifizierungssperre wird erst durch die Abmeldung mit demselben Transponder deaktiviert. Für die Abmeldung muss derselbe Transponder erneut platziert und wieder entfernt werden.

  Hinweis: Die Authentifizierungssperre kann auch über die Web-Anwendung zurückgesetzt werden. Hierzu sind Administrator-Zugriffsrechte auf die Web-Anwendung erforderlich. Das Zurücksetzen über die Web-Anwendung wird protokolliert.

5.3.3 Authentifizierungstyp "4-Augen-Prinzip"

Der Authentifizierungstyp "4-Augen-Prinzip" umfasst alle Funktionen und Möglichkeiten des Authentifizierungstyps "Basis".

Beim Authentifizierungstyp "4-Augen-Prinzip" werden zwei unterschiedliche Transponder zur Authentifizierung benötigt. Mit dem ersten Transponder wird der Authentifizierungsvorgang gestartet. Die eigentliche Authentifizierung erfolgt anschließend mithilfe des zweiten Transponders.

- Authentifizierungsvorgang starten

  Durch das Platzieren des ersten Transponders am PITreader wird der Authentifizierungsvorgang gestartet. Die Geräte-LED blinkt grün.

  Der Transponder durchläuft alle Authentifizierungsschritte bis zur Berechtigungsprüfung (siehe Ablauf der Authentifizierung [📖 21]). Bei ausreichender Berechtigung und Konfiguration für das "4-Augen-Prinzip" wird die Berechtigung intern als "Berechtigung 0" gewertet; d. h. mit dem ersten Transponder ist keine Authentifizierung möglich.

  Nach dem Entfernen des ersten Transponders wird ein Zeitfenster von 30 Sekunden aktiviert. Die Authentifizierung mit dem zweiten Transponder kann innerhalb dieses Zeitfensters erfolgen. Die Geräte-LED blinkt solange grün bis entweder die 30 Sekunden des Zeitfensters abgelaufen sind oder der zweite Transponder platziert wird.

- Authentifizierungsvorgang abbrechen

  Ein gestarteter Authentifizierungsvorgang wird abgebrochen, wenn innerhalb des Zeitfensters von 30 Sekunden entweder kein zweiter gültiger Transponder platziert wird oder derselbe Transponder erneut platziert wird.

  Ein gestarteter Authentifizierungsvorgang wird durch einen ungültigen Transponder nicht abgebrochen.

- Authentifizierungsvorgang nach einem Abbruch erneut starten

  Durch das erneute Platzieren und Entfernen des ersten Transponders kann der Authentifizierungsvorgang wieder gestartet werden.

- Authentifizierung

  Bei gestartetem Authentifizierungsvorgang kann sich ein Anwender innerhalb des Zeitfensters von 30 Sekunden mit einem zweiten Transponder authentifizieren.

  Nach dem Platzieren des zweiten Transponders durchläuft dieser alle Authentifizierungsschritte (siehe Ablauf der Authentifizierung [📖 21]). Handelt es sich um einen gültigen Transponder, erfolgt die Authentifizierung.

Hinweise:

- Bei den beiden Transpondern kann es sich um beliebige Transponder handeln; d. h. es sind keine speziellen oder vorkonfigurierten Transponder erforderlich. Die Transponder müssen jedoch anwendungsabhängig gültig sein.
- Die Berechtigung, die mit der Authentifizierung durch den zweiten Transponder freigeschaltet wird, wird intern ermittelt. Hierbei werden die Berechtigungen der beiden Transponder ausgewertet und die Authentifizierung erfolgt mit der kleineren Berechtigung der beiden Transponder.

  Beispiele:

  – Berechtigung des ersten Transponders: 10

    Berechtigung des zweiten Transponders: 5

    -> Die Authentifizierung erfolgt mit der Berechtigung 5

  – Berechtigung des ersten Transponders: 1

    Berechtigung des zweiten Transponders: 5

    -> Die Authentifizierung erfolgt mit der Berechtigung 1

5.4 Transponder

5.4.1 Transponder von Pilz

Transponder sind in Form von Transponder-Schlüsseln, Transponder-Karten und Transponder-Sticker verfügbar. Die Funktionen sind für alle Transponder identisch.

Einsatzmöglichkeiten eines Transponders

Transponder	PITreader Key PIT gb mit PITreader Key	PITreader Card PIT gb mit PITreader Card
Transponder-Schlüssel	♦	♦
Transponder-Karten	---	♦
Transponder-Sticker [1]	---	♦

[1]

Hinweis: Ein Transponder-Sticker wird auf eine vorhandene Karte aufgeklebt (siehe PITreader Transponder-Sticker aufkleben [📖 59]).

5.4.1.1 Berechtigung eines Transponders

Transponder-Schlüssel

Die Transponder-Schlüssel sind in folgenden Varianten und Berechtigungen verfügbar (siehe auch Bestelldaten [📖 111]):

Bezeichnung	Berechtigung	Seriennummer
PITreader key ye 1	Berechtigung 1	01nnnnnnn
PITreader key ye 2	Berechtigung 2	02nnnnnnn
PITreader key ye 3	Berechtigung 3	03nnnnnnn
PITreader key ye 4	Berechtigung 4	04nnnnnnn
PITreader key ye 5	Berechtigung 5	05nnnnnnn
PITreader key ye 5 service	Berechtigung 5 (Service)	13nnnnnnn
PITreader key ye g	Ohne vorprogrammierte Berechtigung	00nnnnnnn

Anhand der ersten beiden Ziffern (Präfix) der Seriennummer lässt sich die Berechtigung erkennen.

Bis auf "PITreader key ye g" sind alle Transponder-Schlüssel werkseitig vorprogrammiert und die Berechtigung ist nicht änderbar. Die Berechtigung gilt für die Gerätegruppen G0 … G31.

Bei "PITreader key ye g" kann die Berechtigung für die Gerätegruppen geändert und optional auch gesperrt werden.

Transponder-Karten

Transponder-Karten sind in folgenden Varianten verfügbar (siehe auch Bestelldaten [📖 111]):

Bezeichnung	Berechtigung	Seriennummer
PITreader card ye 1	Berechtigung 1	01nnnnnnn
PITreader card ye 2	Berechtigung 2	02nnnnnnn
PITreader card ye 3	Berechtigung 3	03nnnnnnn
PITreader card ye 4	Berechtigung 4	04nnnnnnn
PITreader card ye 5	Berechtigung 5	05nnnnnnn
PITreader card ye 5 service	Berechtigung 5 (Service)	13nnnnnnn
PITreader card ye g	Ohne vorprogrammierte Berechtigung	00nnnnnnn

Anhand der ersten beiden Ziffern (Präfix) der Seriennummer lässt sich die Berechtigung erkennen.

Bis auf "PITreader card ye g" sind alle Transponder-Karten werkseitig vorprogrammiert und die Berechtigung ist nicht änderbar. Die Berechtigung gilt für die Gerätegruppen G0 … G31.

Bei "PITreader card ye g" kann die Berechtigung für die Gerätegruppen geändert und optional auch gesperrt werden.

Transponder-Sticker

Transponder-Sticker sind in folgenden Varianten verfügbar (siehe auch Bestelldaten [📖 111]):

Bezeichnung	Berechtigung	Seriennummer
PITreader sticker ye 1	Berechtigung 1	01nnnnnnn
PITreader sticker ye 2	Berechtigung 2	02nnnnnnn
PITreader sticker ye 3	Berechtigung 3	03nnnnnnn
PITreader sticker ye 4	Berechtigung 4	04nnnnnnn
PITreader sticker ye 5	Berechtigung 5	05nnnnnnn
PITreader sticker ye 5 service	Berechtigung 5 (Service)	13nnnnnnn
PITreader sticker ye g	Ohne vorprogrammierte Berechtigung	00nnnnnnn

Anhand der ersten beiden Ziffern (Präfix) der Seriennummer lässt sich die Berechtigung erkennen.

Bis auf "PITreader sticker ye g" sind alle Transponder-Sticker werkseitig vorprogrammiert und die Berechtigung ist nicht änderbar. Die Berechtigung gilt für die Gerätegruppen G0 … G31.

Bei "PITreader sticker ye g" kann die Berechtigung für die Gerätegruppen geändert und optional auch gesperrt werden.

5.4.1.2 Datenbereiche eines Transponders

Auf einem Transponder sind verschiedene Datenbereiche verfügbar.

Hierzu zählen:

- Datenbereich für die Berechtigung
  - Transponder mit werkseitig vorprogrammierter Berechtigung (Berechtigung nicht änderbar bzw. gesperrt)
  - Transponder mit konfigurierbarer Berechtigung (Berechtigung änderbar)

    Die Berechtigung kann optional gesperrt werden.
- Datenbereich für die Berechtigung von Gerätegruppen
  - Bei Transpondern mit werkseitig vorprogrammierter Berechtigung gilt die vorprogrammierte Berechtigung für die Gerätegruppen G0 … G31.
  - Bei Transpondern mit konfigurierbarer Berechtigung kann für jede der Gerätegruppen G0 … G31 eine eigene Berechtigung konfiguriert werden. Mögliche Berechtigungen sind 0 … 64.
- Datenbereich für das Gültigkeitsdatum des Transponders (Start-/Enddatum)

  Der Datenbereich kann nicht gesperrt werden.
- Datenbereich für freie (kundenspezifische) Anwenderdaten

  Der Datenbereich kann nicht gesperrt werden.

Beispiel

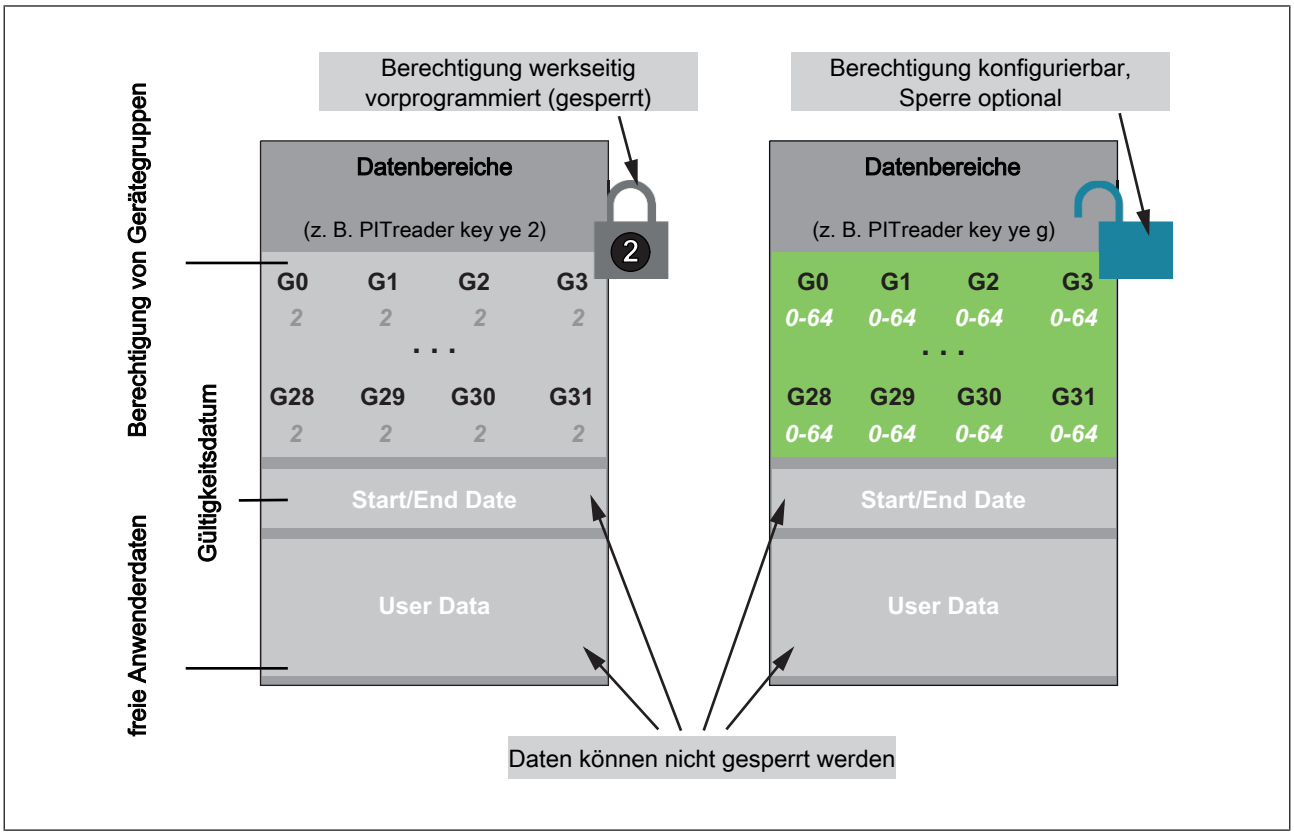


Abb.: Datenbereiche eines Transponders am Beispiel von PITreader key ye 2 und PITreader key ye g

5.4.1.3 Auswertung der Seriennummer eines Transponders

Die Seriennummer der Transponder setzt sich aus einem Präfix (2 Stellen) und einer fortlaufenden Nummer (7 Stellen) zusammen. Beachten Sie bei der Auswertung der Seriennummer in einem externen System, dass Präfix und fortlaufende Nummer innerhalb des 4-Byte umfassenden Seriennummern-Feldes (z. B. in der Modbus/TCP-Schnittstelle) separat abgespeichert und übermittelt werden. Das oberste Byte enthält das Präfix, die unteren 3 Byte enthalten die fortlaufende Nummer.

5.4.2 Transponder von Fremdherstellern mit gewähltem ISO/IEC Standards (ohne MIFARE DESFire-Anwendungen)

Die Lesegeräte PITreader S card unit und PIT gb mit PITreader Card können Transponder von Fremdherstellern lesen. Dies ist möglich, auch wenn auf den Transpondern keine spezifischen PITreader-Daten abgelegt sind, wenn sie einem der folgenden Standards entsprechen:

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

Dabei werden von den Fremdtranspondern ausschließlich die UID nach ISO-Standard gelesen und daraus die Security-ID des Transponders berechnet. Weitere Daten können nicht gelesen oder geschrieben werden.

Daraus ergeben sich folgende Einschränkungen:

- Verschiedene Security-Funktionen des PITreaders können nicht genutzt werden, z. B. Codierung oder geschützte Kommunikation über AES-Schlüssel.
- Der Authentifizierungsmodus "Transponder-Daten" kann nicht genutzt werden.
- Anwenderdaten können nicht auf den Fremdtransponder geschrieben werden.
- Die sichere Auswerteeinheit PIT m4SEU kann mit Einschränkungen genutzt werden: An der Key-ID-Schnittstelle IDo0 ... IDo3 der sicheren Auswerteeinheit PIT m4SEU werden in dieser Konfiguration die niederwertigsten 3 Byte der UID ausgegeben.
- Fremdtransponder können nicht im Wartungssicherungssystem "Key-in-Pocket" von Pilz eingesetzt werden.

Damit der PITreader die Fremdtransponder unterstützt, muss die Option ***Fremdtransponder unterstützen*** in der Konfiguration aktiviert werden (siehe Fremdtransponder mit ISO/IEC Standard als RFID-Protokoll konfigurieren [📖 73]).

WICHTIG

Mögliche Security-Schwachstelle durch Fremdtransponder deren Identität nicht bestimmt werden können

Die Verwendung von Fremdtranspondern ist ein potenzielles Security-Risiko.

Wenn die Option ***Fremdtransponder unterstützen*** aktiviert und im Dropdown-Menü ***RFID-Protokoll*** ein ***ISO/IEC*** Standard gewählt ist, kann die Identität (UID) des Transponders nicht sicher bestimmt werden. Dadurch besteht kein systematischer Schutz gegen Kopieren von Transpondern oder Vortäuschen von anderen Transpondern.

Berücksichtigen Sie bei Ihrer Security-Risikoanalyse, dass die Verwendung von Fremdtranspondern eine Security-Schwachstelle für Cyber-Bedrohungen darstellen kann.

WICHTIG

Wenn die Option ***Fremdtransponder unterstützen*** aktiviert und im Dropdown-Menü ***RFID-Protokoll*** der Standard ***ISO/IEC 14443-A*** gewählt ist, werden die PILZ-Transponder wie Fremdtransponder behandelt. Von den Pilz-Transpondern wird dann nur noch die UID gelesen und es gelten dieselben Einschränkungen wie für Fremdtransponder, siehe Transponder von Fremdherstellern mit gewähltem ISO/IEC Standards (ohne MIFARE DESFire-Anwendungen) [📖 32]

5.4.3 Transponder von Fremdherstellern mit MIFARE DESFire-Anwendungen

Mit den folgenden Produkten können Sie Transponder mit MIFARE DESFire-Anwendungen verwenden:

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

Folgende Transponder mit MIFARE DESFire-Anwendungen werden unterstützt:

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

Mit diesen Transpondern stehen für den PITreader alle Funktionen zur Verfügung, wie bei der Nutzung von Transpondern von Pilz.

Damit Transponder mit MIFARE DESFire-Anwendungen genutzt werden können

- muss die PITreader-Datenstruktur auf den Transpondern aufgebracht werden.
  Diese entspricht technisch einer eigenen MIFARE DESFire-Anwendung. Zum Aufbringen der PITreader-Datenstruktur müssen im Transponderspeicher mindestens 1440 Byte frei sein. Danach verhalten sich die Transponder mit MIFARE DESFire-Anwendungen wie Transponder von Pilz und unterstützen alle PITreader-Funktionen.
- müssen AES-Schlüssel im PITreader hinterlegt werden. Diese kryptografischen Schlüssel ermöglichen es dem PITreader sich am Transponder zu authentifizieren. Dadurch kann der PITreader Daten auf den Transponder schreiben und lesen. Über die so genannte Diversifikation kann für jeden Transponder ein individueller AES-Schlüssel generiert werden.

5.4.4 Security-ID (SID) eines Transponders

Bei der Security-ID (SID) eines Transponders handelt es sich um eine eindeutige Kennung, die ausschließlich für diesen einen Transponder gilt.

- Transponder von Pilz
  Alle Pilz-Transponder sind werkseitig mit einer Security-ID vorprogrammiert. Die Security-ID eines Transponders ist nicht änderbar.
  Hinweis: Wenn im PITreader die Option ***Fremdtransponder unterstützen*** aktiviert ist, gilt für die Pilz-Transponder nicht die vorprogrammierte Security-ID, sondern eine Security-ID, die im PITreader aus der UID des Transponders berechnet wird.
- Fremdtransponder bei denen im Dropdown-Menü ***RFID-Protokoll*** ISO/IEC 14443 Typ A, ISO/IEC 15693 oder ISO/IEC 18092 (FeliCa) gewählt wurde
  Die Security-ID wird im PITreader aus der UID des Transponders berechnet.
- Fremdtransponder mit MIFARE DESFire-Anwendungen
  Die Security-ID wird beim Initialisieren aus der Artikelnummer, der Seriennummer und der UID des Transponders berechnet. Danach ist sie nicht änderbar.

Die Security-ID dient zur eindeutigen Identifikation eines Transponders am PITreader; d. h. mithilfe der Security-ID wird ein Transponder beim PITreader authentifiziert. Die Berechtigungen, die für einen Transponder konfiguriert sind, sind an die Security-ID gebunden.

Die Security-ID wird in der Web-Anwendung angezeigt. In einer vom Benutzer erstellten Anwendung (z. B. Auswertung und Aktivierung der gewählten Betriebsart über HMI, Web-Anwendung, Benutzer-Software) kann die Security-ID über Modbus/TCP, REST API oder OPC UA ausgelesen werden. In solchen Anwendungen sollte die Security-ID vom Benutzer ebenfalls ausgewertet und zur Authentifizierung verwendet werden.

Indem die Security-ID eines Transponders in eine Blockierliste eingetragen wird, kann die Authentifizierung gesperrt werden (siehe Blockierliste verwenden [📖 84]).

5.4.5 Transponder-Erkennung bei einem PITreader Card

- Maximaler Leseabstand bei der Platzierung eines Transponders
  - Transponder-Schlüssel

    Die optimale Platzierung eines Transponder-Schlüssels ist dann gegeben, wenn die Spitze des Transponder-Schlüssels im Zentrum des Lesekopfs platziert ist und dabei die Oberfläche des Lesekopfs berührt.
  - Transponder-Karte oder Transponder-Sticker

    Das Zentrum des Transponders sollte möglichst über dem Zentrum des Lesekopfs platziert werden.

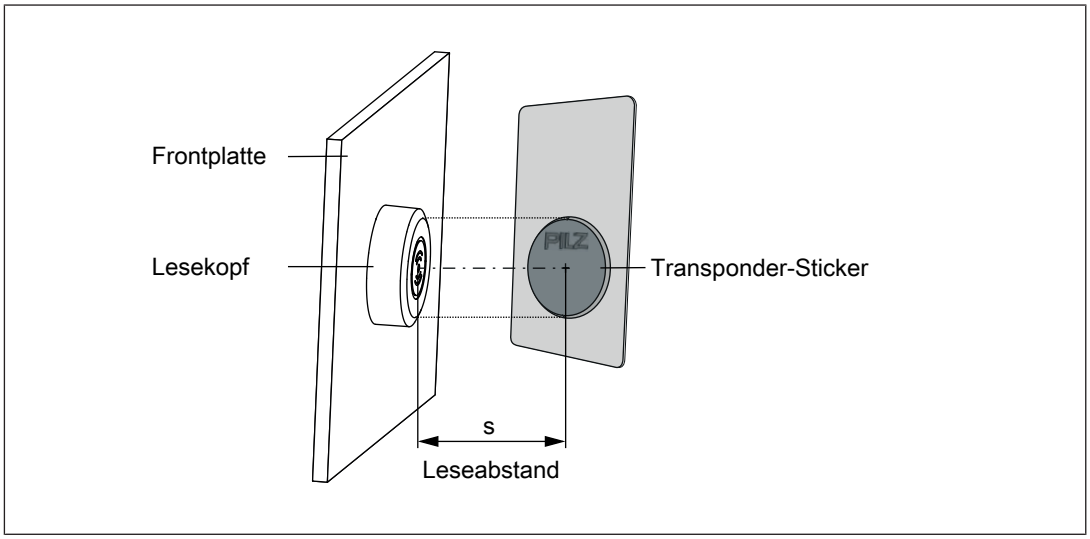
    Die optimale Platzierung einer Transponder-Karte oder eines Transponder-Stickers ist dann gegeben, wenn der Lesekopf des PITreader Card und der Lesebereich des Transponders parallel zueinander ausgerichtet sind und beide Zentren übereinander liegen.

    Bei optimaler Platzierung ist der zugesicherte maximale Leseabstand s wie folgt:

    - metallische Frontplatte: s = 10 mm

    - nicht metallische Frontplatte: s = 20 mm

    Beispiel:



- Transponder-Erkennung bei mehreren Transpondern im Lesebereich

  Die Authentifizierung erfolgt nur, wenn sich genau ein gültiger Transponder im Lesebereich befindet. Befinden sich weitere Transponder im Lesebereich, die jedoch nicht lesbar sind (z. B. Transponder für Fremdanwendungen), dann werden diese Transponder ignoriert.

Störungen bei der Transponder-Erkennung werden über die LED-Anzeige gemeldet. Sie finden weitere Informationen bei der Beschreibung des LED-Zustands "rot blinkend" (siehe LED-Anzeige [📖 93]).

5.5 Anwenderdaten

Auf einem Transponder steht ein freier Datenbereich zur Verfügung. In diesem freien Datenbereich können kundenspezifische Daten gespeichert werden (z. B. Sprache, Anwendername, …). Außerdem können die Anwenderdaten genutzt werden, um die Anzahl der Gerätegruppen auf mehr als 32 zu erweitern.

Die Anwenderdaten sind in Parametern organisiert. Es gibt Parameter, deren Funktion der Anwender selbst bestimmt (Anwenderparameter) und es gibt Systemparameter. Die Systemparameter haben eine vordefinierte Funktion (siehe Systemparameter [📖 38]).

Jeder Parameter hat eine ID, einen Namen und einen Datentyp:

- Parameter-ID

  Die ID ist eine Nummer im Bereich 1 ... 65535. Sie kennzeichnet einen Parameter eindeutig.
  Die ID kann vom Anwender frei vergeben werden.
  Hinweis: Die IDs 1 ... 9999 sollten vom Anwender nicht verwendet werden, weil sie von Pilz für Systemparameter verwendet werden könnten.

- Name

  Der Name kann vom Anwender frei vergeben werden.

- Datentyp

  Es können die Datentypen verwendet werden, die in der Tabelle zu finden sind. Jeder Wert eines Parameters hat die in der Tabelle angegebene Datenlänge. Beim Anlegen eines Parameters wird die Typ-ID angegeben und nicht der Name des Datentyps.

Typ-ID	Name	Datenlänge	Wertebereich	Initialwert
1	STRING	2 … 255 Byte		leerer 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		leere Zeit/Datum
30	PERMISSION	4 Byte	0 ... 64 (Hamming-codiert)	0
31	BIT	1 Byte	0 oder 1	0

Damit die Anwenderdaten genutzt werden können, müssen sie auf dem PITreader konfiguriert werden. In der Konfiguration werden die einzelnen Parameter angelegt. Auf dem PITreader können maximal 64 Parameter angelegt werden.
Werden Parameter auf einem PITreader angelegt, erweitert sich der Bereich der Gerätegruppen von 0 ... 31 auf 0 ... 9999. Damit die Gruppen 32 ... 9999 genutzt werden können, muss zwingend der Systemparameter mit der ID 1 angelegt werden (siehe Systemparameter [📖 38]).
Wie Sie Anwenderdaten konfigurieren, ist hier beschrieben: Anwenderdaten konfigurieren [📖 85]

Die Werte der Parameter werden auf dem Transponder gespeichert. Auf dem Transponder können Werte für maximal 64 Parameter und maximal 48 Gerätegruppen gespeichert werden. Wie viele Werte tatsächlich gespeichert werden können, hängt von der Datenlänge der Werte ab. Je mehr Parameter genutzt werden, umso weniger Gerätegruppen sind möglich. In der Web-Anwendung wird die Auslastung des Speichers auf dem Transponder angezeigt.

Für jeden Parameter kann pro gewünschter Gerätegruppe (Gruppennummer 0 ... 9999) ein eigener Wert gespeichert werden. Um Speicherplatz zu sparen ist es möglich, pro Parameter einen Default-Wert zu konfigurieren. Dieser Default-Wert wird für alle Gerätegruppen 0 ... 9999 verwendet, für die kein eigener Wert konfiguriert ist.

Wie Sie die Werte für die Parameter auf einen Transponder schreiben, ist hier beschrieben: Werte der Anwenderdaten bearbeiten [📖 83]

Die Anwenderdaten können über Modbus/TCP, über REST API oder über den OPC UA-Server vom Transponder gelesen werden (siehe Bedienungsanleitung PITreader REST API oder PITreader OPC Server UA). Der PITreader gibt für einen Parameter immer genau einen Wert zurück und zwar den Wert für die Gerätegruppe, zu der der PITreader gehört. Sollte der Parameter nicht auf dem Transponder vorhanden sein, wird der Initialwert des Datentyps zurückgegeben.
Ist der Parameter auf dem Transponder vorhanden, aber die Gerätegruppe nicht, wird der Default-Wert zurückgegeben. Ist kein Default-Wert gespeichert, wird der Initialwert des Datentyps zurückgegeben.

5.5.1 Systemparameter

Es gibt Parameter mit vordefinierten Funktionen. Die ID und der Datentyp ist für diese Parameter vorgegeben. Der Name darf vom Anwender vergeben werden.

ID	Datentyp	Bedeutung
1	PERMISSION	Berechtigung Berechtigungen der Gerätegruppen 32 ... 9999 Hinweis: In den Anwenderdaten können auch Berechtigungen für die Gruppen 0 bis 31 festgelegt werden, aber diese werden ignoriert. Für die Gerätegruppen 0 bis 31 gelten immer die Berechtigungen, die in der Web-Anwendung unter ***Transponder -> Berechtigungen*** eingegeben wurden.
2	DATETIME	Startdatum Angabe, ab wann die Berechtigung für eine Gerätegruppe gültig sein soll. Dieser Wert kann für die Gruppen 0 ... 9999 festgelegt werden. Hinweis: Das Startdatum wird nur ausgewertet, wenn für den PITreader die Option ***Gültigkeitsdatum auswerten*** aktiviert ist.
3	DATETIME	Enddatum Angabe, bis wann die Berechtigung für eine Gerätegruppe gültig sein soll. Dieser Wert kann für die Gruppen 0 ... 9999 festgelegt werden. Hinweis: Das Enddatum wird nur ausgewertet, wenn für den PITreader die Option ***Gültigkeitsdatum auswerten*** aktiviert ist.

5.6 Codierung

Durch den Vorgang der Codierung können PITreader auf die Erkennung von bestimmten, mit derselben Kennung codierten, Transponder beschränkt werden.

Es gibt zwei verschiedene Codierungen:

- Basis-Codierung [40]
- OEM-Codierung [41]

Auf einem PITreader können die Kennungen für beide Codierungen gespeichert werden. Ein Transponder kann jedoch nur auf eine der beiden Codierungen eingelernt werden. Das Einlernen eines Transponders auf eine der beiden Codierungen erfolgt in der Web-Anwendung. Zum Einlernen eines Transponders auf eine Basis-Codierung muss hierbei die Basis-Kennung als Basis-Codierung eingetragen werden. Zum Einlernen eines Transponders auf eine OEM-Codierung muss die OEM-Kennung ebenfalls als Basis-Codierung eingetragen werden.

Kennungen werden im Gerät in einem Hardware-Security-Baustein sicher abgelegt. Beim Einlernen von Transpondern werden diese mit einer fälschungssicheren kryptographischen Signatur versehen, die ein Anwendersystem sicher vor Manipulationen und fremden Transpondern schützt.

Einlernen eines codierten Transponders

Wenn ein PITreader, bei dem eine Codierung genutzt wird, um weitere Transponder erweitert werden soll, müssen die neuen Transponder vor der ersten Verwendung an einem entsprechend codierten PITreader eingelernt werden.

INFO

Wenn ein (noch) nicht codierter Transponder im Lesebereich des PITreader platziert wird oder PITreader und Transponder mit unterschiedlichen Kennungen codiert sind, wird der Transponder nicht ausgelesen und der PITreader zeigt einen Fehler an (LED blinkt rot). In diesem Fall sind die Daten des Transponders auch nicht über externe Schnittstellen (Modbus/TCP-Verbindung, OPC UA, REST API) auslesbar und es kann keine (externe) Authentifizierung des Transponders stattfinden.

Schutz vor unbefugtem Auslesen eines codierten Transponders

An einem nicht codierten PITreader funktionieren sowohl codierte, als auch nicht codierte Transponder; d. h. die Daten eines codierten Transponders können auch von einem nicht codierten PITreader ausgelesen werden. Um dies zu verhindern, kann ein codierter Transponder zusätzlich so konfiguriert werden, dass das Auslesen auf identisch codierte PITreader beschränkt ist (siehe Transponder auf identisch codierte PITreader beschränken [83]).

Überwachung der Codierung mithilfe einer Prüfsumme

Mithilfe einer Prüfsumme kann sowohl für die Basis- als auch OEM-Codierung überwacht werden, ob die Codierung im PITreader geändert wurde.

Eigenschaften der Prüfsumme:

- Datenlänge der Prüfsumme: 16 Byte
- Wenn keine Codierung gesetzt ist, dann ist die Prüfsumme 0.
- Wenn eine Codierung gesetzt ist, dann wird eine Prüfsumme ermittelt. Die Prüfsumme wird jedes Mal neu ermittelt, wenn die Codierung geändert wird; d. h. mit jeder Änderung der Codierung ändert sich die Prüfsumme.

Über Modbus/TCP, REST API oder OPC UA kann die Prüfsumme ausgelesen werden. Die Prüfsumme wird außerdem in der Web-Anwendung angezeigt (siehe Basis-Codierung setzen [📖 72] und OEM-Codierung setzen [📖 72]).

5.6.1 Basis-Codierung

Durch die Basis-Codierung können PITreader ausschließlich Transponder erkennen, die mit derselben Basis-Kennung codiert wurden oder mit einer gegebenenfalls im PITreader hinterlegten OEM-Kennung (siehe OEM-Codierung [📖 41]).

Die Basis-Codierung kann z. B. genutzt werden, um eine "Unternehmenskennung" zu codieren. Dadurch werden nur noch intern codierte Transponder erkannt.

Die Basis-Codierung erfolgt durch die Konfiguration des PITreader mit einer Basis-Kennung (siehe Basis-Codierung setzen [📖 72]). Transponder werden auf eine Basis-Kennung eingelernt, wenn an einem codierten PITreader Berechtigungen auf den Transponder geschrieben werden (siehe Transponder auf Basis-Codierung einlernen [📖 81]).

Die Basis-Codierung kann manuell vom Gerät gelöscht werden, ohne die Basis-Kennung zu kennen. Beim Zurücksetzen des Geräts auf Werkseinstellungen wird die Basis-Codierung automatisch gelöscht.

5.6.2 OEM-Codierung

Durch die OEM-Codierung kann im PITreader eine zweite Kennung zur Prüfung von Transpondern hinterlegt werden. PITreader mit OEM-Codierung akzeptieren Transponder, mit derselben OEM-Kennung oder mit der passenden Basis-Kennung (siehe Basis-Codierung [📖 40]).

Die OEM-Codierung kann z. B. von Maschinenherstellern genutzt werden, um einen Transponder zu erstellen, den ein Service-Mitarbeiter bei allen Kunden einsetzen kann.

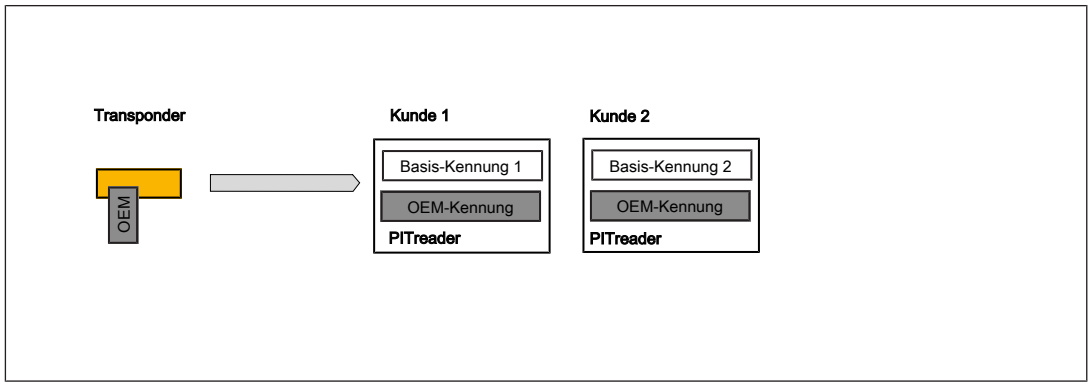


Abb.: OEM-Codierung

Neue Transponder mit dieser OEM-Kennung können nur von einer Person erstellt werden, die die OEM-Kennung kennt oder die einen speziell für diesen Zweck konfigurierten PITreader verwendet. Siehe Transponder auf OEM-Codierung einlernen [📖 82].

Die OEM-Codierung kann manuell nur vom PITreader gelöscht werden, wenn die OEM-Kennung eingegeben wird. Beim Zurücksetzen auf Werkseinstellungen wird die OEM-Codierung nicht gelöscht. Siehe OEM-Codierung setzen [📖 72].

5.7 Blockierliste

Sie können die Authentifizierung bestimmter Transponder sperren. Ein in der Blockierliste enthaltener Transponder kann sich nicht mehr am PITreader authentifizieren. Diese Funktion kann beispielsweise nützlich sein, wenn ein Anwender seinen Transponder verloren hat. Somit kann verhindert werden, dass sich unbefugte Personen am PITreader authentifizieren.

Die Blockierliste kann bis zu 1000 Einträge enthalten.

Die Blockierliste kann in jedem Authentifizierungsmodus verwendet werden.
Siehe auch Blockierliste verwenden [📖 84].

5.8 Echtzeituhr und Betriebsstundenzähler

Der PITreader besitzt eine Echtzeituhr und einen Betriebsstundenzähler.
Die Echtzeituhr kann in der Web-Anwendung auf einen neuen Datum-/Zeitwert gesetzt werden.
In der Web-Anwendung kann die Synchronisation mit einem SNTP-Server aktiviert werden. Wenn ein SNTP-Server konfiguriert wurde, erfolgt erstmalig nach 10 Sekunden eine Synchronisation mit dem konfigurierten SNTP-Server. Anschließend wird in der durch den Anwender konfigurierten Zeit ein Abgleich mit dem SNTP-Server durchgeführt.

5.9 Synchronisierung mit externen Daten

Es gibt Daten auf dem PITreader (z. B. die Berechtigungsliste und die Blockierliste), die von einem externen Dienst (z. B. PIT User Authentication Service) aktualisiert werden können. Die Daten werden in einer Datenbank gepflegt und dann vom externen Dienst mit dem PITreader synchronisiert.

Um sicherzustellen, dass diese Synchronisierung auch tatsächlich erfolgt, kann die Synchronisierung überwacht werden. Es kann eine Zeit von 5 Minuten bis 3 Tagen konfiguriert werden, der sogenannte "Timeout der Synchronisierung". Wenn die Synchronisierung überwacht wird und innerhalb des Timeouts keine Synchronisierung erfolgt, dann wird die Authentifizierung von Transpondern gesperrt. Erst nachdem erneut eine Synchronisierung der Daten stattgefunden hat, ist die Authentifizierung von Transpondern wieder möglich. Die Überwachung der Synchronisierung beginnt erneut.

Wenn der PITreader ausgeschaltet wird, wird die bereits abgelaufene Zeit gespeichert und läuft weiter, wenn der PITreader wieder eingeschaltet wird. Ist die Zeit bis zum Eintreten des Timeouts beim Einschalten kürzer als 10 Minuten, dann wird sie automatisch auf 10 Minuten gesetzt. Somit steht nach dem Einschalten immer ein Zeitfenster von 10 Minuten für die erste Synchronisierung zur Verfügung.

Wenn ein Timeout auftritt, wird in der Diagnoseliste solange der Alarm "Es ist ein Timeout der Synchronisierung aufgetreten." angezeigt, bis eine erfolgreiche Synchronisierung der Daten stattgefunden hat.

Die Überwachung der Synchronisierung erhöht die Security. Ein potentieller Angreifer kann die Verbindung zwischen PITreader und externem Dienst nicht mehr unterbrechen, um die Aktualisierung der Daten auf dem PITreader zu verhindern.

Zur Konfiguration der Überwachung (siehe Überwachung der Synchronisierung konfigurieren [📖 86]).

5.10 Modbus/TCP

Über die Ethernet-Schnittstelle kann eine Modbus/TCP-Verbindung mit einer Steuerung (PLC, HMI) hergestellt werden. Es werden bis zu 4 Modbus/TCP-Verbindungen unterstützt. Der PITreader ist immer der Server (Modbus/TCP-Slave) einer Verbindung.

Die Port-Nummer für den Datenaustausch über Modbus/TCP ist konfigurierbar, die Standard-Port-Nummer ist 502.
Die Modbus/TCP-Server-Funktion kann in der Web-Anwendung deaktiviert werden.

5.10.1 Steuerung der LED

Farbe und Blinkmodus der LED kann über die Modbus/TCP-Verbindung überschrieben werden.
Die Farbe der LED kann einen der folgenden Werte annehmen:

- 0 = ausgeschaltet (Default-Einstellung)
- 1 = blau
- 2 = gelb
- 3 = rot
- 4 = grün

Der Blinkmodus kann einen der folgenden Werte annehmen:

- 0 = Dauerlicht (Default-Einstellung)
- 1 = langsames Blinken (1 Hz)

5.10.2 Function Codes (Client-Verbindungen)

Der Modbus/TCP-Server im PITreader unterstützt die folgenden Function Codes (FC):

Function Code	Funktion	
02	Read Discrete Input	Der Client einer Verbindung liest Bit-Daten vom Server der Verbindung, Datenlänge ≥ 1 Bit, (Daten empfangen aus 1x)
03	Read Holding Register	Der Client einer Verbindung liest Wort-Daten vom Server der Verbindung, Datenlänge ≥ 1 Wort, (Daten empfangen aus 4x)
04	Read Input Register	Der Client der Verbindung liest Wort-Daten vom Server der Verbindung, Datenlänge ≥ 1 Wort, (Daten empfangen aus 3x)
06	Write Single Register	Der Client der Verbindung schreibt auf ein Wort-Datum im Server der Verbindung, Datenlänge = 1 Wort, (Daten senden nach 4x)
16	Write Multiple Registers	Der Client einer Verbindung schreibt auf mehrere Wort-Daten im Server der Verbindung, Datenlänge ≥ 1 Wort, (Daten senden nach 4x)

5.10.3 Modbus/TCP-Datenbereiche

INFO

Beim PITreader beginnt die Adressierung für Modbus/TCP-Datenbereiche bei "1". Bei anderen Geräten kann die Adressierung mit "0" beginnen. Beachten Sie die Bedienungsanleitung des entsprechenden Herstellers.

Das Produkt unterstützt die folgenden Modbus/TCP-Datenbereiche:

- Discrete Inputs (Bit)
  PITreader -> Modbus Client, Bitzugriff lesend (mit FC02)

Adresse	Inhalt
1x4001	Ist authentifiziert (Daten des Transponders)

- Input Register (Wort/16 Bits)
  PITreader -> Modbus Client, Registerzugriff lesend (mit FC04)

Adresse	Inhalt
3x0001 … 3x0002	PITreader Artikelnummer (codiert) Bits 31 bis 24: Produktgruppe (00 = leer, 01 = G1) Bits 19 bis 0: Produktnummer Beispiele: 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 Seriennummer
3x0005 ... 3x0006	Betriebsstundenzähler in Minuten
3x0007 ... 3x0008	RTC-Zeitstempel, Sekunden seit 01.01.2000 00:00 (UTC)
3x0009	LED-Farbe (siehe auch Steuerung der LED [43])
3x0010	LED-Blinkmodus (siehe auch Steuerung der LED [43])
3x0011	Diagnose-Status (Alle Diagnosemeldungen werden einem Schweregrad zugeordnet, Schweregrad 3 = Störung, Schweregrad 8 = Warnung, Schweregrad 13 = Statusinformation)
3x0012	reserviert
3x0013 … 3x0016	PITreader Artikelnummer (ASCII)
3x0017	PITreader Revision (ASCII)
3x0018	reserviert
3x0019	SEU-Statusinformation (siehe auch Bedienungsanleitung PIT m4SEU, Kapitel 5.5) Standardwert wenn keine SEU angeschlossen ist: 0x00F0 (dezimal: 240)
3x0020 … 3x0024	reserviert
3x0025 … 3x0028	Security-ID (Daten des Transponders)
3x0029 … 3x0030	reserviert

Adresse	Inhalt
3x0031 … 3x0032	Berechtigung (Codewort)
3x0033	Berechtigung (Ganzzahl, 0 bis 64)
3x0034	Authentifizierungsstatus (0 = nicht authentifiziert, 1 = Transponder erfolgreich authentifiziert)
3x0035 … 3x0036	Artikelnummer (Transponder)
3x0037 … 3x0038	Seriennummer (Transponder) (siehe auch Auswertung der Seriennummer eines Transponders [📖 32])
3x0039 ... 3x0042	reserviert
3x0043 ... 3x0047	UID des Transponders nach ISO-Standard (4, 7 oder 10 Bytes); die Datenlänge steht im Register 3x0048
3x0048	Datenlänge der UID (Anzahl der Bytes)
3x0049 ... 3x0054	reserviert
3x0055 ... 3x0056	Startdatum, ab dem der Transponder gültig ist; Sekunden seit 01.01.2000 00:00 (UTC)
3x0057 ... 3x0058	Enddatum, bis zu dem der Transponder gültig ist; Sekunden seit 01.01.2000 00:00 (UTC)
3x0059 … 3x0060	Berechtigung Gruppe 0
3x0061 … 3x0062	Berechtigung Gruppe 1
3x0063 … 3x0064	Berechtigung Gruppe 2
3x0065 … 3x0066	Berechtigung Gruppe 3
3x0067 … 3x0068	Berechtigung Gruppe 4
3x0069 … 3x0070	Berechtigung Gruppe 5
3x0071 … 3x0072	Berechtigung Gruppe 6
3x0073 … 3x0074	Berechtigung Gruppe 7
3x0075 … 3x0076	Berechtigung Gruppe 8
3x0077 … 3x0078	Berechtigung Gruppe 9
3x0079 … 3x0080	Berechtigung Gruppe 10
3x0081 … 3x0082	Berechtigung Gruppe 11
3x0083 … 3x0084	Berechtigung Gruppe 12
3x0085 … 3x0086	Berechtigung Gruppe 13
3x0087 … 3x0088	Berechtigung Gruppe 14
3x0089 … 3x0090	Berechtigung Gruppe 15
3x0091 … 3x0092	Berechtigung Gruppe 16
3x0093 … 3x0094	Berechtigung Gruppe 17
3x0095 … 3x0096	Berechtigung Gruppe 18
3x0097 … 3x0098	Berechtigung Gruppe 19
3x0099 … 3x0100	Berechtigung Gruppe 20
3x0101 … 3x0102	Berechtigung Gruppe 21
3x0103 … 3x0104	Berechtigung Gruppe 22

Adresse	Inhalt
3x0105 … 3x0106	Berechtigung Gruppe 23
3x0107 … 3x0108	Berechtigung Gruppe 24
3x0109 … 3x0110	Berechtigung Gruppe 25
3x0111 … 3x0112	Berechtigung Gruppe 26
3x0113 … 3x0114	Berechtigung Gruppe 27
3x0115 … 3x0116	Berechtigung Gruppe 28
3x0117 … 3x0118	Berechtigung Gruppe 29
3x0119 … 3x0120	Berechtigung Gruppe 30
3x0121 …3x0122	Berechtigung Gruppe 31
3x0123 ... 3x0158	reserviert
3x0159 … 3x0166	Prüfsumme der Basis-Codierung
3x0167 … 3x0174	Prüfsumme der OEM-Codierung
3x0175 ... 3x0999	reserviert
3x1000 … 3x1519	Anwenderdaten (siehe auch Info unten und Anwenderdaten [📖 37])
3x1520 ... 3x9999	reserviert

INFO

Werte aus den Anwenderdaten starten immer an Registergrenzen. Bei Daten, die nur eine Datenbreite von 1 Byte benötigen, wird der eigentliche Wert in das Low-Byte geschrieben und das High-Byte mit „0“ aufgefüllt.
Die Adresse des Modbus/TCP-Registers wird in der Web-Anwendung unter ***Konfiguration -> Anwenderdaten*** angezeigt. Die Adresse kann auch mit folgender Formel berechnet werden:
$Adresse_n = Adresse_{(n-1)} + Aufrunden_{2\text{-}Byte}\ (Länge_{(n-1)})$

- Holding Register (Wort/16 Bits)
  Modbus Client -> PITreader, Registerzugriff lesend (mit FC03) und schreibend (mit FC06 oder FC16)

Adresse	Inhalt
4x6001	Farbe überschreiben (PITreader LED-Zugriff)
4x6002	Blinkmodus überschreiben (PITreader LED-Zugriff)
4x6003	Überschreiben aktivieren (=1) oder deaktivieren (=0)

INFO

Beim Lesen von Datenbereichen, die keine Daten enthalten, wird "0" zurückgegeben.

5.10.3.1 Grenzen bei der Datenübertragung

Diese Tabelle enthält die maximal unterstützten Datenlängen pro Telegramm:

Datenübertragung		max. Datenlänge pro Telegramm
Daten lesen (Bit)	FC 02 (Read Discrete Inputs)	1 … 2000
Daten lesen (Wort)	FC 03 (Read Holding Registers)	1 … 125
	FC 04 (Read Input Registers)	
Daten schreiben (Wort)	FC 06 (Write Single Register)	1 Wort
	FC 16 (Write Multiple Registers)	1 … 123 Worte

5.11 HTTP(S)-Verbindung

Über die Ethernet-Schnittstelle kann eine Verbindung mit einem Konfigurations-Rechner hergestellt werden. Der PITreader kann über eine Web-Anwendung konfiguriert werden und es können Transponder ausgelesen und beschrieben werden (siehe auch Kapitel Konfiguration [66] und Firmware-Update [90]).

5.12 24 V-I/O-Port

Der PITreader verfügt über einen 24 V-I/O-Port. Im Auslieferungszustand ist dem I/O-Port keine Funktion zugewiesen. Der I/O-Port kann in der Web-Anwendung entweder als Ausgang oder als Eingang konfiguriert werden.

I/O-Port als Ausgang

Wenn der I/O-Port als Ausgang konfiguriert ist, kann über diesen Ausgang der aktuelle Authentifizierungsstatus ausgegeben werden.
In der Web-Anwendung kann die minimale Berechtigung des Transponders eingestellt werden, ab welcher der Ausgang eingeschaltet werden soll. Wenn die Berechtigung des Transponders der eingestellten Berechtigung entspricht oder höher ist, nimmt der Ausgang den Status "1" an.

I/O-Port als Eingang

Wenn der I/O-Port als Eingang konfiguriert ist, kann über diesen Eingang eine Authentifizierungssperre aktiviert werden. Die Authentifizierungssperre ist aktiv, solange an dem Eingang 24 V anliegen.

Hinweis: Die Authentifizierungssperre funktioniert unabhängig vom Authentifizierungstyp "Einzelauthentifizierung" (siehe Authentifizierungstypen [26]).

5.13 Verbindung der Basiseinheit mit einer sicheren Auswerteeinheit

Über die Klemmen TxD/RxD von X1 kann eine sichere Auswerteeinheit PIT m4SEU an einen PITreader Key oder PITreader Card angeschlossen werden (siehe auch Bedienungsanleitung PIT m4SEU).

6 Montage und Demontage

6.1 Allgemeine Hinweise zur Montage und Demontage

WICHTIG

Beschädigung durch elektrostatische Entladung!

Durch elektrostatische Entladung können Bauteile beschädigt werden. Sorgen Sie für Entladung, bevor Sie das Produkt berühren, z. B. durch Berühren einer geerdeten, leitfähigen Fläche oder durch Tragen eines geerdeten Armbands.

WICHTIG

Beschädigung durch Montage/Demontage unter Spannung!

Durch die Montage/Demontage unter Spannung können Bauteile beschädigt werden. Stellen Sie sicher, dass das Produkt spannungsfrei geschaltet ist, bevor Sie es montieren/demontieren.

6.2 Montage und Demontage eines PITreader Key

6.2.1 Montage PITreader Key

Vorgehensweise

- Montieren Sie das Gerät in die Frontplatte eines Schaltschranks oder in ein Bedienpult.

  Maximal erlaubte Materialstärke:

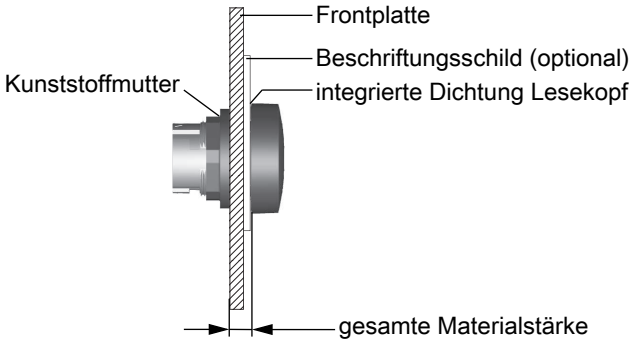
  – nicht metallische Frontplatte: 2 … 6 mm

  – metallische Frontplatte: 2 … 4 mm.

  Beachten Sie: Die gesamte Materialstärke ist bei montiertem Lesekopf der Abstand von der Auflage der Kunstoffmutter bis einschließlich der integrierten Dichtung des Lesekopfs; d. h.:

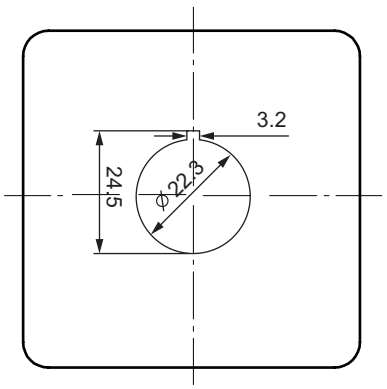
  $Materialstärke_{maximal} = Materialstärke_{Frontplatte} + Materialstärke_{optionale\ Materialien}$

  Als "optionale Materialien" gelten z. B. Beschriftungsschilder. Bei korrekter Montage kann die Materialstärke der Dichtung vernachlässigt werden.



- Versehen Sie die Frontplatte des Schaltschranks oder das Bedienpult mit einer Einbauöffnung (Ø 22,3 mm +0,4 mm/-0,0 mm, D22 gemäß EN 60947-5-1) und versehen Sie die Öffnung mit einer Aussparung für die Rastnase des Lesekopfs PITreader key Adapter h. Die Rastnase dient als Verdrehschutz.

  Beispiel:



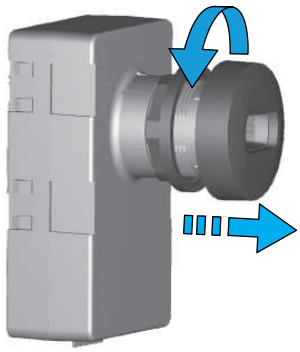
  Im Beispiel ist die Position der Aussparung so angebracht, dass die Basiseinheit entweder mit Kabelabgang nach oben oder unten eingebaut werden kann.

  Beachten Sie: Durch die Positionierung der Rastnase sind bezüglich des Kabelabgangs der Basiseinheit zwei unterschiedliche Einbauweisen möglich. Die Basiseinheit kann entweder so montiert werden, dass die Rastnase in Richtung des Kabelabgangs zeigt oder,

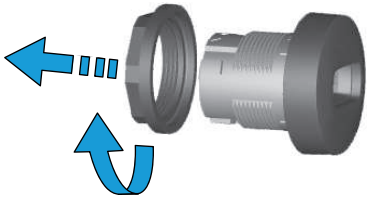
dass die Rastnase in die entgegengesetzte Richtung zeigt (Basiseinheit um 180° verdreht). Positionieren Sie die Aussparung so, dass Sie den gewünschten Kabelabgang erzielen.

- Wenn bei Ihrem Gerät der Lesekopf nicht an der Basiseinheit montiert ist, können Sie diesen Schritt überspringen.

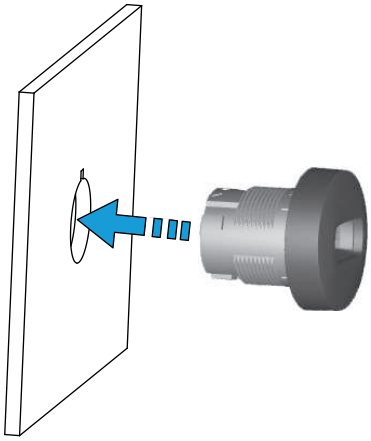
  Sonst:
  Halten Sie die Basiseinheit fest, drehen Sie den Lesekopf um 15° gegen den Uhrzeigersinn und ziehen Sie den Lesekopf aus der Basiseinheit.



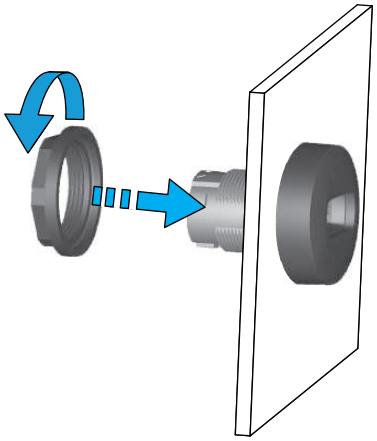
- Entfernen Sie die Kunststoffmutter (M22) vom Lesekopf.



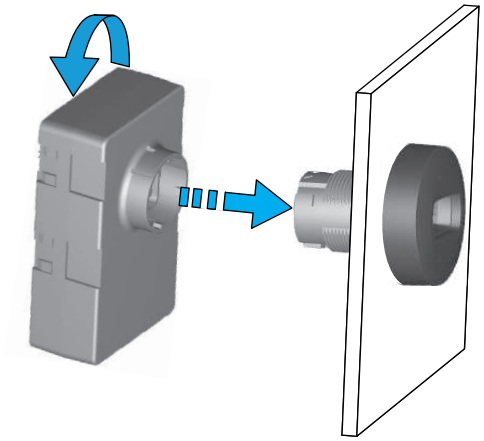
- Stecken Sie den Lesekopf von vorne so in die Einbauöffnung, dass sich die Rastnase in der Aussparung der Einbauöffnung befindet.



- Befestigen Sie den Lesekopf von der anderen Seite mit der Kunststoffmutter (M22). Beachten Sie das Anzugsdrehmoment von 1,3 … 2,1 Nm. Wir empfehlen Ihnen, für die Befestigung der Kunststoffmutter den Montageschlüssel "PIT es wrench" zu verwenden (siehe Bestelldaten [📖 111]).



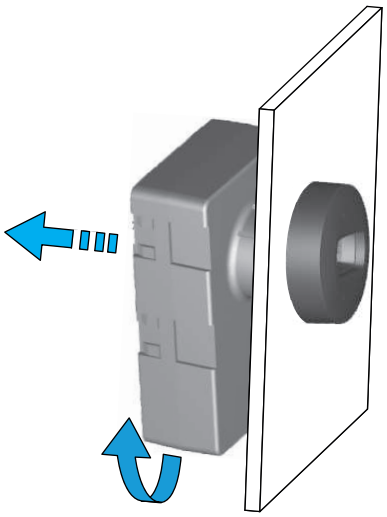
- Stecken Sie die Basiseinheit auf den Lesekopf und drehen Sie die Basiseinheit im Uhrzeigersinn um 15°, bis sie einrastet.



6.2.2 Demontage PITreader Key

Vorgehensweise

- Schalten Sie den PITreader spannungsfrei.
- Drehen Sie die Basiseinheit um 15° gegen den Uhrzeigersinn.
- Ziehen Sie leicht an der Basiseinheit des PITreader bis sich die Basiseinheit vom Lesekopf löst.



6.3 Montage und Demontage eines PITreader Card

6.3.1 Montage PITreader Card

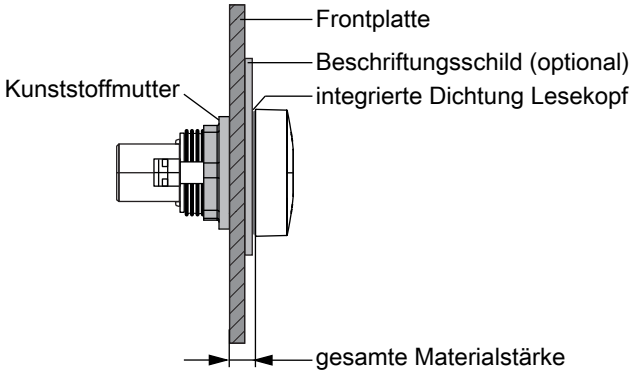
Vorgehensweise

- Montieren Sie das Gerät in die Frontplatte eines Schaltschranks oder in ein Bedienpult. Maximal erlaubte Materialstärke: 2 … 6 mm

  Beachten Sie: Die gesamte Materialstärke ist bei montiertem Lesekopf der Abstand von der Auflage der Kunstoffmutter bis einschließlich der integrierten Dichtung des Lesekopfs; d. h.:

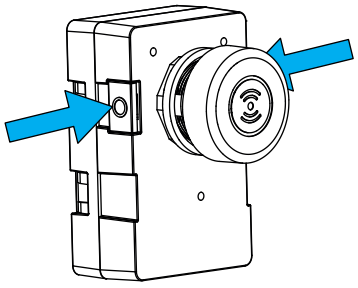
  $\text{Materialstärke}_{\text{maximal}} = \text{Materialstärke}_{\text{Frontplatte}} + \text{Materialstärke}_{\text{optionale Materialien}}$

  Als "optionale Materialien" gelten z. B. Beschriftungsschilder. Bei korrekter Montage kann die Materialstärke der Dichtung vernachlässigt werden.



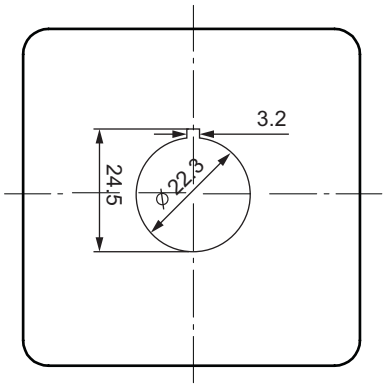
  Die gesamte Materialstärke darf die maximal erlaubte Materialstärke nicht überschreiten.

- Beachten Sie das Folgende bezüglich des Montageorts:
  - Berücksichtigen Sie bei der Montage einen ausreichenden seitlichen Abstand, damit Sie zur Demontage die beiden Entriegelungsknöpfe betätigen können.



  - Wenn Sie bei einer NICHT-metallischen Frontplatte mehrere PITreader Card nebeneinander montieren möchten, dann muss zwischen zwei PITreader Card ein Mindestabstand von 15 cm eingehalten werden.
- Versehen Sie die Frontplatte des Schaltschranks oder das Bedienpult mit einer Einbauöffnung (Ø 22,3 mm +0,4 mm/-0,0 mm, D22 gemäß EN 60947-5-1) und versehen Sie die Öffnung mit einer Aussparung für die Rastnase des Lesekopfs PITreader card Adapter. Die Rastnase dient als Verdrehschutz.

Beispiel:

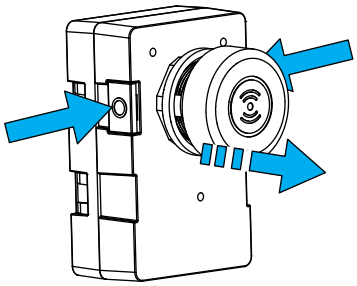


Im Beispiel ist die Position der Aussparung so angebracht, dass das Kabel der Basiseinheit nach oben abgeht.

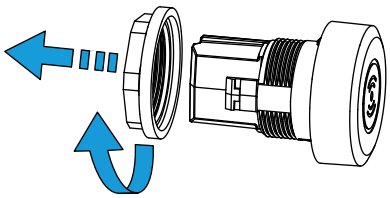
Beachten Sie: Die Aussparung für die Rastnase des Lesekopfs zeigt in Richtung des Kabelabgangs der Basiseinheit. Positionieren Sie die Aussparung so, dass Sie den gewünschten Kabelabgang erzielen.

- Wenn bei Ihrem Gerät der Lesekopf nicht an der Basiseinheit montiert ist (z. B. Auslieferungszustand), können Sie diesen Schritt überspringen.

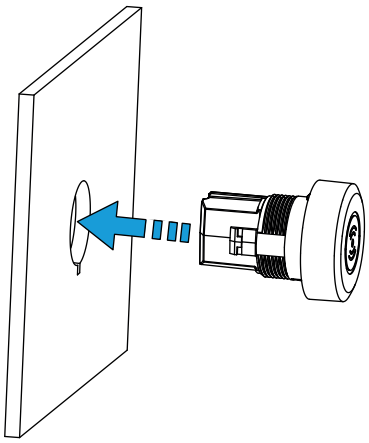
  Sonst:
  Drücken Sie seitlich am Gehäuse der Basiseinheit die beiden Entriegelungsknöpfe, halten Sie diese gedrückt und ziehen Sie den Lesekopf aus der Basiseinheit.



- Entfernen Sie die Kunststoffmutter (M22) vom Lesekopf.



- Stecken Sie den Lesekopf von vorne so in die Einbauöffnung, dass sich die Rastnase in der Aussparung der Einbauöffnung befindet.

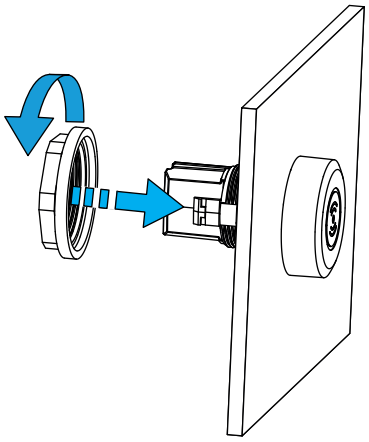


- Richten Sie die Silikonkappe des Lesekopfs in der gewünschten Richtung aus.

  Hinweis: Die Rastnase muss sich nach der Ausrichtung in einer der Aussparungen der Silikonkappe befinden.

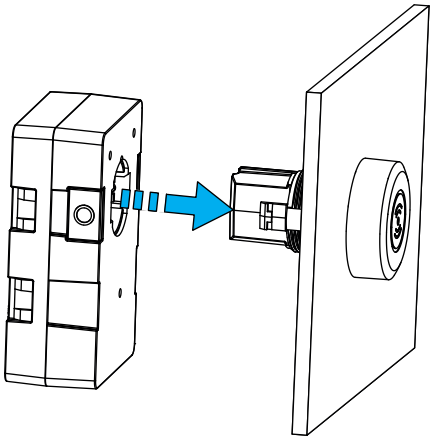
- Befestigen Sie den Lesekopf von der anderen Seite mit der Kunststoffmutter (M22).

  Beachten Sie das Anzugsdrehmoment von 1,3 … 2,1 Nm. Wir empfehlen Ihnen, für die Befestigung der Kunststoffmutter den Montageschlüssel "PIT es wrench" zu verwenden (siehe Bestelldaten [📖 111]).



- Stecken Sie die Basiseinheit auf den Lesekopf.

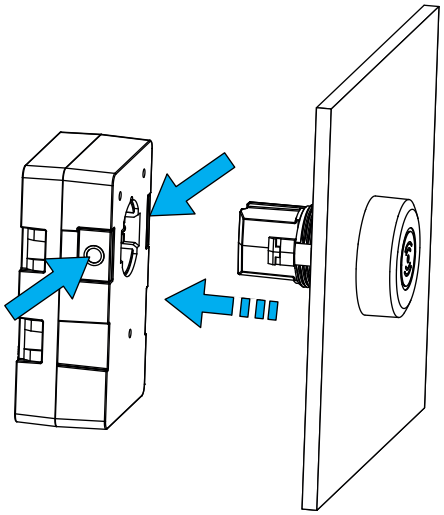
  Die Basiseinheit muss einrasten.



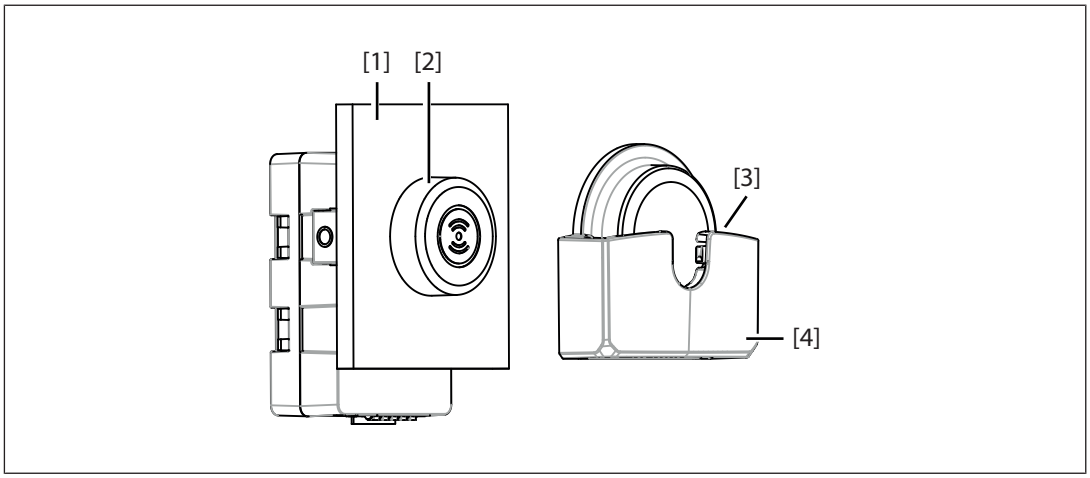
6.3.2 Demontage PITreader Card

Vorgehensweise

- Schalten Sie den PITreader spannungsfrei.
- Drücken Sie seitlich am Gehäuse der Basiseinheit die beiden Entriegelungsknöpfe und halten Sie diese gedrückt.
- Ziehen Sie leicht an der Basiseinheit des PITreader bis sich die Basiseinheit vom Lesekopf löst.



6.3.3 Montage PITreader card holder



- Reinigen Sie die Frontplatte [1] rund um den Lesekopf [2]. Die Aufklebeposition muss glatt, schmutz-, staub- und fettfrei sein.
- Ziehen Sie am PITreader card holder [4] die Schutzfolie von der Klebefläche ab. Berühren Sie dabei nicht die Klebefläche, damit die Klebefunktion nicht beeinträchtigt wird.
- Führen Sie den PITreader card holder [4] etwas über den Lesekopf [2], dabei muss die Öffnung [3] des PITreader card holders [4] nach oben zeigen.
- Richten Sie den PITreader card holder [4] waagerecht aus.
- Führen Sie den PITreader card holder [4] weiter über den Lesekopf [2], bis dieser an der Frontplatte [1] anliegt.

- Drücken Sie den PITreader card holder [4], rund um den Lesekopf [2], fest auf die Frontplatte [1].

6.3.4 PITreader Transponder-Sticker aufkleben

Der PITreader Transponder-Sticker hat eine selbstklebende Seite und kann auf eine bereits vorhandene Karte, z. B. Firmenausweis, geklebt werden. Die Karte wird dann als Träger-Karte bezeichnet. Auf diese Weise lässt sich die Anzahl der erforderlichen Karten reduzieren.

WICHTIG

Beeinträchtigung der Transponder-Erkennung

Wird der PITreader Transponder-Sticker auf eine metallische Träger-Karte geklebt, kann der Transponder vom PITreader möglicherweise nicht erkannt werden.

Kleben Sie den PITreader Transponder-Sticker nicht auf eine metallische Träger-Karte.

WICHTIG

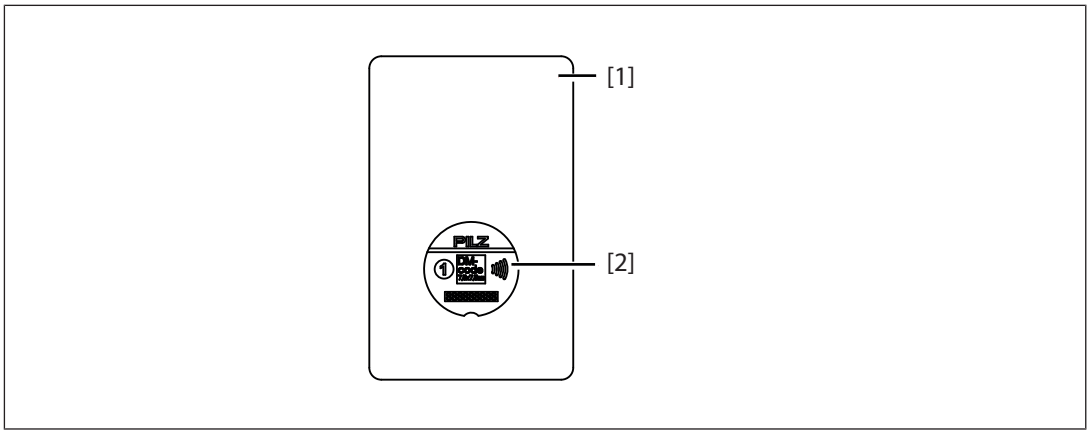
Funktionsbeeinträchtigung der Träger-Karte oder des PITreader Transponder-Stickers

Wird der PITreader Transponder-Sticker auf eine Funktionsfläche der Träger-Karte geklebt, z. B. Magnetstreifen oder Kontaktfläche einer Chipkarte, können Funktionen der Träger-Karte nicht mehr zur Verfügung stehen oder beeinträchtigt sein.

Der PITreader Transponder-Sticker und die Träger-Karte mit RFID Funktion können sich gegenseitig beeinträchtigen und dadurch können nicht alle Funktionen zur Verfügung stehen.

- Kleben Sie den PITreader Transponder-Sticker nur auf Flächen ohne Funktion. Benutzen Sie gegebenenfalls eine andere Träger-Karte.
- Prüfen Sie nach dem Aufkleben des PITreader Transponder-Stickers die Funktionen des PITreader Transponder-Stickers und der Träger-Karte.

6.3.4.1 Verwendung ohne PITreader card holder



- Reinigen Sie die Träger-Karte [1] auf der Sie den PITreader Transponder-Sticker [2] aufkleben möchten. Die Aufklebeposition muss schmutz-, staub- und fettfrei sein.
- Ziehen Sie am PITreader Transponder-Sticker [2] die Schutzfolie von der Klebefläche ab. Berühren Sie dabei nicht die Klebefläche, damit die Klebefunktion nicht beeinträchtigt wird.
- Kleben Sie den PITreader Transponder-Sticker [2] auf die Träger-Karte [1].

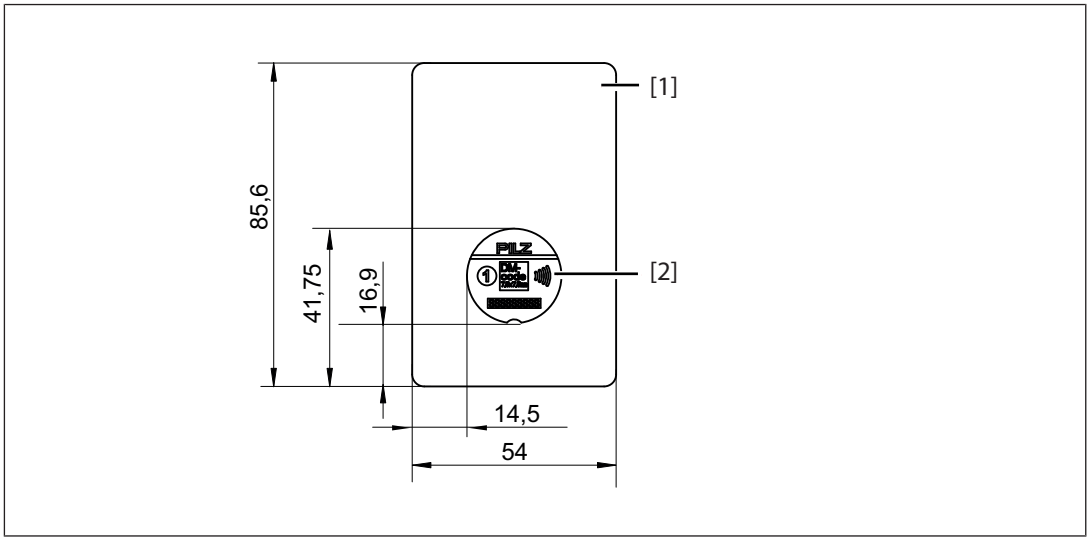
6.3.4.2 Verwendung mit PITreader card holder

WICHTIG

Beeinträchtigung der Transponder-Lesbarkeit

Wenn der PITreader Transponder-Sticker nicht auf die vorgegebene Aufklebeposition der Träger-Karte geklebt wird, kann der Transponder möglicherweise nicht von PITreader Card erkannt werden.

- Kleben Sie den PITreader Transponder-Sticker nur auf die vorgegebene Aufklebeposition.
- Kleben Sie den PITreader Transponder-Sticker nur auf Flächen ohne Funktion. Benutzen Sie gegebenenfalls eine andere Träger-Karte.



- Verwenden Sie eine Träger-Karte [1] mit den angegebenen Abmessungen.
- Reinigen Sie die Träger-Karte [1] im Bereich der Aufklebeposition des PITreader Transponder-Stickers [2].
  Die Aufklebeposition muss schmutz-, staub- und fettfrei sein.
- Ziehen Sie am PITreader Transponder-Sticker [2] die Klebefläche-Schutzfolie ab.
  Berühren Sie dabei nicht die Klebefläche, damit die Klebefunktion nicht beeinträchtigt wird.
- Kleben Sie den PITreader Transponder-Sticker [2] auf die Aufklebeposition der Träger-Karte [1].

6.4 Montage und Demontage eines PIT gb mit PITreader

Sie finden die erforderlichen Informationen in der Bedienungsanleitung PIT gb mit PITreader.

6.5 Abmessungen

6.5.1 Abmessungen PITreader Key

Abmessungen in mm

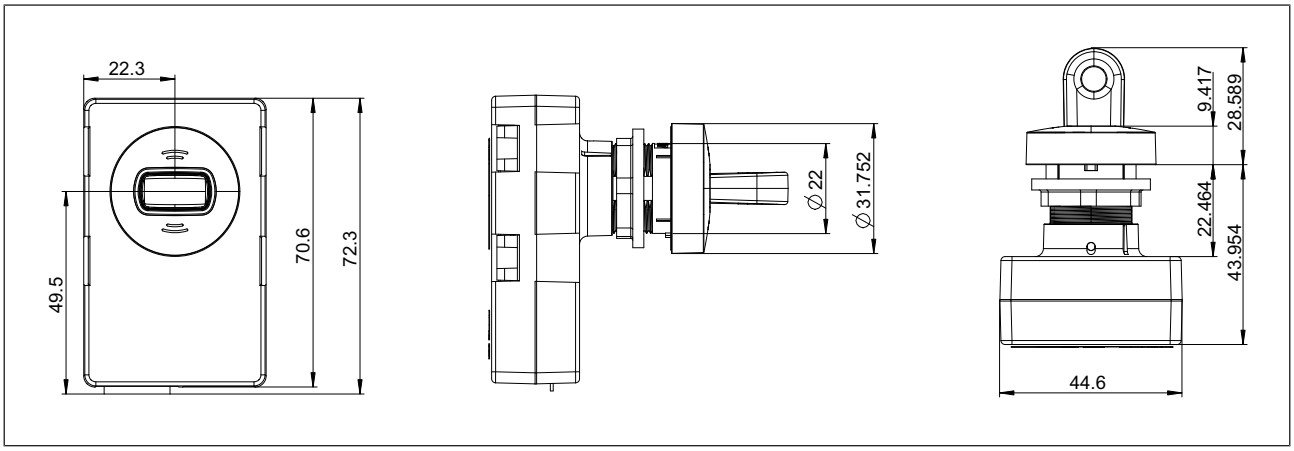


Abb.: Abmessungen eines PITreader Key (Basiseinheit mit Federkraftklemme, Lesekopf PITreader key adapter h und platziertem Transponder-Schlüssel)

6.5.2 Abmessungen PITreader Card

Abmessungen in mm

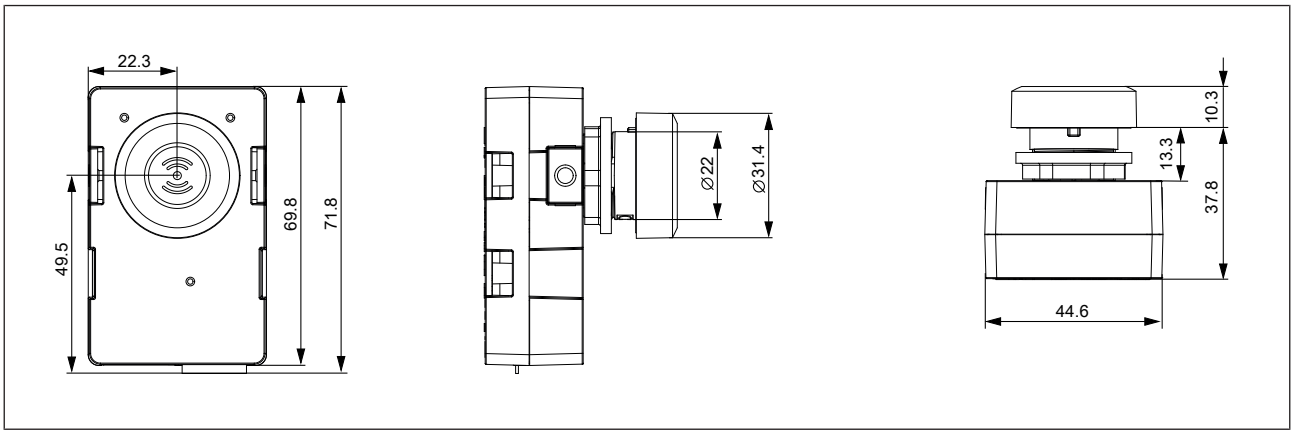


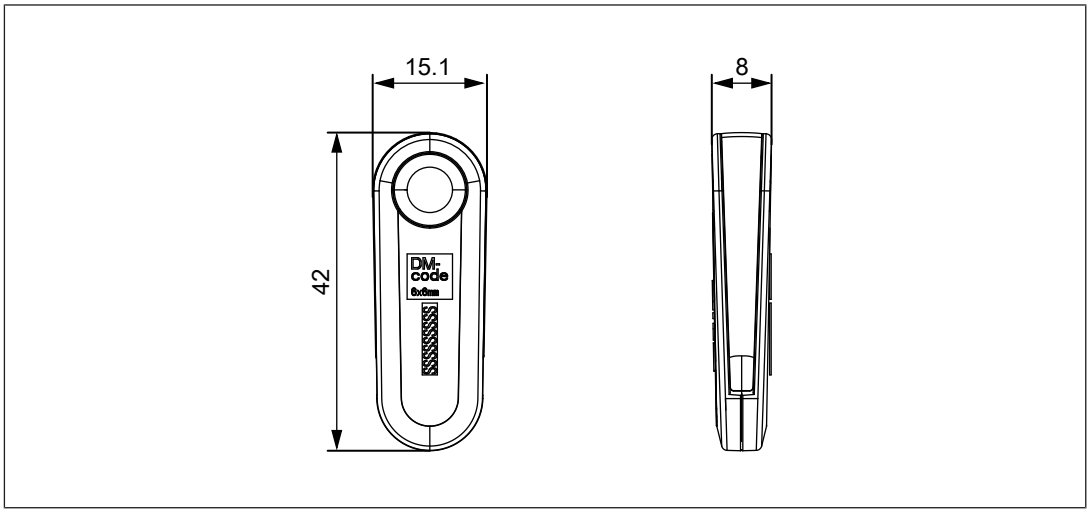
Abb.: Abmessungen eines PITreader Card (Basiseinheit mit Federkraftklemme und Lesekopf PITreader card adapter)

6.5.3 Abmessungen PIT gb mit PITreader

Sie finden die erforderlichen Informationen in der Bedienungsanleitung PIT gb mit PITreader.

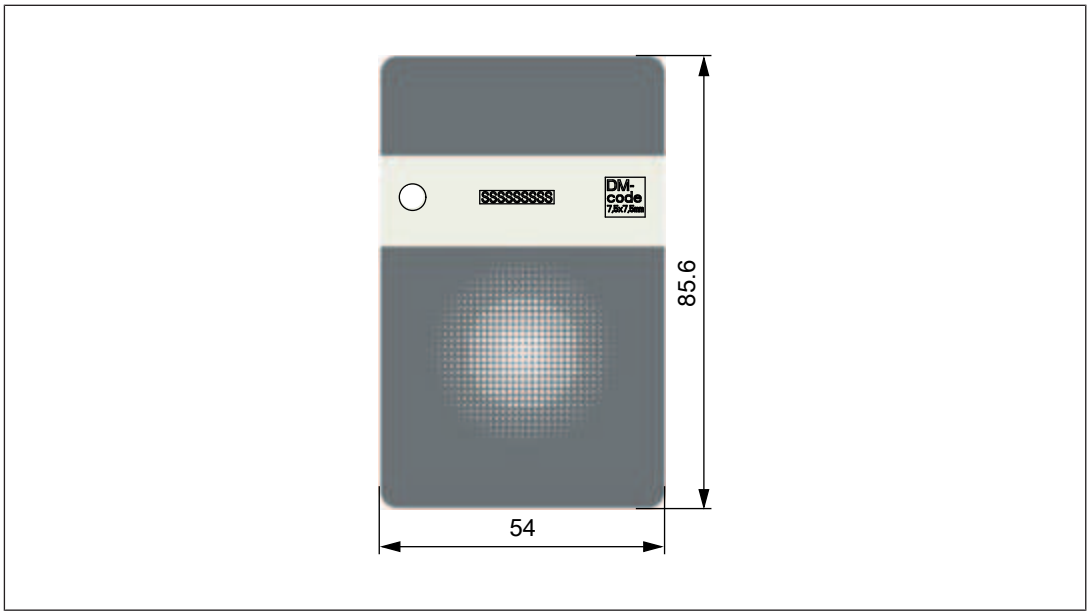
6.5.4 Abmessungen PITreader Transponder-Schlüssel

Abmessungen in mm



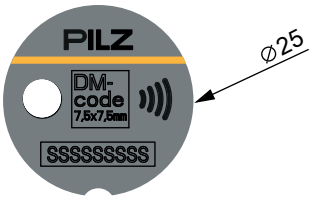
6.5.5 Abmessungen PITreader Transponder-Karte

Abmessungen in mm



6.5.6 Abmessungen PITreader Transponder-Sticker

Abmessungen in mm



7 Verdrahtung

7.1 Basiseinheit ohne sichere Auswerteeinheit (Standalone)

Hier ist beschrieben, wie Sie die Basiseinheit eines PITreader Key oder eines PITreader Card verdrahten, wenn Sie keine sichere Auswerteeinheit (SEU) verwenden.

Informationen zur Verdrahtung der PIT gb mit PITreader finden Sie in der Bedienungsanleitung PIT gb mit PITreader.

Vorgehensweise

1. Versorgungsspannung anschließen
   ⇨ Schließen Sie die Versorgungsspannung an X1 (Pin "24V" und "0V") an.
   Beachten Sie unbedingt:
   Das Netzteil muss den Vorschriften für Kleinspannungen mit sicherer elektrischer Trennung (SELV, PELV) entsprechen.
   Die Leitungen für die Versorgungsspannung des Geräts müssen mit einer Sicherung 4 A, Charakteristik B/C abgesichert werden.
2. Verbinden Sie den PITreader über die Ethernet-Schnittstelle (X2) mit einer Steuerung (PLC, HMI).

7.2 Basiseinheit mit sicherer Auswerteeinheit

Informationen zur Verdrahtung eines PITreader Key oder eines PITreader Card mit einer sicheren Auswerteeinheit PIT m4SEU finden Sie in der Bedienungsanleitung PIT m4SEU.

8 Konfiguration

8.1 Web-Anwendung

Die Konfiguration des PITreader wird mithilfe einer Web-Anwendung vorgenommen. Die Konfiguration ist nur nach vorheriger Anmeldung an der Web-Anwendung möglich.
Die Web-Anwendung steht auf Deutsch und Englisch zur Verfügung.

Systemvoraussetzungen:

Die Web-Anwendung wird über einen Standard-Browser aufgerufen.
Folgende Web-Browser werden unterstützt:

- Microsoft Edge, alle Versionen
- Mozilla Firefox, ab Version 52
- Google Chrome, ab Version 48

Andere Web-Browser können funktionieren, wurden aber nicht getestet.

Über HTTPS kann eine sichere Verbindung zum PITreader aufgebaut werden. Der PITreader unterstützt HTTPS-Verbindungen mit TLS v1.2.

8.2 Netzwerkerkennung mit Multicast DNS (mDNS)

Über das Multicast-DNS-Protokoll (mDNS) kann ein PITreader im Netzwerk aufgefunden werden.

PITreader können über mDNS unter folgenden beiden Domain-Namen gefunden werden:

- pitreader.pilz.local
  Über die Adresse pitreader.pilz.local können alle PITreader in einem Netzwerk gefunden werden.
- pilz-<Artikelnummer>-<Seriennummer>.local
  Über die Adresse pilz-<Artikelnummer>-<Seriennummer>.local kann ein einzelner PITreader gezielt in einem Netzwerk angesprochen werden.

Eine Multicast DNS-Anfrage verwendet die Multicast IPv4-Gruppenadresse 224.0.0.251.
Multicast DNS-Anfragen an einen PITreader erfolgen über UDP und über den Port 5353.
Ein PITreader antwortet auf folgende Multicast DNS-Anfragen:

- QTYPE: ANY, A
- CLASS: IN

Multicast DNS-Anfragen mit QTYPE ANY enthalten die folgenden Antwortteile:

- IP-Adresse des PITreader
- Hostname und Domain
- HTTPS-Portnummer
- Artikelnummer
- Seriennummer
- MAC-Adresse

Multicast DNS-Anfragen mit QTYPE A enthalten die folgenden Antwortteile:

- <IP-Adresse des PITreader>

Die Netzwerkerkennung über mDNS ist im Auslieferungszustand eines PITreader aktiv und kann vom Anwender über die Geräteeinstellungen deaktiviert werden.

8.3 Netzwerkkonfiguration über Multicast-Protokoll

Über IPv4-Multicast kann ein Gerät in Betrieb genommen werden, ohne dass sich der Anwender mit seinem Endgerät im selben Subnetz befinden muss. Dies ist z. B. mit dem PIT Transponder Manager ab Version 01.02.00 möglich.
Über IPv4-Multicast kann die IP-Konfiguration des Gerätes vorgenommen werden:

- IP-Adresse
- Subnetz-Maske
- Standard-Gateway

Über IPv4-Multicast ist es möglich die LED blinken zu lassen, die zum Auffinden, Lokalisieren oder Identifizieren des Geräts dient.
Zur Konfiguration über IPv4-Multicast hört das Gerät auf der IPv4-Multicast-Adresse 239.255.0.12 und UDP-Port 7075.

Die Konfiguration über IPv4-Multicast ist nur möglich, wenn für den Standard-Benutzer "admin" noch das Kennwort entsprechend dem Auslieferungszustand aktiv ist.

Die Netzwerkkonfiguration über Multicast-Protokoll ist im Auslieferungszustand eines PITreader aktiv und kann vom Anwender über die Geräteeinstellungen deaktiviert werden.

8.4 Verbindung zum PITreader herstellen

Im folgenden Abschnitt ist die typische Vorgehensweise zum Herstellen einer Verbindung zum PITreader und zum Öffnen der Web-Anwendung beschrieben.

1. **Ethernet-Verbindung herstellen**
   ⇨ Verbinden Sie den Konfigurations-PC direkt mit der Ethernet-Schnittstelle X2 des PITreader**.**
2. **IP-Adresse des Konfigurations-PC anpassen**

   Um auf den PITreader zugreifen zu können, muss sich die IP-Adresse des PC im selben Subnetz befinden wie die IP-Adresse des PITreader.

   Default-Einstellung PITreader :

   IP-Adresse: 192.168.0.12
   Netzmaske: 255.255.255.0

   ⇨ Ändern Sie die IP-Adresse in den Netzwerkeinstellungen Ihres Konfigurations-PC.
3. **Web-Anwendung aufrufen**
   ⇨ Starten Sie den Web-Browser und geben Sie die IP-Adresse des PITreader ein.

   Wird im Internet-Browser ein Zertifikatsfehler angezeigt, dann fügen Sie temporär eine Ausnahmeregel hinzu und/oder umgehen Sie diese Warnmeldung, um dennoch auf die Web-Anwendung zuzugreifen (siehe auch Zertifikate verwalten [📖 70]).

   Es wird die Startseite angezeigt. Um Änderungen an der Konfiguration vorzunehmen, müssen Sie sich an der Web-Anwendung anmelden.
4. **An der Web-Anwendung anmelden**

⇨ Klicken Sie rechts oben auf ***Login*** und geben Sie den Anwendernamen und das Kennwort ein.

Default-Anmeldedaten:

Anwendername: admin

Kennwort: <Seriennummer des PITreader> (die Seriennummer befindet sich auf der Unterseite des Geräts (siehe Geräteansicht PITreader Key [📖 12]).

Nach 5 Fehlversuchen ist die Anmeldung für 5 Minuten gesperrt.

5. **Default-Kennwort ändern**

   Die Meldung "Das Default-Kennwort wurde nicht geändert" wird angezeigt. Ändern Sie unter ***Anwender -> Profil -> Kennwort ändern*** das Default-Kennwort. Geben Sie ein sicheres Kennwort mit mindestens 8 Zeichen ein (Merkmale eines sicheren Kennworts siehe Security [📖 18]).

6. **Netzwerkeinstellungen ändern**

   Zur Integration des PITreader in ein bestehendes Netzwerk, ändern Sie die Netzwerkeinstellungen des PITreader. Die Einstellungen werden in der Web-Anwendung unter ***Konfiguration -> Einstellungen*** angepasst. Klicken Sie auf den Button ***Speichern*** um die Änderungen zu übernehmen.

7. **Web-Anwendung mit der neuen IP-Adresse starten**

   Nach dem Ändern der Netzwerkeinstellungen startet der PITreader neu und ist anschließend unter der neuen IP-Adresse erreichbar.

8.5 Geräteanwender

In der Web-Anwendung können unter ***Anwender -> Geräteanwender*** zusätzliche Geräteanwender angelegt werden. Es ist bereits ein Geräteanwender "admin" mit den folgenden Eigenschaften angelegt:

- Status: aktiv
- Rolle: Administrator
- Authentifizierung: Name/Kennwort
- Kennwort: Seriennummer des PITreaders

Den Geräteanwendern können Rollen mit unterschiedlichen Berechtigungen zugewiesen werden.

Wenn neue Geräteanwender angelegt werden, sollten nur die erforderlichen Zugriffsrechte über die entsprechende Rolle zugewiesen werden. Dies hilft dabei, die Sicherheit und den Zugriff auf Daten zu kontrollieren.

Es gibt 4 Rollen:

	Administrator	Geräteverwalter	Transponder-Verwalter	Gast (Lesezugriff)
Geräteeinstellungen	R/W	R/W*	R	R
TLS-Konfiguration	R/W	R	R	R
OPC UA-Konfiguration	R/W	R/W		
Basis-Codierung	R/W	R/W	R	R
OEM-Codierung	R/W	-	-	-
Gerätegruppen-Namen	R/W	R/W	R	R
Anwenderdaten-Konfiguration	R/W	R/W	R	R
Fremdtransponder unterstützen	R/W	R	R	R
Kryptographische Schlüssel	R/W	R/W	-	-
Geräteanwender verwalten	R/W	R/W**	-	-
Berechtigungsliste	R/W	R/W	R/W	-
Blockierliste	R/W	R/W	R/W	-
Transponder	R/W	R/W	R/W	R
Externe Authentifizierung und LED (API)	R/W	R/W	R/W	R
Einzelauthentifizierung zurücksetzen	R/W	R/W	R	R
Diagnose	R	R	R	R
Firmware-Update	R/W	R/W	-	-
Gerätekonfiguration sichern/wiederherstellen	R/W	R/W***	-	-
Werksreset	R/W	-	-	-

R = Lesezugriff, R/W = Lese- und Schreibzugriff

* nur die folgenden Einstellungen: Ortsbeschreibung, Gerätegruppe, Gültigkeitsdatum auswerten, Zeitzone, Datum/Uhrzeit

** mit Ausnahme von Anwendern mit der Rolle "Administrator"

*** mit Ausnahme von Anwendern mit der Rolle "Administrator" und es können nur die erlaubten Einstellungen der Gerätekonfiguration wiederhergestellt werden (siehe Konfiguration sichern und wiederherstellen [📖 86])

Es können max. 20 Geräteanwender verwaltet werden. Jedem Geräteanwender muss ein eindeutiger Name zugeordnet werden, jeder Name darf nur einmal vorkommen. Jedem Geräteanwender kann eine der 4 Rollen zugewiesen werden.

Durch die Angabe einer Remote IP-Adresse kann der Zugriff auf das Gerät mit den entsprechenden Zugangsdaten auf eine bestimmte IP-Adresse der Gegenstelle (IP-Adresse des PCs oder der Steuerung) beschränkt werden.

8.6 Zertifikate verwalten

8.6.1 Umgang mit Zertifikaten

Der PITreader verwendet X.509 Zertifikate, um die Kommunikation zwischen dem Gerät und der Web-Anwendung abzusichern. Standardmäßig verwendet das System ein self-signed Server-Zertifikat. Dieses Zertifikat wird vom PITreader automatisch generiert.

Damit eine Kommunikation stattfinden kann, wird das Zertifikat von der Web-Anwendung auf den PC heruntergeladen und im Web-Browser überprüft. Wenn Sie ein self-signed-Zertifikat verwenden, dann erscheint bei dem Versuch, eine Verbindung zum PITreader aufzubauen eine Warnung, die besagt, dass die Verbindung nicht sicher ist. Um eine Verbindung aufbauen zu können, müssen Sie eine Sicherheits-Ausnahmeregel zum Web-Browser hinzufügen.

ACHTUNG!

Gefahr von Datenmanipulation

Möglicher Verlust der Datensicherheit.

Sie dürfen eine Sicherheits-Ausnahmeregel nur dann zum Web-Browser hinzufügen, wenn Sie sicher sind, dass Sie mit dem PITreader kommunizieren.

Alternativ können Sie in der Web-Anwendung unter ***Einstellungen -> Zertifikat*** das aktuelle Zertifikat für die HTTPS-Verbindung des PITreader herunterladen und in den Web-Browser importieren.

Neue Zertifikate werden generiert, wenn der PITreader auf Werkseinstellungen zurückgesetzt wird.
Sie können auch ein eigenes Server-Zertifikat mit privatem Schlüssel hochladen.

Zertifikate und private Schlüssel sind nicht Teil der Gerätekonfiguration und können durch die Funktion ***Konfiguration sichern***/***Konfiguration wiederherstellen*** nicht auf andere Geräte übertragen werden.

8.6.2 Zertifikat in eine Public-Key-Infrastruktur (PKI) einbinden

Zum Einbinden eines PITreader in eine bestehende Public-Key-Infrastruktur können Sie entweder ein eigenes Server-Zertifikat, zusammen mit dem privaten Schlüssel, auf das Gerät hochladen oder einen Certificate-Signing-Request (CSR) vom PITreader herunterladen, in Ihre bestehende PKI importieren und das signierte Zertifikat wieder auf das Gerät hochladen.

Zertifikate können im PEM- (Zertifikat oder Zertifikat + privater Schlüssel) oder DER-Format (nur Zertifikat) auf das Gerät geladen werden.

Das Gerät unterstützt Zertifikate, die auf einem der folgenden kryptographischen Verfahren basieren:

- ECC (prime256v1, secp256r1 oder NIST P-256), **empfohlen**
- RSA (2048 Bit)

8.7 Authentifizierungsmodus konfigurieren

Sie können in der Web-Anwendung unter ***Konfiguration -> Einstellungen*** den Authentifizierungsmodus für den PITreader konfigurieren. Wählen Sie entweder den Authentifizierungsmodus "Transponder-Daten", "Extern", "Berechtigungsliste" oder "Feste Berechtigung".
Sie können erlauben, dass unabhängig vom Authentifizierungsmodus sowohl die Berechtigung für die Gerätegruppe als auch die Anwenderdaten extern über die REST API überschrieben werden dürfen. Aktivieren Sie dafür unter ***Konfiguration -> Einstellungen -> Funktion*** das Feld ***Externes Überschreiben erlauben***.
Wenn das Feld ***Externes Überschreiben erlauben*** aktiviert ist, dann

- wird die Berechtigung, die im Authentifizierungsmodus "Transponder-Daten" vom Transponder oder im Authentifizierungsmodus "Berechtigungsliste" aus einer Datei gelesen wird, überschrieben.
- werden die Anwenderdaten, die vom Transponder gelesen werden, überschrieben.

Die externen Anwenderdaten sind solange gültig, bis der Transponder entfernt oder ein anderer Transponder im Lesebereich platziert wird. Es können nur externe Anwenderdaten überschrieben werden, für die eine ID in der Anwenderdaten-Konfiguration vorhanden ist.

8.8 Authentifizierungstyp konfigurieren

Sie können in der Web-Anwendung unter ***Konfiguration -> Einstellungen*** den Authentifizierungstyp für den PITreader konfigurieren. Wählen Sie einen der Authentifizierungstypen "Basis", "Einzelauthentifizierung" oder "4-Augen-Prinzip".

8.9 Ortsbeschreibung

Sie können in der Web-Anwendung unter ***Konfiguration -> Einstellungen -> Ortsbeschreibung*** eine Beschreibung zum Standort des PITreader eingeben. Es sind max. 47 Zeichen erlaubt.

8.10 Datenprotokollierung mit personenbezogenen Daten

Sie können in der Web-Anwendung unter ***Konfiguration -> Einstellungen*** einstellen, ob im Diagnoseprotokoll personenbezogene Daten (Security-ID, Anwender und IP-Adresse) protokolliert werden sollen. In der Default-Konfiguration ist diese Funktion deaktiviert.

8.11 Automatisches Löschen von Audit-Trail-Meldungen

Sie können in der Web-Anwendung festlegen, dass Audit-Trail-Meldungen automatisch nach einer konfigurierbaren Anzahl von Tagen gelöscht werden.

Wählen Sie dazu ***Konfiguration -> Einstellungen***. Stellen Sie im Bereich ***Erweiterte Funktionen*** im Feld ***Automatisches Löschen von Audit-Trail-Meldungen nach*** die gewünschten Tage ein.

In der Default-Konfiguration ist diese Funktion deaktiviert.

8.12 Gerätegruppe einstellen

Sie können in der Web-Anwendung unter ***Konfiguration -> Einstellungen*** dem PITreader eine Gerätegruppe zuweisen (siehe auch Gerätegruppen [📖 23]). Unter ***Konfiguration -> Gerätegruppen*** können Sie einen Namen für jede der Gerätegruppen von 0 … 31 eintragen. Es sind max. 47 Zeichen erlaubt. Wenn Sie einen Namen für eine Gerätegruppe eingetragen haben, wird Ihnen beim Zuweisen der Gerätegruppe unter ***Konfiguration -> Einstellungen*** der entsprechende Name in der Auswahlliste angezeigt. Wenn kein Name eingetragen wurde, wird die Nummer der Gerätegruppe angezeigt.

8.13 Basis-Codierung setzen

Sie können den PITreader codieren, indem Sie in der Web-Anwendung unter ***Konfiguration -> Codierung*** im Bereich ***Basis-Codierung*** eine ***Kennung*** eintragen und auf den Button ***Codierung setzen*** klicken. Weiterhin steht ein Kommentar-Feld zur Verfügung, in das Sie einen Kommentar zu Ihrer Basis-Codierung eintragen können. Beide Felder sind auf max. 63 Zeichen begrenzt.

Nachdem Sie den PITreader codiert haben, wird unter ***Status*** die Information ***Basis-Codierung gesetzt*** angezeigt und unter ***Prüfsumme*** die zugehörige Prüfsumme. Sie haben die Möglichkeit, die Basis-Codierung zu löschen oder die Basis-Codierung zu ändern.

Der Kommentar zur Basis-Kennung kann nachträglich angepasst und über den Button ***Kommentar speichern*** im Gerät gespeichert werden.

INFO

Die Basis-Kennung kann nach dem Setzen nicht mehr ausgelesen oder angezeigt werden. Das Kommentarfeld kann daher dazu genutzt werden, einen Hinweis auf die gesetzte Basis-Kennung zu hinterlegen.

Siehe auch Codierung [📖 39].

8.14 OEM-Codierung setzen

Sie können den PITreader mit einer OEM-Kennung codieren, indem Sie in der Web-Anwendung unter ***Konfiguration -> Codierung*** im Bereich ***OEM-Codierung*** eine ***Kennung*** eintragen und auf den Button ***Codierung setzen*** klicken. Weiterhin steht ein Kommentar-Feld zur Verfügung, in das Sie einen Kommentar zu Ihrer OEM-Kennung eintragen können. Beide Felder sind auf max. 63 Zeichen begrenzt.

Nachdem Sie den PITreader codiert haben, wird unter ***Status*** die Information ***OEM-Codierung gesetzt*** angezeigt und unter ***Prüfsumme*** die zugehörige Prüfsumme. Sie haben die Möglichkeit, die OEM-Codierung zu löschen oder die OEM-Codierung zu ändern, dafür muss die aktuell gesetzte OEM-Kennung eingegeben werden.

Der Kommentar zur OEM-Kennung kann nachträglich angepasst und über den Button ***Kommentar speichern*** im Gerät gespeichert werden.

INFO

Die OEM-Kennung kann nach dem Setzen nicht mehr ausgelesen oder angezeigt werden. Das Kommentarfeld kann daher dazu genutzt werden, einen Hinweis auf die gesetzte OEM-Kennung zu hinterlegen.

Wenn Sie die OEM-Codierung z. B. für Ihre Service-Mitarbeiter nutzen möchten, muss bei allen PITreader-Geräten, die Sie an Ihre Kunden ausliefern, die entsprechende Kennung als OEM-Codierung gesetzt sein.

Siehe auch Codierung [📖 39].

8.15 Fremdtransponder mit ISO/IEC Standard als RFID-Protokoll konfigurieren

Die Lesegeräte PITreader S card unit und PIT gb mit PITreader Card unterstützen auch Transponder von Fremdherstellern.

Zum Konfigurieren aktivieren Sie in der Web-Anwendung unter ***Konfiguration -> Einstellungen ->*** unter der Überschrift ***Erweiterte Funktionen*** die Option ***Fremdtransponder unterstützen***. Es erscheint das Dropdown-Menü ***RFID-Protokoll***.

Im Dropdown-Menü ***RFID-Protokoll*** können Sie dann zwischen folgenden Standards wählen:

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

Es werden nur Transponder entsprechend dem ausgewählten Standard erkannt. Werden Transponder mit anderen RFID Protokoll verwendet, reagiert das Lesegeräte PITreader nicht und die LED des Lesegeräts leuchtet weiterhin blau.

WICHTIG

Wenn die Option ***Fremdtransponder unterstützen*** aktiviert und im Dropdown-Menü ***RFID-Protokoll*** der Standard ***ISO/IEC 14443-A*** gewählt ist, werden die PILZ-Transponder wie Fremdtransponder behandelt. Von den Pilz-Transpondern wird dann nur noch die UID gelesen und es gelten dieselben Einschränkungen wie für Fremdtransponder, siehe Transponder von Fremdherstellern mit gewähltem ISO/IEC Standards (ohne MIFARE DESFire-Anwendungen) [📖 32]

8.16 Fremdtransponder mit MIFARE DESFire-Anwendung konfigurieren

Die Lesegeräte PITreader S card unit und PIT gb mit PITreader Card unterstützen auch Transponder von Fremdherstellern.

Die kryptografischen Schlüssel (AES-Schlüssel) ermöglichen es dem PITreader sich am Transponder zu authentifizieren. Dadurch kann der PITreader Daten auf den Transponder schreiben und lesen. Über die so genannte Diversifikation kann für jeden Transponder ein individueller AES-Schlüssel generiert werden.

Folgende kryptographische Schlüssel stehen zur Verfügung	Erklärung
Application Master Key Verwendung: immer erforderlich Diversifikation: empfohlen, ist frei wählbar	Der Application Master Key dient dazu, die PITreader-Applikation auf dem Transponder gegen Manipulation und Überschreiben zu schützen. Dazu muss der Application Master Key auf dem PITreader eingerichtet werden. Mit diesem Schlüssel kann dann die gewünschte PITreader-Anwendung auf den Transponder mit MIFARE DESFire-Anwendungen übertragen werden.
PICC Master Key Verwendung: optional Diversifikation: muss passend zur Konfiguration des Transponders mit MIFARE DESFire-Anwendung eingestellt werden	Der PICC Master Key wird benötigt, um die PITreader-Anwendung auf einem Transponder mit MIFARE DESFire-Anwendungen zu programmieren, wenn Bit 2 der PICCKey-Settings den Wert 0 hat. Die vom Hersteller oder Lieferanten des Transponders mit MIFARE DESFire-Anwendungen vorgegeben AES-Schlüssel und Diversifikations-Einstellungen müssen im PITreader hinterlegt werden. Dazu muss der PICC Master Key in dem PITreader hinterlegt werden, mit dem auch die PITreader-Applikation auf den Transponder mit MIFARE DESFire-Anwendungen aufgebracht werden soll.
Application User Key Verwendung: optional Diversifikation: empfohlen, ist frei wählbar	Im regulären Betrieb verwenden die PITreader die PITreader-Anwendung über den Application User Key. Wenn kein eigener Application User Key im entsprechenden PITreader hinterlegt ist, wird ein AES-Schlüssel auf Basis der eingestellten Basis-Codierung verwendet. Dadurch entfällt die Notwendigkeit, eigene AES-Schlüssel für PITreader zu konfigurieren, die auf Transponder mit MIFARE DESFire zugreifen sollen. Wenn jedoch ein eigener Application User Key auf dem Initialisierungs-PITreader konfiguriert wurde, muss dieser in allen weiteren PITreadern hinterlegt werden, an denen der entsprechende Transponder mit MIFARE DESFire funktionieren soll.

Folgende kryptographische Schlüssel stehen zur Verfügung	Erklärung
Application Default Key Verwendung: optional Diversifikation: nicht unterstützt	Der Application Default Key wird vom Hersteller oder Lieferanten des Transponders mit MIFARE DESFire-Anwendungen vorgegeben. Wenn der Standardwert des Application Default Key auf dem Transponder mit MIFARE DESFire nicht 0x00..00 ist, muss der entsprechende Wert im Initialisierungs-PITreader eingetragen werden. Dies ist wichtig, damit der Transponder vom PITreader authentifiziert werden kann.
Transport Key Verwendung: optional Diversifikation: muss passend zur Konfiguration des Transponders mit MIFARE DESFire-Anwendung eingestellt werden	Damit externe Dritte die PITreader-Datenstruktur auf den MIFARE DESFire-Transponderspeicher aufbringen können, können vorübergehend sogenannte "Transport Keys" verwendet werden. Diese temporären AES-Schlüssel können später im PITreader durch eigene AES-Schlüssel ersetzt werden. Dadurch wird die Sicherheit und Kontrolle über die Datenstruktur auf dem Transponder gewährleistet.

Diversifikation

Die Diversifikation erfolgt gemäß dem Verfahren für 128-Bit AES-Schlüssel, wie in der NXP Application Note AN10922 (Symmetric key diversifications) beschrieben. Dieses Verfahren wird verwendet, um die Sicherheit und Authentifizierung zwischen dem Transponder und dem PITreader zu gewährleisten.

Die Eingabe der Diversifikation kann in der PITreader Web-Anwendung unter ***Konfiguration -> Krypto. Schlüssel*** für jeden AES-Schlüssel angegeben werden. Diese muss als hexadezimal kodierte Bytes erfolgen, z. B. A1B9.... Dabei kann der Platzhalter "$UID" genutzt werden, um AES-Schlüssel für jeden Transponder individuell zu diversifizieren.

Bei der Diversifikation wird der Platzhalter "$UID" durch die Transponder-UID gemäß ISO 14443-A ersetzt. Ein Beispiel für eine Diversifikation mit Platzhalter für "$UID" wäre A1B9F0$UID03.

8.16.1 RFID-Protokoll wählen

Zum Konfigurieren aktivieren Sie in der Web-Anwendung unter ***Konfiguration -> Einstellungen ->*** unter der Überschrift ***Erweiterte Funktionen*** die Option ***Fremdtransponder unterstützen***. Es erscheint das Dropdown-Menü ***RFID-Protokoll***.

Im Dropdown-Menü ***RFID-Protokoll*** können Sie dann den Standard ***MIFARE DESFire mit PITreader-Datenstruktur*** wählen. Bei diesem Standard müssen die kryptographischen Schlüssel und die Codierung hinterlegt werden.
Pilz-Transponder können nicht verwendet werden.

Es werden nur Transponder entsprechend dem ausgewählten Standard erkannt. Werden Transponder mit anderen RFID Protokoll verwendet, reagiert das Lesegeräte PITreader nicht und die LED des Lesegeräts leuchtet weiterhin blau.

8.16.2 Kryptographische Schlüssel hinterlegen

Zum Hinterlegen der kryptographischen Schlüssel wählen Sie in der Web-Anwendung unter ***Konfiguration -> Krypto. Schlüssel***. Es erscheint das Auswahlmenü ***Kryptographische Schlüssel.***

Speicherplatz 1 und Speicherplatz 2

Wählen Sie unter der Überschrift ***Speicherplatz 2*** die Option ***Bearbeiten***. Es erscheint das Menü ***Kryptographische Schlüssel setzen***. Im Dropdown-Menü ***Typ,*** bei ***Speicherplatz 1*** und ***Speicherplatz 2*** können Sie dann zwischen folgenden kryptographischen Schlüssel wählen:

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

Wenn der kryptographische Schlüssel gewählt ist:

- Geben Sie im Feld ***AES-Schlüssel*** den entsprechenden 128-Bit AES-Schlüssel ein: hexadezimale Eingabe von genau 32 Zeichen, z. B.: C963EC29964DE3399B-DE34E478014963
- Geben Sie im Feld ***Diversifikation*** den entsprechenden Schlüssel ein: hexadezimale Eingabe von maximal 62 Zeichen mit AES-Schlüssel Platzhalter "$UID", z. B.: A1B9F0$UID03

Application Default Key

Wählen Sie unter der Überschrift ***Application Default Key*** die Option ***Bearbeiten***. Es erscheint das Menü ***Application Default Key setzen***.

- Geben Sie im Feld ***AES-Schlüssel*** den entsprechenden 128-Bit AES-Schlüssel ein: hexadezimale Eingabe von genau 32 Zeichen, z. B.: C963EC29964DE3399B-DE34E478014963

8.17 Fremdtransponder mit MIFARE DESFire-Anwendung initialisieren

Es gibt 4 Möglichkeiten um Fremdtransponder mit MIFARE DESFire-Anwendung zu initialisieren:

- Fremdtransponder selbst initialisieren [📖 77]
  - Zum Erstellen neuer Anwendungen erfordert der Fremdtransponder keine vorherige Authentifizierung mit dem PICC Master Key [📖 78]
  - Zum Erstellen neuer Anwendungen erfordert der Fremdtransponder die vorherige Authentifizierung mit dem PICC Master Key [📖 78]
- Fremdtransponder durch Dritte initialisieren [📖 79]
  - Nutzung eigener Application Master Keys und Application User Keys [📖 79]

– Nutzung von Transport Keys [📖 79]

8.17.1 Fremdtransponder selbst initialisieren

- Wählen Sie im RFID-Protokoll den Standard ***MIFARE DESFire mit PITreader-Datenstruktur***, siehe RFID-Protokoll wählen [📖 75].
- Setzen Sie die Basis-Codierung und hinterlegen Sie die nötigen kryptographischen Schlüssel:
  – Zum Erstellen neuer Anwendungen erfordert der Fremdtransponder keine vorherige Authentifizierung mit dem PICC Master Key [📖 78]
  – Zum Erstellen neuer Anwendungen erfordert der Fremdtransponder die vorherige Authentifizierung mit dem PICC Master Key [📖 78]
- Wählen Sie in der Web-Anwendung unter ***Transponder -> Initialisierung***.
- Geben Sie für den Transponder im Feld Seriennummer eine eindeutige Seriennummer ein.
- Geben Sie für den Transponder optional im Feld Artikelnummer eine Artikelnummer ein.
- Platzieren Sie den Transponder der initialisiert werden soll am PITreader-Lesekopf, siehe Transponder platzieren [📖 91].
- Klicken Sie unten auf das Feld Initialisieren.
  Der Transponder wird initialisiert und kann nun programmiert werden, siehe Transponder beschreiben/programmieren [📖 80].

WARNUNG!

Key-in-Pocket-System: Möglicher Verlust der Sicherheitsfunktion, wenn Fremdtranspondern keine eindeutige Seriennummern zugewiesen wurde.

Wenn Fremdtranspondern keine eindeutige Seriennummer zugewiesen wurde, kann unter Umständen das Key-in Pocket-System die interne Anmeldeliste nicht korrekt auswerten. Dadurch könnte das Key-in Pocket-System den Aufenthalt von Personen im Gefahrenbereich nicht erkennen.

Es besteht erhöhte Verletzungsgefahr oder sogar Lebensgefahr!

– Vergeben Sie bei der Initialisierung von Fremdtransponder immer eindeutige Seriennummern.

Auch wenn Transponder mit MIFARE DESFire-Anwendung eine PITreader-Anwendung enthalten, können diese erneut initialisiert werden. Dazu muss der im PITreader hinterlegte Application Master Key mit dem Application Master Key der vorherigen Initialisierung übereinstimmen. Bei der Initialisierung werden alle Daten in der vorhandenen PITreader-Anwendung zurückgesetzt und die Seriennummer sowie die Artikelnummer überschrieben.

8.17.1.1 Zum Erstellen neuer Anwendungen erfordert der Fremdtransponder keine vorherige Authentifizierung mit dem PICC Master Key

PITreader Konfiguratio		
	Initialisierungs-PITreader	**alle weiteren PITreader**
Basis-Codierung	muss gesetzt sein	muss gesetzt sein
Kryptographische Schlüssel	Key 1: Application Master Key (eigenen Schlüssel wählen, Diversifikation frei wählbar)	Key 1: (leer)
	Key 2: (leer)	
	Bei Bedarf für den Transponder passenden Application Default Key eingeben.	

- Setzen Sie die Kennung für die Basis-Codierung unter ***Konfiguration -> Codierung***, siehe Basis-Codierung setzen [📖 72].
- Hinterlegen Sie die oben in der Tabelle aufgeführten kryptographischen Schlüssel, siehe Kryptographische Schlüssel hinterlegen [📖 76].

8.17.1.2 Zum Erstellen neuer Anwendungen erfordert der Fremdtransponder die vorherige Authentifizierung mit dem PICC Master Key

Konfiguration des PITreaders		
	Initialisierungs-PITreader	**alle weiteren PITreader**
Basis-Codierung	muss gesetzt sein	muss gesetzt sein
Kryptographische Schlüssel	Key 1: Application Master Key (eigenen Schlüssel wählen, Diversifikation frei wählbar)	Key 1: (leer)
	Key 2: PICC Master Key (passend zu den Transpondern, Diversifikation muss ebenfalls passend gesetzt werden)	
	Bei Bedarf für den Transponder passenden Application Default Key eingeben.	

- Setzen Sie die Kennung für die Basis-Codierung unter ***Konfiguration -> Codierung***, siehe Basis-Codierung setzen [📖 72].
- Hinterlegen Sie die oben in der Tabelle aufgeführten kryptographischen Schlüssel, siehe Kryptographische Schlüssel hinterlegen [📖 76].

8.17.2 Fremdtransponder durch Dritte initialisieren

Um die Initialisierung durch Dritte zu ermöglichen, können Sie bei PILZ anfragen, um eine Definition der PITreader-Datenstruktur zu erhalten. Sie haben dann den Vorteil, dass Sie die Transponder-Seriennummern nicht selbst vergeben müssen.
Dadurch könnten Ihre Transponder im Voraus mit einheitlichen Seriennummern eingerichtet werden.

8.17.2.1 Nutzung eigener Application Master Keys und Application User Keys

Wenn Sie einen eigenen Application Master Key und Application User Key nutzen, dann benötigen Sie keinen eigenen Initialisierungs-PITreader zum Einrichten der Transponder mit MIFARE DESFire-Anwendung.
Allerdings müssen dann alle PITreader, an denen die Transponder verwendet werden, mit dem passenden „Application User Key“ eingerichtet werden.

Konfiguration des PITreaders	
	alle PITreader
Basis-Codierung	muss **nicht** gesetzt sein
kryptographische Schlüssel	Key 1: Application User Key (Einstellung entsprechend der mit Dritten vereinbarten Daten)
	Key 2: (leer)

- Hinterlegen Sie die oben in der Tabelle aufgeführten kryptographischen Schlüssel, siehe Kryptographische Schlüssel hinterlegen [📖 76].

8.17.2.2 Nutzung von Transport Keys

Damit nicht an allen PITreader der eigene Application User Key eingerichtet werden muss, können temporäre Transport-Keys verwendet werden. Dazu benötigen Sie einen eigenen Initialisierungs-PITreader, an dem ein Application Master Key und der Transport Key eingerichtet sind.

Die Transport-Keys werden durch eigene Schlüssel ersetzt, sobald der Transponder von einem mit Application Master Key und entsprechendem Transport Key konfigurierten Initialisierungs-PITreader erkannt wird. Die Transport-Keys werden durch die eigenen Application User Keys ersetzt.

Konfiguration des PITreaders		
	Initialisierungs-PITreader	**alle weiteren PITreader**
Basis-Codierung	muss gesetzt sein	muss gesetzt sein
kryptographische Schlüssel	Key 1: Application Master Key (eigenen Schlüssel wählen, Diversifikation frei wählbar)	Key 1: (leer)
	Key 2: Transport Key (Einstellung entsprechend der mit Dritten vereinbarten Daten)	

- Setzen Sie die Kennung für die Basis-Codierung unter Konfiguration -> Codierung, siehe Basis-Codierung setzen [📖 72].

- Hinterlegen Sie die oben in der Tabelle aufgeführten kryptographischen Schlüssel, siehe Kryptographische Schlüssel hinterlegen [📖 76].
- Platzieren Sie alle Transponder mit MIFARE DESFire-Anwendung am Initialisierungs-PITreader. Der Transport Key wird durch den Application User Key ersetzt.

8.18 Transponder beschreiben/programmieren

8.18.1 Berechtigungen programmieren

Sie können in der Web-Anwendung die Berechtigungen der Transponder auslesen (unter ***Transponder -> Daten***) und die Transponder mit Berechtigungen beschreiben (unter ***Transponder -> Berechtigungen -> Programmieren)***.
Sie haben die Möglichkeit, die selbe Berechtigung für alle Gerätegruppen zu übernehmen (Default-Einstellung) oder für jede der 32 Gerätegruppen eine andere Berechtigung zu vergeben (entfernen Sie dafür den Haken bei ***für alle übernehmen***).
Außerdem haben Sie die Möglichkeit, die Berechtigungen auf dem Transponder zu sperren, dadurch kann ein nachträgliches Ändern der Berechtigungen verhindert werden.

WICHTIG

Beachten Sie:

– An einem gesperrten Transponder können keine Änderungen an den Gruppenberechtigungen vorgenommen werden.

– Die Sperre kann nicht rückgängig gemacht werden.

Wenn Sie eine Basis-Kennung gesetzt haben, wird der Transponder beim schreiben/programmieren der Berechtigungen automatisch auch auf die Basis-Codierung des PITreader eingelernt.

8.18.2 Gültigkeit des Transponders konfigurieren

INFO

Das Gültigkeitsdatum von Transpondern kann ausschließlich im Authentifizierungsmodus "Transponderdaten" ausgewertet werden.

Sie können die Gültigkeit von Transpondern auf einen bestimmten Zeitraum einschränken. Aktivieren Sie dafür unter ***Konfiguration -> Einstellungen -> Erweiterte Funktionen*** das Feld ***Gültigkeitsdatum auswerten*** und stellen Sie die gültige Zeitzone ein. Die ausgewählte Zeitzone wird nur für die Auswertung des Gültigkeitsdatums verwendet.
Unter ***Transponder -> Berechtigungen*** können Sie ein Startdatum und ein Enddatum (im Format Tag, Monat, Jahr "TT.MM.JJJJ") für die Gültigkeit des Transponders eintragen.

8.18.3 Transponder auf Basis-Codierung einlernen

Wenn Sie einen nicht gesperrten Transponder verwenden und eine Basis-Kennung gesetzt haben, können Sie unter ***Transponder -> Berechtigungen -> Programmieren*** den Transponder auf die Basis-Codierung einlernen.

Wenn Sie einen gesperrten Transponder oder einen von Pilz werkseitig vorprogrammierten Transponder verwenden und eine Basis-Kennung gesetzt haben, können Sie unter ***Transponder -> Daten -> Transponder einlernen*** den Transponder auf die Basis-Codierung einlernen.

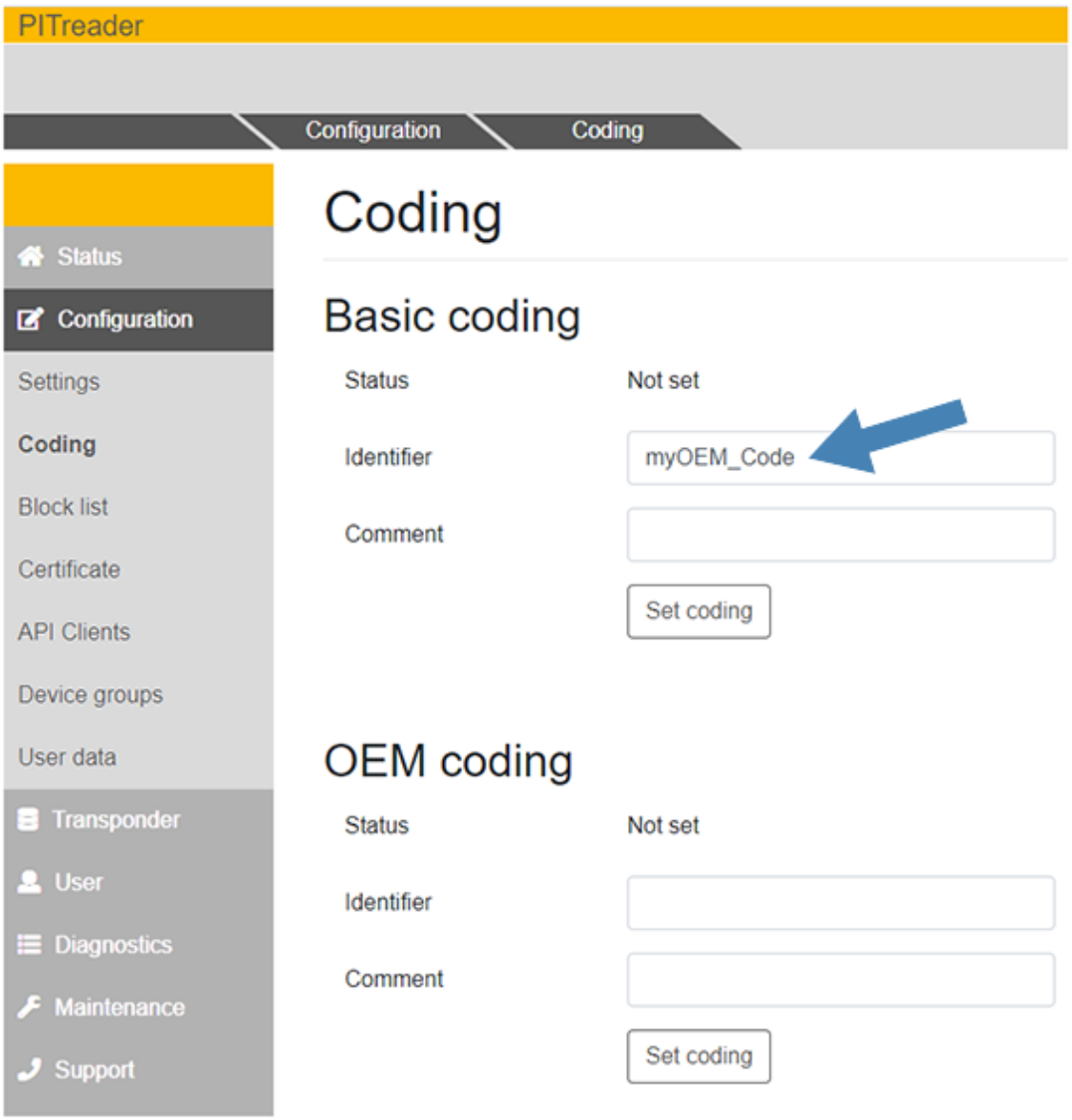
Sie können die Codierung des Transponders ändern, in dem Sie den Transponder auf eine andere Basis-Codierung einlernen. Sie können die Codierung des Transponders entfernen, in dem Sie an einem PITreader ohne gesetzte Basis-Codierung die Berechtigungen erneut auf den Transponder schreiben.

8.18.4 Transponder auf OEM-Codierung einlernen

Transponder können nur auf die in einem PITreader hinterlegte Basis-Codierung eingelernt werden. Um einen Transponder auf eine OEM-Codierung einzulernen, muss zunächst die OEM-Kennung als Basis-Codierung im PITreader eingestellt werden.

Tragen Sie in der Web-Anwendung unter ***Konfiguration -> Codierung*** im Bereich ***Basis-Codierung*** anstatt einer Basis-Kennung die OEM-Kennung ein und klicken Sie auf den Button ***Codierung setzen.***

Beispiel:



Wenn Sie einen nicht gesperrten Transponder verwenden, können Sie unter ***Transponder -> Berechtigungen -> Programmieren*** den Transponder auf die OEM-Kennung einlernen.

Wenn Sie einen gesperrten Transponder oder einen von Pilz werkseitig vorprogrammierten Transponder verwenden, können Sie unter ***Transponder -> Daten -> Transponder einlernen*** den Transponder auf die OEM-Kennung einlernen.

Sie können die Codierung ändern, in dem Sie den Transponder auf eine andere Codierung einlernen. Sie können die Codierung entfernen, in dem Sie an einem PITreader ohne gesetzte Codierung die Berechtigungen erneut auf den Transponder schreiben.

Hinweis: Wenn Sie als Maschinenhersteller Transponder für Service-Mitarbeiter codieren möchten, verwenden Sie dafür idealerweise einen PITreader, der nur diesem Zweck dient. Auf diese Weise ist sichergestellt, dass neue Transponder mit dieser OEM-Kennung nur von einer Person erstellt werden können, die die OEM-Kennung kennt oder über einen speziell für diesen Zweck konfigurierten PITreader verfügt.

8.18.5 Transponder auf identisch codierte PITreader beschränken

Sie können verhindern, dass die Daten eines codierten Transponders von einem nicht codierten PITreader ausgelesen werden können. Durch Konfiguration können Sie codierte Transponder auf identisch codierte PITreader beschränken. Sie können die Option sowohl für Transponder mit Basis- als auch OEM-Codierung konfigurieren.

Wenn Sie codierte Transponder auf identisch codierte PITreader beschränken möchten, dann wählen Sie unter ***Transponder -> Daten*** die Option ***Auf identisch codierte PITreader beschränken*** an und klicken Sie anschließend auf ***Programmieren***.

8.18.6 Werte der Anwenderdaten bearbeiten

Mit der Web-Anwendung kann angezeigt werden, welche Werte die Parameter auf dem Transponder haben. Die Werte können geändert werden.
Bestimmte Daten des PITreader können auch mit dem Tool PIT Transponder Manager konfiguriert und Transponder programmiert werden.

Alle Aktionen werden unter ***Transponder -> Anwenderdaten*** ausgeführt.

Hinweise:

- In der Web-Anwendung werden immer die Parameter angezeigt, die auf dem PITreader angelegt sind (siehe Anwenderdaten konfigurieren [📖 85]). Sollten auf dem Transponder mehr Parameter vorhanden sein, so werden diese ignoriert. Sollten auf dem Transponder weniger Parameter vorhanden sein, so wird für die fehlenden Parameter der Initialwert des Datentyps angezeigt.
  Beim Speichern der Anwenderdaten auf dem Transponder, werden alle vorhandenen Anwenderdaten überschrieben.
- In der Web-Anwendung wird unter ***Transponder -> Anwenderdaten*** auch angezeigt, wieviel von dem Speicherplatz für die Anwenderdaten auf dem Transponder bereits belegt ist.
- Berechtigungen für Gerätegruppen
  Falls Sie die Anzahl der Gerätegruppen auf mehr als 32 erweitert haben, können Sie in den Anwenderdaten zwar Berechtigungen für die Gruppen 0 bis 31 eingeben, aber diese werden ignoriert. Für die Gerätegruppen 0 bis 31 gelten immer die Berechtigungen, die unter ***Transponder -> Berechtigungen*** eingegeben wurden.

8.18.7 Anwenderdaten auf Transpondern löschen

- Wählen Sie in der Web-Anwendung ***Transponder -> Anwenderdaten***.
- Wählen Sie die Option ***Anwenderdaten auf Transponder löschen***.

8.19 Berechtigungsliste

Sie können in der Web-Anwendung unter ***Berechtigungsliste*** Berechtigungen eintragen. Sie können die Berechtigungsliste in eine CSV-Datei exportieren oder eine Berechtigungsliste importieren. Beachten Sie für den Import folgendes:

- Die CSV-Datei muss zwei Spalten enthalten, in der ersten Spalte muss die Security-ID stehen, in der zweiten Spalte die Berechtigung zur Security-ID.
- Die erste Zeile der CSV-Datei kann Spaltenüberschriften enthalten und wird beim Import übersprungen.
- In der Berechtigungsliste darf jede Security-ID nur einmal vorkommen. Überprüfen Sie deshalb vor dem Import, dass keine doppelten Einträge in der CSV-Datei enthalten sind.
- Die Berechtigungen können in Hex- oder Dezimalschreibweise importiert werden (siehe auch Übersicht der Berechtigungen [📖 109]).
- Als Trennzeichen wird ein Semikolon verwendet.
- Felder und Werte dürfen in Anführungszeichen (") eingefasst sein.
- Der Import wird nur durchgeführt, wenn alle Einträge erfolgreich validiert werden können.
- Beim Import werden alle Einträge der Berechtigungsliste in der Web-Anwendung durch die importierten Einträge ersetzt.
- Die Berechtigungsliste kann bis zu 1000 Einträge enthalten.

Siehe auch Authentifizierungsmodus "Berechtigungsliste" [📖 26].

8.20 Blockierliste verwenden

Sie können die Authentifizierung bestimmter Transponder sperren, in dem Sie die Security-IDs dieser Transponder (und optional einen Kommentar) unter ***Blockierliste*** eintragen. Sie können die Blockierliste in eine CSV-Datei exportieren oder eine Blockierliste importieren. Beachten Sie für den Import folgendes:

- Die CSV-Datei muss zwei Spalten enthalten, in der ersten Spalte muss die Security-ID stehen, in der zweiten Spalte der Kommentar.
- Die erste Zeile der CSV-Datei kann Spaltenüberschriften enthalten und wird beim Import übersprungen.
- In der Blockierliste darf jede Security-ID nur einmal vorkommen. Überprüfen Sie deshalb vor dem Import, dass keine doppelten Einträge in der CSV-Datei enthalten sind.
- Felder und Werte dürfen in Anführungszeichen (") eingefasst sein. Wenn in einem Feld oder Wert ein Anführungszeichen enthalten ist, muss das komplette Feld in Anführungszeichen eingefasst und die Anführungszeichen im Feld verdoppelt sein.
- Als Trennzeichen wird ein Semikolon verwendet.
- Beim Import werden alle Einträge der Blockierliste in der Web-Anwendung durch die importierten Einträge ersetzt.
- Die Blockierliste kann bis zu 1000 Einträge enthalten.

Siehe auch Blockierliste [📖 42].

8.21 Anwenderdaten konfigurieren

Damit die Anwenderdaten genutzt werden können, müssen die Parameter auf dem PITreader angelegt werden. Dies geschieht mithilfe der REST API (siehe Bedienungsanleitung PITreader REST API). Alternativ kann in der Web-Anwendung eine Konfigurationsdatei mit den Parametern importiert werden.

Bestimmte Daten des PITreader können auch mit dem Tool PIT Transponder Manager konfiguriert und Transponder programmiert werden.

Die Konfigurationsdatei wird in der Web-Anwendung unter ***Konfiguration -> Anwenderdaten*** importiert. Die Konfigurationsdatei ist eine JSON-Datei, die mit jedem Text-Editor erstellt und bearbeitet werden kann.

Soll zum Beispiel ein Parameter mit der Parameter-ID 10000, dem Namen "myParameter", dem Datentyp STRING (Typ-ID = 1) und einer maximalen Anzahl von 30 Zeichen angelegt werden, steht in der Konfigurationsdatei folgendes:

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

"size" muss ausschließlich beim Datentyp STRING angegeben werden. Die anzugebene Zeichenanzahl ist um 1 größer als die gewünschte Zeichenanzahl.

In der Web-Anwendung werden unter ***Konfiguration -> Anwenderdaten*** die aktuell auf dem PITreader vorhandenen Parameter angezeigt. Die Anwenderdaten können versioniert werden. Die Version kann mit einem Kommentar versehen werden. Der Kommentar darf alle gültigen UTF-8-Zeichen enthalten.

Die aktuell auf dem PITreader angelegten Parameter können in eine Konfigurationsdatei exportiert werden.

INFO

Falls Sie ausschließlich die Anzahl der Gerätegruppen auf mehr als 32 erweitern möchten, können Sie als Konfigurationsdatei die JSON-Datei verwenden, die mit dem Firmware-Update ausgeliefert wird. Sie können die Datei einfach importieren.

8.22 Konfiguration für PIT Windows Logon

Um PIT Windows Logon nutzen zu können, muss auf dem Transponder ein PIT Windows Logon Key geschrieben/programmiert werden. Der PIT Windows Logon Key kann aus der Software PIT Windows Logon oder vom PITreader benutzt werden.

PIT Windows Logon Key über den PITreader auf den Transponder schreiben/ programmieren:

Wählen Sie in der Web-Anwendung ***Konfiguration -> Krypto. Schlüssel*** den Bereich ***PIT Windows Logon Key***.
Hinterlegen Sie hier einen PIT Windows Logon Key und sichern Sie diesen mit einem Kennwort.

Anschließend kann der PIT Windows Logon Key auf den Transponder geschrieben/programmiert werden:
Wählen Sie in der Web-Anwendung ***Transponder -> Krypto. Schlüssel*** den Bereich ***Transponder programmieren.***
Geben Sie im Feld Kennwort das zuvor vergebene Kennwort für den PIT Windows Logon Key ein und klicken Sie auf ***Programmieren***.

Um zu prüfen, ob bzw. welcher PIT Windows Logon Key auf dem Transponder gespeichert ist: Wählen Sie in der Web-Anwendung ***Transponder -> Krypto. Schlüssel*** und klicken Sie im Bereich ***Kryptographische Schlüssel auf Transponder*** auf ***Aktualisieren***.

PIT Windows Logon Key über Software PIT Windows Logon auf den Transponder schreiben/programmieren:

Informationen finden Sie in der Bedienungsanleitung PIT Windows Logon (1007324).

8.23 Überwachung der Synchronisierung konfigurieren

Die Synchronisierung mit externen Daten kann überwacht werden (siehe Synchronisierung mit externen Daten [📖 42]).

Aktivieren Sie dazu in der Web-Anwendung unter ***Konfiguration -> Einstellungen -> Erweiterte Funktionen*** die Option ***Überwachung der Sychronisierung*** und geben Sie den maximalen Abstand zwischen zwei Synchronisierungen (5 Minuten bis 3 Tage) in das Feld ***Timeout der Synchronisierung*** ein.

8.24 API-Clients

Für den automatisierten Zugriff auf Daten des Geräts über die HTTPS-Schnittstelle können Sie unter ***Anwender -> Geräteanwender*** entsprechende Verbindungseinstellungen anlegen. Eine detaillierte Beschreibung dazu finden Sie im separaten Dokument „Bedienungsanleitung PITreader REST API“.

8.25 Konfiguration sichern und wiederherstellen

Alle Einstellungen, die in der Web-Anwendung vorgenommen werden, können in einer Datei gespeichert werden. Klicken Sie hierzu in der Web-Anwendung unter ***Wartung -> Sichern*** auf ***Konfiguration sichern***.

Wenn Sie eine Konfiguration auf dem Rechner gesichert haben, dann können Sie die Konfiguration wiederherstellen, indem Sie in der Web-Anwendung die Sicherungsdatei hochladen. Klicken Sie hierzu unter ***Wartung -> Wiederherstellen*** auf ***Konfiguration wiederherstellen***.

Die Sicherung enthält die Einstellungen, die Geräteanwender, die Blockierliste, die Berechtigungsliste, die Namen der Gerätegruppen, die Anwenderdaten-Konfiguration und die OPC UA Client-Zertifikate. TLS-Zertifikate, OPC UA Server-Zertifikate und Codierungskennungen sind nicht in der Sicherung enthalten und können nicht wiederhergestellt werden.

Das Sichern und Wiederherstellen der Konfiguration ist abhängig von der Rolle des Anwenders.

Anwender mit der Rolle "Administrator":

- Sichern der Konfiguration durch einen Anwender mit der Rolle "Administrator":
  - Der Administrator darf alle verfügbaren Daten sichern.
  - Die gesicherte Liste der Geräteanwender enthält alle Geräteanwender.
- Wiederherstellen der Konfiguration durch einen Anwender mit der Rolle "Administrator":
  - Der Administrator darf alle Daten wiederherstellen, die in der Sicherungsdatei vorhanden sind.
  - Ist in der Sicherungsdatei eine Liste der Geräteanwender enthalten und ist in der Liste mindestens ein Anwender mit dem Namen "Admin", der Rolle "Administrator" und der Authentifizierung "Name/Kennwort" vorhanden, dann werden sämtliche Anwender importiert. Sie ersetzen die vorhandenen Anwender auf dem Gerät.
  - Ist in der Sicherungsdatei eine Liste der Geräteanwender enthalten und sind in der Liste keine Anwender mit der Rolle "Administrator" vorhanden, dann bleiben die auf dem Gerät vorhandenen Anwender mit der Rolle "Administrator" erhalten. Die Anwender mit den Rollen "Geräteverwalter", "Transponder-Verwalter" und "Gast" werden durch die Anwender in der Sicherungsdatei ersetzt.

Anwender mit der Rolle "Geräteverwalter":

- Sichern der Konfiguration durch einen Anwender mit der Rolle "Geräteverwalter":
  - Der Geräteverwalter darf nur die Daten sichern, auf die er Lese- und Schreibzugriff hat. Siehe Geräteanwender [68].
  - Die gesicherte Liste der Geräteanwender enthält alle Geräteanwender, aber nicht die Anwender mit der Rolle "Administrator".
- Wiederherstellen der Konfiguration durch einen Anwender mit der Rolle "Geräteverwalter":
  - Der Geräteverwalter darf nur die Daten wiederherstellen, auf die er Lese- und Schreibzugriff hat. Siehe Geräteanwender [68].
  - Ist in der Sicherungsdatei eine Liste der Geräteanwender enthalten und sind in der Liste Anwender mit der Rolle "Administrator" vorhanden, dann werden diese ignoriert. Die auf dem Gerät vorhandenen Anwender mit der Rolle "Administrator" bleiben erhalten. Die Anwender mit den Rollen "Geräteverwalter", "Transponder-Verwalter" und "Gast" werden durch die Anwender in der Sicherungsdatei ersetzt.

8.26 Auf Werkseinstellungen zurücksetzen

Der PITreader kann durch einen Kurzschluss an den Klemmen TxD/RxD oder in der Web-Anwendung auf die Werkseinstellungen zurückgesetzt werden. Abhängig davon, welche Art des Zurücksetzens gewählt wird, werden unterschiedliche Daten gelöscht.

8.26.1 Zurücksetzen durch Kurzschluss an den Klemmen TxD/RxD

Bei einem Kurzschluss an den Klemmen TxD/RxD werden sämtliche Daten des PITreaders auf die Werkseinstellungen zurückgesetzt (auch die Basis-Codierung), nur das Diagnoseprotokoll bleibt erhalten.
Gehen Sie wie folgt vor:

- Legen Sie vor dem Booten des Geräts einen Kurzschluss an den Klemmen TxD und RxD an.
  Die LED leuchtet gelb, das Gerät bootet nicht.
- Entfernen Sie den Kurzschluss.
  Die LED blinkt gelb.
- Legen Sie den Kurzschluss innerhalb von 10 Sekunden wieder an.
  Die LED leuchtet gelb und das Zurücksetzen auf Werkseinstellungen wird ausgeführt. Wenn das Zurücksetzen erfolgreich war, leuchtet die LED grün.

WICHTIG

Wenn innerhalb der 10 Sekunden der Kurzschluss nicht wieder angelegt wird, startet der PITreader ohne dass die Konfigurationsdaten auf Werkseinstellungen zurückgesetzt wurden.

- Entfernen Sie den Kurzschluss.
  Die LED leuchtet nicht mehr gelb bzw. grün und der Boot-Vorgang wird fortgesetzt.

INFO

Die Beschreibung, wie Sie die PIT gb mit PITreader auf Werkseinstellungen zurücksetzen, finden Sie in der Bedienungsanleitung PIT gb mit PITreader.

8.26.2 Zurücksetzen in der Web-Anwendung

- Wählen Sie im Menü ***Wartung*** unter der Überschrift ***Werksreset*** die Option ***Auf Werkseinstellungen zurücksetzen.***
  Das Auswahlmenü erscheint.
- Wählen Sie im Auswahlmenü ***Auf Werkseinstellungen zurücksetzen*** welche Daten zurückgesetzt werden sollen:
  - ***Gerätekonfiguration***
  - ***Diagnoseprotokoll***
  - ***Namen der Gerätegruppen***
  - ***Konfiguration der Anwenderdaten***
  - ***Berechtigungsliste***

– ***Transponder-Blockierliste***

- Klicken Sie unten auf das Feld ***Zurücksetzen***.
  Zur Bestätigung erscheint eine entsprechende Anzeige.

9 Firmware-Update

Die PITreader Firmware kann aktualisiert werden, wenn eine neue Firmware-Version vorliegt. Das Firmware-Update wird in der PITreader Web-Anwendung unter ***Wartung -> Firmware aktualisieren*** durchgeführt.

Ein Update-Paket kann im Download-Bereich zum Produkt auf der Pilz Internetseite heruntergeladen werden. Es gibt zwei unterschiedliche Dateiendungen:

- .fw
- .fwu

In der PITreader Web-Anwendung wird angezeigt, welches Update-Paket mit welcher Dateiendung für Ihr Produkt verwendet werden soll.

WICHTIG

Führen Sie regelmäßig ein Firmware-Update durch, um Security-relevante Aktualisierungen zu erhalten.

Ab der Firmware-Version 02.02.01 ist es auch möglich eine ältere Firmware-Version zu installieren, beachten Sie dabei:

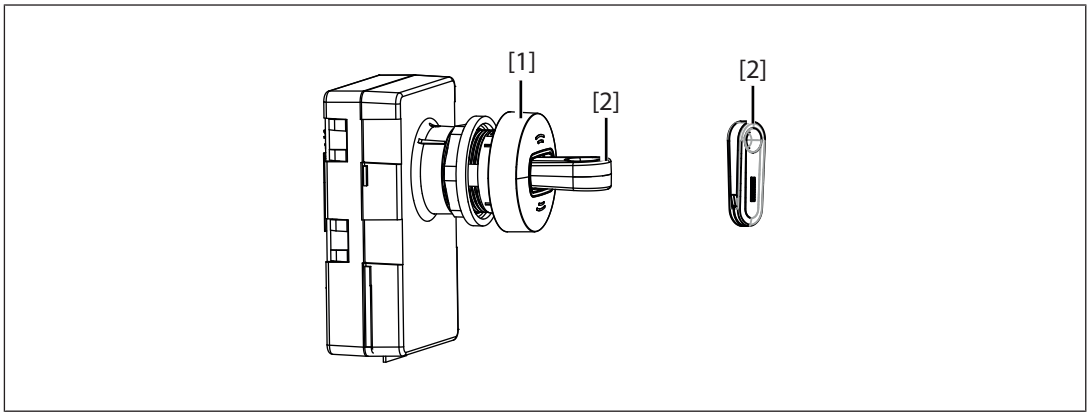
- Die Hinweise zur Unterstützung der Hardware-/Firmware-Versionen finden Sie in der Beschreibung "Produktänderungen" von PITreader.
- Falls der PITreader nach einem Downgrade nicht korrekt funktioniert, setzen Sie den PITreader auf Werkseinstellung zurück (siehe Auf Werkseinstellungen zurücksetzen [📖 88]).
- Pilz bietet Support ausschließlich für die aktuelle Firmware-Version.
- Pilz überwacht ausschließlich die aktuelle Firmware-Version auf Security-Schwachstellen.

10 Betrieb

10.1 Transponder platzieren

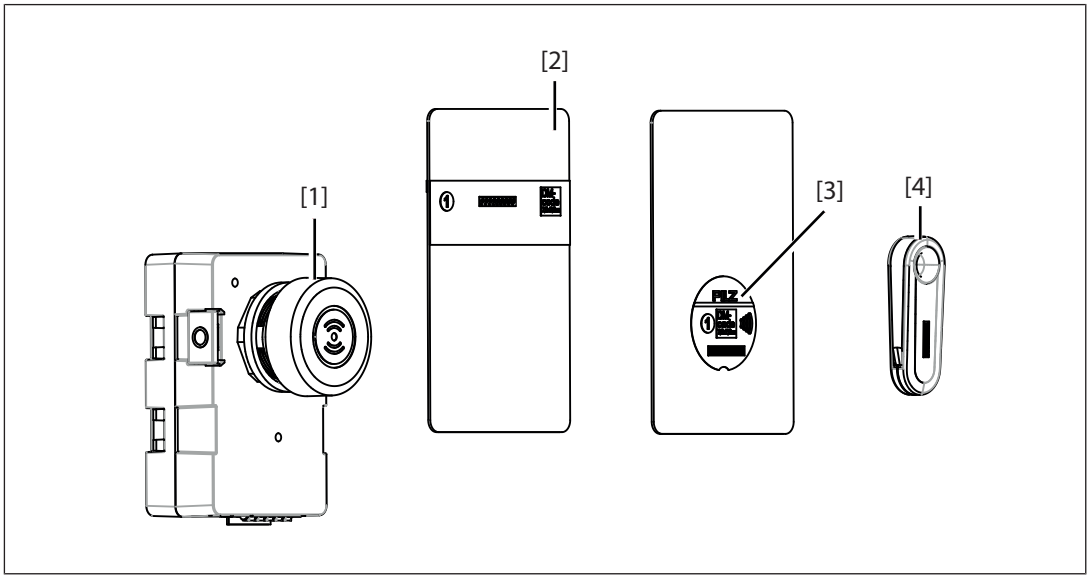
Nachfolgend sind die Transponder von Pilz beschrieben. Transponder von Fremdherstellern können teilweise auch verwendet werden, weitere Informationen finden Sie im Kapitel Transponder von Fremdherstellern mit gewähltem ISO/IEC Standards (ohne MIFARE DESFire-Anwendungen) [32].

10.1.1 PITreader Key



- Führen Sie den PITreader Transponder-Schlüssel [2] in den Lesekopf [1] ein, bis zum Anschlag.

10.1.2 PITreader Card

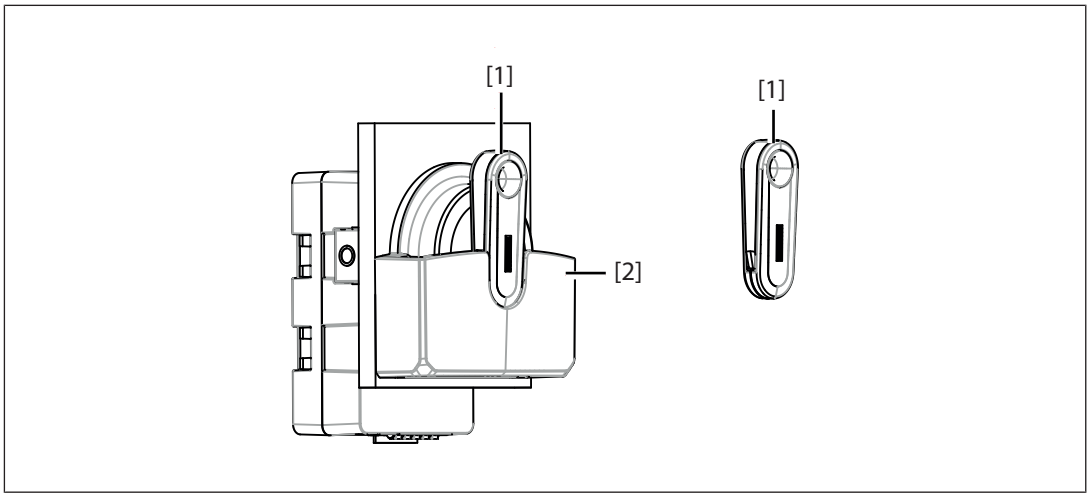


- Halten Sie die PITreader Transponder-Karte [2], den PITreader Transponder-Sticker [3] oder den PITreader Transponder-Schlüssel [4], vor den Lesekopf [1].

10.1.3 PITreader card holder

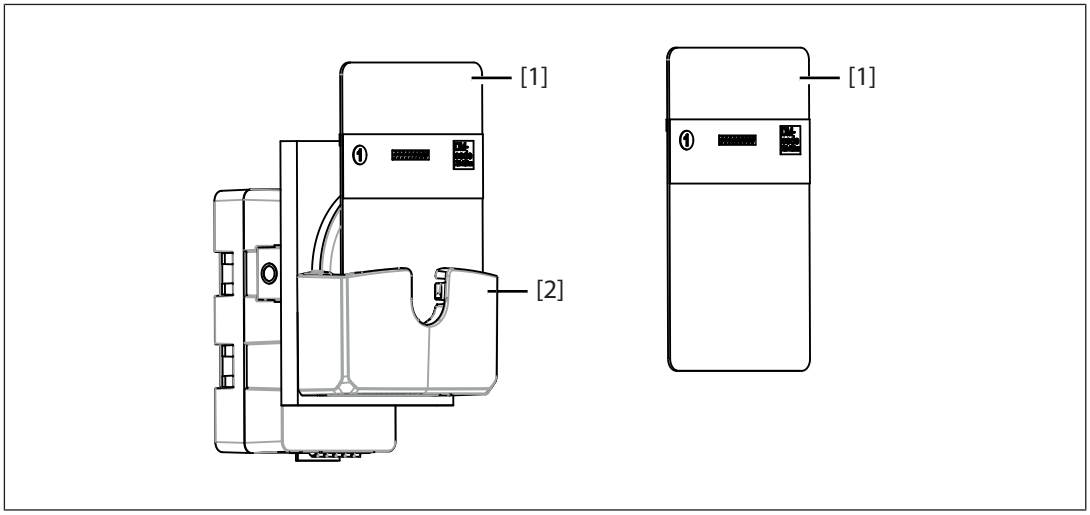
Sie können geeignete Transponder in den PITreader card holder einsetzen, oder auch nur vor den Lesekopf halten.

10.1.3.1 PITreader Transponder-Schlüssel



- Führen Sie den PITreader Transponder-Schlüssel [1] von oben in den PITreader card holder [2] ein, bis dieser einrastet.

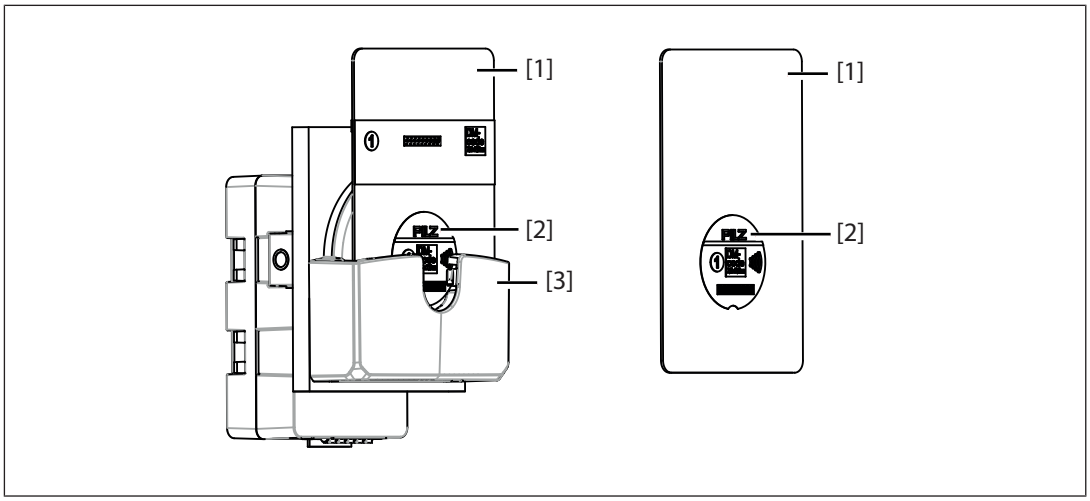
10.1.3.2 PITreader Transponder-Karte



Beachten Sie, dass immer nur eine PITreader Transponder-Karte [1] gesteckt wird.

- Führen Sie die PITreader Transponder-Karte [1] von oben in den PITreader card holder [2] ein, bis zum Anschlag.

10.1.3.3 PITreader Transponder-Sticker



- Führen Sie die Träger-Karte [1], mit dem aufgeklebten PITreader Transponder-Sticker [2], von oben in den PITreader card holder [3] ein, bis zum Anschlag.

10.2 LED-Anzeige

Legende

LED an

LED blinkt

Farbe	Zustand	Bedeutung
gelb		Gerät startet oder es wird ein Firmware-Update durchgeführt (wenn das Gerät nach dem Hochladen eines Firmware-Updates neu startet und das Firmware-Update übernommen wird, blinkt die LED gelb).
gelb		Gerät befindet sich im Authentifizierungsmodus Extern und es wurde noch keine Authentifizierung für den platzierten Transponder gesetzt.
blau		Gerät ist betriebsbereit, es wurde kein Transponder erkannt.
blau		Modus zur Lokalisierung des Geräts ist aktiv (siehe Netzwerkkonfiguration über Multicast-Protokoll [📖 67]).
grün		Transponder wurde als gültig erkannt.

Farbe	Zustand	Bedeutung
grün		4-Augen-Prinzip Mögliche Gründe: ▸ Der Authentifizierungsvorgang wurde mit dem ersten Transponder gestartet. ▸ Nach dem Entfernen des ersten Transponders blinkt die LED solange, bis entweder der zweite Transponder im Lesebereich platziert wird oder das Zeitfenster von 30 s abgelaufen ist.
rot		Transponder wurde als nicht gültig erkannt mögliche Gründe: ▸ Transponder im Lesebereich vorhanden: Die Authentifizierung wird verweigert (z. B. Berechtigung = 0). ▸ Kein Transponder im Lesebereich vorhanden: Die Authentifizierung am Gerät ist gesperrt (z. B. über 24 V-I/O-Port oder Einzelauthentifizierung). Sie finden weitere Informationen in der Web-Anwendung unter ***Status -> Authentifizierung***

Farbe	Zustand	Bedeutung
rot		Störung ▸ Mögliche Gründe (nur PITreader Card): – Ein Transponder von Pilz wurde nicht eindeutig erkannt. – Es werden mehrere Transponder von Pilz erkannt. – Es wird mindestens ein Transponder eines Fremdherstellers erkannt. Mögliche Abhilfen: – Transponder aus dem Lesebereich entfernen – genau einen Transponder von Pilz im Lesebereich platzieren. Hinweis: Nach der Fehlerbehebung wird die Störungsanzeige automatisch deaktiviert. ▸ Weitere Gründe (alle PITreader): z. B. Hardware-Fehler, Konfigurationsfehler, ungültiger oder nicht codierter Transponder, usw. Mögliche Abhilfen bei einem Konfigurationsfehler und wenn das Gerät nicht mehr unter der eingestellten IP-Adresse erreichbar ist: – Versuchen Sie die Web-Anwendung mit der Default-IP-Adresse zu öffnen oder – Setzen Sie das Gerät auf Werkseinstellungen zurück.

Wenn der PITreader durch einen Kurzschluss an TxD/RxD auf die Werkseinstellungen zurückgesetzt wird, nimmt die LED folgende Zustände an:

Beschreibung	Farbe	Zustand
Kurzschluss liegt an	gelb	
Kurzschluss wird weggenommen		
Kurzschluss wird wieder angelegt, das Rücksetzen auf die Werkseinstellungen wird ausgeführt		
Gerät wurde erfolgreich auf die Werkseinstellungen zurückgesetzt	grün	

Siehe auch Auf Werkseinstellungen zurücksetzen [88].

10.3 Personenbezogene Daten

In PITreadern und Transponder können personenbezogene Daten erfasst, gespeichert und verarbeitet werden.

10.3.1 PITreader

Personenbezogene Daten werden im PITreader über die Web-Anwendung abgelegt unter

- ***Anwender -> Geräteanwender***, siehe Geräteanwender [68].
- ***Diagnose -> Protokoll,*** siehe Datenprotokollierung mit personenbezogenen Daten [71].

Sie können alle personenbezogene Daten löschen, indem Sie die Konfiguration auf Werkseinstellung zurücksetzen, siehe Auf Werkseinstellungen zurücksetzen [88].

10.3.2 Transponder

Anwenderdaten werden auch auf dem Transponder gespeichert. Informationen zum Löschen von Anwenderdaten, siehe Anwenderdaten auf Transpondern löschen [83].

10.4 Diagnose

Der PITreader stellt Möglichkeiten zur Gerätediagnose und Statistikauswertung zur Verfügung.

- Diagnose mithilfe der Geräte-LED

  Sie finden Informationen zur Auswertung der Geräte-LED unter LED-Anzeige [93].

- Diagnose mithilfe der Diagnoseliste (Web-Anwendung)

  Die Diagnoseliste enthält eine Liste mit den aktiven Alarmen. Sie können die Diagnoseliste in der Web-Anwendung unter ***Diagnose*** auslesen.

- Diagnose mithilfe des Diagnoseprotokolls (Web-Anwendung)

  Im Diagnoseprotokoll werden die Ereignisse mit Zeitstempel protokolliert; d. h. eine Meldung wird nach "Meldung aufgetreten" und "Meldung gegangen" protokolliert. Sie können das Diagnoseprotokoll in der Web-Anwendung unter ***Diagnose*** auslesen.

  Unter ***Diagnose -> Protokoll*** können Sie über den Filter einstellen, ob ***Alle Meldungstypen*** oder nur ***Audit-Trail-Meldungen*** (Meldungen zum Prozessablauf) angezeigt werden sollen. Über den Button ***Protokoll exportieren*** können Sie eine Sicherung der im Filter ausgewählten Diagnosemeldungen erstellen. Beim Export wird eine CSV-Datei erstellt.

  Wenn Sie eine sichere Auswerteeinheit PIT m4SEU angeschlossen haben, werden alle Informationen über die Schnittstelle für Statusinformationen der PIT m4SEU protokolliert.

WICHTIG

Sicherung personenbezogener Daten

Abhängig vom eingestellten Filter können Protokolle personenbezogene Daten enthalten.

Stellen Sie sicher, dass beim Export eines Protokolls mit personenbezogenen Daten ein ausreichend gesichertes Speichermedium verwendet wird.

- Statistik (Web-Anwendung)

  Sie finden Informationen zu verschiedenen Einstellungen und Auswertungen unter Statistik [📖 98].

10.4.1 Statistik

In der Web-Anwendung können unter ***Diagnose -> Statistik*** verschiedene Einstellungen für die statistischen Auswertungen vorgenommen werden und es werden verschiedene Informationen zu den statistische Auswertungen angezeigt.

- Startdatum

  Das tatsächliche Startdatum für die statistische Auswertung wird angezeigt.

- Button ***Aktualisieren***

  Über den Button ***Aktualisieren*** kann die Statistik neu erstellt werden.

- ***Startdatum*** und ***Enddatum*** festlegen

  Durch die Eingabe eines Start- und Enddatums kann ein Zeitfenster festgelegt werden, für das die statistischen Auswertungen angezeigt werden.

- Bereich ***Transponder***

  Die Tabelle unter ***Transponder*** wird nur angezeigt, wenn die Protokollierung personenbezogener Daten unter ***Konfiguration -> Einstellungen -> Erweiterte Funktionen*** aktiviert ist. Die Transponder werden in der Tabelle über ihre Security-IDs identifiziert (Spalte ***Security-ID***).

  Statistische Werte zu einem Transponder:

  – ***Dauer (Gesamt)***

    Die Spalte enthält die entsprechend berechnete gesamte Zeit, die sich ein Transponder im Lesebereich befunden hat.

    - Format der Zeitangabe siehe [1].

  – ***Dauer (Median)***

    Die Spalte enthält die nach "Median"-Gesichtspunkten berechnete Zeit, die sich ein Transponder im Lesebereich befunden hat.

    - Format der Zeitangabe siehe [1]
    - Definition für "Median" siehe [2]

  – ***Erfolgreiche Authentifizierung***

    Die Spalte enthält die Summe aller erfolgreichen Authentifizierungsversuche eines Transponders.

  – ***Fehlgeschlagene Authentifizierung***

    Die Spalte enthält die Summe aller fehlgeschlagenen Authentifizierungsversuche eines Transponders.

  Hinweis:

  Protokolleinträge, die aufgrund der Einstellung zur Protokollierung personenbezogener Daten keine Security-ID in den Parametern enthalten, werden bei der Statistik-Auswertung ignoriert; d. h. die Tabelle unter ***Transponder*** enthält keine Einträge für Transponder ohne Angabe in der Spalte ***Security-ID***.

- Bereich ***Authentifizierte Berechtigung***

  In der Tabelle unter ***Authentifizierte Berechtigung*** werden nur die Berechtigungen aufgelistet, mit denen mindestens einmal eine erfolgreiche Authentifizierung ausgeführt wurde.

Statistische Werte zu einer Berechtigung:

– ***Berechtigung***

Die Spalte enthält die authentifizierte Berechtigung als Wert zwischen 0 und 64.

– ***Anzahl***

Der Wert in dieser Spalte gibt an, wie oft mit einer Berechtigung eine erfolgreiche Authentifizierung durchgeführt wurde.

– ***Dauer (Gesamt)***

Die Spalte enthält die entsprechend berechnete gesamte Zeit, während der die Berechtigung im Gerät aktiv war.

- Format der Zeitangabe siehe [1]

– ***Dauer (Median)***

Die Spalte enthält die nach "Median"-Gesichtspunkten berechnete Zeit, während der die Berechtigung im Gerät aktiv war.

- Format der Zeitangabe siehe [1]
- Definition für "Median" siehe [2]

Hinweis:

Wenn ein Transponder entfernt und innerhalb von maximal 2 s erneut platziert wird, dann wird dies in der Statistik nicht als neue Authentifizierung gewertet.

▸ Bereich ***Aktivierte Betriebsart***

Die Auswertungen basieren auf den gemeldeten Daten einer sicheren Auswerteeinheit PIT m4SEU. Die Tabelle wird deswegen nur angezeigt, wenn an einer Basiseinheit eine sichere Auswerteeinheit angeschlossen ist.

In der Tabelle unter ***Aktivierte Betriebsart*** werden Auswertungen zu den Betriebsarten angezeigt.

– Betriebsart

In der Spalte sind alle Betriebsarten aufgelistet (Betriebsart 1 … 5).

– Dauer (Gesamt)

Die Spalte enthält die entsprechend berechnete gesamte Zeit, während der die Betriebsart im Gerät aktiv war.

- Format der Zeitangabe siehe [1]

– Dauer (Median)

Die Spalte enthält die nach "Median"-Gesichtspunkten berechnete Zeit, während der die Betriebsart im Gerät aktiv war.

- Format der Zeitangabe siehe [1]
- Definition für "Median" siehe [2]

[1]

Zeitformat: *<Tag(d) Stunde(h) Minute(m) Sekunde(s)>*

Beispiele:

▸ 1h 0m 1s

▸ 1d 0h 20m 5s

[2]

Der Median einer Reihe von Werten ist derjenige Wert, der genau in der Mitte steht, wenn man die Werte der Größe nach sortiert.

11 Wartung und Prüfung

Bei bestimmungsgemäßem Betrieb müssen an dem Produkt keine Wartungsarbeiten vorgenommen werden.

- Schicken Sie ein fehlerhaftes Produkt an Pilz zurück.

12 Außerbetriebnahme

PITreader und Transponder können personenbezogene Daten enthalten.

- Setzen Sie im PITreader die Konfiguration auf Werkseinstellungen zurück, siehe Auf Werkseinstellungen zurücksetzen [📖 88].
- Löschen Sie die Daten auf den Transpondern, siehe Anwenderdaten auf Transpondern löschen [📖 83].

12.1 Entsorgung

- Beachten Sie bei der Außerbetriebnahme die lokalen Gesetze zur Entsorgung von elektronischen Geräten, z. B. Elektro- und Elektronikgerätegesetz.

13 Technische Daten

Bei Normenangaben ohne Datum gelten die 2018-12 gültigen Ausgabestände.

Die technischen Daten der PITreader base unit (Artikelnummer 402255) und die technischen Daten der PITreader S base unit (Artikelnummer 402256) sind identisch.

Die technischen Daten der PITreader card unit (Artikelnummer 402320) und die technischen Daten der PITreader S card unit (Artikelnummer 402321) sind identisch.

Allgemein	**402255**	**402320**
Zertifizierungen	**CE, FCC, IC, UKCA, cULus Listed**	**CE, FCC, IC, UKCA, cULus Listed**
Funktionsweise Sensor	**Transponder**	**Transponder**
Transponder	**402255**	**402320**
Art des Transponders	**Transponder-Schlüssel**	**Transponder-Karte, Transponder-Schlüssel, Transponder-Sticker**
Energieversorgung des Transponders	**passiv (batterielos)**	**passiv (batterielos)**
Frequenzband	**13,24 - 13,88 MHz**	**13,24 - 13,88 MHz**
Max. Sendeleistung	**170 mW**	**170 mW**
Elektrische Daten	**402255**	**402320**
Versorgungsspannung		
Spannung	**24 V**	**24 V**
Art	**DC**	**DC**
Art des Netzteils	**SELV/PELV**	**SELV/PELV**
Spannungstoleranz	**-15 %/+20 %**	**-15 %/+20 %**
Leistung des externen Netzteils (DC)	**4 W**	**4 W**
Externe Gerätesicherung F1	**4 A, Leitungsschutzschalter 24 V DC, Charakteristik B/C**	**4 A, Leitungsschutzschalter 24 V DC, Charakteristik B/C**
Statusanzeige	**LED**	**LED**
Verlustleistung	**2,5 W**	**2,5 W**
Eingänge	**402255**	**402320**
Signalpegel bei "1"	**15 - 30 V DC**	**15 - 30 V DC**
Eingangsstrombereich	**4 mA**	**4 mA**
Galvanische Trennung	**nein**	**nein**
Halbleiterausgänge	**402255**	**402320**
Gesamtleistung ext. Last, Halbleiter	**1,2 W**	**1,2 W**
Anzahl	**1**	**1**
Schaltstrom pro Ausgang	**50 mA**	**50 mA**
Galvanische Trennung	**nein**	**nein**
Kurzschlussfest	**ja**	**ja**
Ethernet-Schnittstelle	**402255**	**402320**
Anzahl	**1**	**1**

Ethernet-Schnittstelle	402255	402320
IP-Adresse Werkseinstellung	**192.168.0.12**	**192.168.0.12**
Anschlussart	**RJ45**	**RJ45**
Übertragungsrate	**10/100 Mbit/s**	**10/100 Mbit/s**
Zeiten	**402255**	**402320**
Überbrückung bei Spannungseinbrüchen der Versorgungsspannung	**10 ms**	**10 ms**
Umweltdaten	**402255**	**402320**
Umgebungstemperatur		
nach Norm	**EN 60068-2-14**	**EN 60068-2-14**
Temperaturbereich	**-30 - 55 °C**	**-30 - 55 °C**
Lagertemperatur		
nach Norm	**EN 60068-2-1/-2**	**EN 60068-2-1/-2**
Temperaturbereich	**-30 - 70 °C**	**-30 - 70 °C**
Feuchtebeanspruchung		
nach Norm	**EN 60068-2-78**	**EN 60068-2-78**
Feuchtigkeit	**93 % r. F. bei 40 °C**	**93 % r. F. bei 40 °C**
Max. Betriebshöhe über NN	**2000 m**	**2000 m**
EMV	**EN 301489-1 V2.1.1**	**EN 301489-1 V2.1.1**
MTBF	**36 Jahre**	**36 Jahre**
Schwingungen		
nach Norm	**EN 60068-2-6**	**EN 60068-2-6**
Frequenz	**5 - 8,4 Hz, 8,4 - 150 Hz**	**5 - 8,4 Hz, 8,4 - 150 Hz**
Amplitude	**3,5 mm**	**3,5 mm**
Beschleunigung	**max. 1g**	**max. 1g**
Schockbeanspruchung		
nach Norm	**EN 60068-2-27**	**EN 60068-2-27**
Beschleunigung	**15g**	**15g**
Dauer	**11 ms**	**11 ms**
Schutzart		
nach Norm	**EN 60529**	**EN 60529**
Gehäuse	**IP20**	**IP20**
Front	**IP65/IP67**	**IP65/IP67**
Einbauraum (z. B. Schaltschrank)	**≥ IP54**	**≥ IP54**
Mechanische Daten	**402255**	**402320**
Einbaulage	**beliebig**	**beliebig**
Material		
Unterseite	**PC**	**PC**
Front	**PC**	**PC**
Anschlussart	**Federkraftklemme steckbar**	**Federkraftklemme steckbar**
Befestigungsart	**steckbar**	**steckbar**
Max. Anzugsdrehmoment Befestigungsschrauben	**1,3 - 2,1 Nm**	**1,3 - 2,1 Nm**

Mechanische Daten	402255	402320
Leiterquerschnitt bei Federkraftklemmen: flexibel mit/ohne Aderendhülse	**0,2 - 1,5 mm², 24 - 14 AWG**	**0,2 - 1,5 mm², 24 - 14 AWG**
Federkraftklemmen: Klemmstellen pro Anschluss	**1**	**1**
Abisolierlänge bei Federkraftklemmen	**8 mm**	**8 mm**
Abmessungen		
Höhe	**54 mm**	**49 mm**
Breite	**72 mm**	**72 mm**
Tiefe	**45 mm**	**45 mm**
Gewicht	**47 g**	**62 g**

Hinweis:

Die technischen Daten der PIT gb mit PITreader finden Sie in der Bedienungsanleitung PIT gb mit PITreader.

14 Sicherheitstechnische Kenndaten

Informationen zur Berechnung der sicherheitstechnischen Kenndaten finden Sie - je nach Produkt - in der

- Systembeschreibung PITmode flex (1005276).
- Systembeschreibung PITmode flex visu (1005364).
- Systembeschreibung Wartungssicherung Key-in-pocket (1006613).
- Bedienungsanleitung PIT m4SEU (1004648).

15 Ergänzende Daten

15.1 Funkzulassungen PITreader Key

FCC/IC-Zulassung

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.

15.2 Funkzulassungen PITreader Card

FCC/IC-Zulassung

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.

15.3 Netzwerkdaten

Proto-koll	Rich-tung [*]	Trans-port-protokoll	Port-Nr.	Deakti-vierbar	Beschreibung
HTTP	in	TCP	1 … 65535 Default: 80	ja	**Web-Anwendung:** Browser wird immer nach HTTPS weitergeleitet
HTTPS	in	TCP	1 … 65535 Default: 443	nein	**Web-Anwendung:** Transport-Schutz durch TLSv1.2. Zugriff auf Web-Anwendung über Anwendername und Kennwort. Der Server wird durch ein X.509-Zertifikat authentifiziert.
Modbus TCP	in	TCP	1 … 65535 Default: 502	ja Default: inaktiv	**Modbus/TCP Server**
NTP	out	UDP	1 … 65535 Default: 123	ja Default: inaktiv	**SNTP-Client**
OPC UA	in	TCP	4840	ja Default: inaktiv	**PITreader OPC Server UA**
mDNS	in	UDP	5353	ja	**Netzwerkerkennung mit Multicast DNS** (224.0.0.251)
Multicast Configu-ration	in	UDP	7075	ja	**Netzwerkkonfiguration über Multicast-Protokoll** (239.255.0.12)

[*]

in: Der Kommunikationspartner startet die Kommunikation mit dem Produkt.

out: Das Produkt startet die Kommunikation mit dem Kommunikationspartner.

15.4 Übersicht der Berechtigungen

Berechtigung	Code	
	hexadezimal	dezimal
0	0x00000000	0
1	0x000001ff	511
2	0x00003e0f	15887
3	0x00003ff0	16368
4	0x0001c633	116275
5	0x0001c7cc	116684
6	0x0001f83c	129084
7	0x0001f9c3	129475
8	0x00064a55	412245
9	0x00064baa	412586
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

Berechtigung	Code	
	hexadezimal	dezimal
35	0x0030739a	3175322
36	0x00318a59	3246681
37	0x00318ba6	3247014
38	0x0031b456	3257430
39	0x0031b5a9	3257769
40	0x0036063f	3540543
41	0x003607c0	3540928
42	0x00363830	3553328
43	0x003639cf	3553743
44	0x0037c00c	3653644
45	0x0037c1f3	3654131
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

16 Bestelldaten

16.1 Authentifizierungssystem PITreader Key

Produkttyp	Merkmale	Artikel-Nr.
PITreader base unit	RFID-Authentifizierungssystem Inhalt: Basiseinheit, Stecker [402307] Notwendiges Zubehör: PITreader key adapter	402255
PITreader S base unit	RFID-Authentifizierungssystem mit erweitertem Funktionsumfang, Inhalt: Basiseinheit, Stecker [402307] Notwendiges Zubehör: PITreader key adapter	402256
PITreader key Adapter h	1x PITreader Schlüsselaufnahme horizontal + 1x Mutter für PITreader base unit	402308

16.2 Authentifizierungssystem PITreader Card

Produkttyp	Merkmale	Artikel-Nr.
PITreader card unit	RFID-Authentifizierungssystem für Karten, Sticker & Schlüssel Inhalt: Basiseinheit, Stecker [402307], PITreader card Adapter	402320
PITreader S card unit	RFID-Authentifizierungssystem für Karten, Sticker & Schlüssel, mit erweitertem Funktionsumfang Inhalt: Basiseinheit, Stecker [402307], PITreader card Adapter	402321

16.3 Transponder-Schlüssel

Produkttyp	Merkmale	Artikel-Nr.
PITreader key ye g	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigungen frei konfigurierbar Farbe: gelb Material: Kunststoff	402260
PITreader key ye g bk	Generischer Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigungen frei konfigurierbar Farbe: schwarz Material: Kunststoff	402260BK
PITreader key ye g bl	Generischer Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigungen frei konfigurierbar Farbe: blau Material: Kunststoff	402260BL
PITreader key ye g gn	Generischer Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigungen frei konfigurierbar Farbe: grün Material: Kunststoff	402260GN
PITreader key ye g rd	Generischer Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigungen frei konfigurierbar Farbe: rot Material: Kunststoff	402260RD

Produkttyp	Merkmale	Artikel-Nr.
PITreader key ye g wt	Generischer Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigungen frei konfigurierbar Farbe: weiß Material: Kunststoff	402260WT
PITreader key ye g ye	Generischer Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigungen frei konfigurierbar Farbe: hellgelb Material: Kunststoff	402260YE
PITreader key ye 1	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1 Farbe: gelb Material: Kunststoff	402261
PITreader key ye 2	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1 und 2 Farbe: gelb Material: Kunststoff	402262
PITreader key ye 3	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1, 2 und 3 Farbe: gelb Material: Kunststoff	402263
PITreader key ye 4	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1, 2, 3 und 4 Farbe: gelb Material: Kunststoff	402264
PITreader key ye 5	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1, 2, 3, 4 und 5 Farbe: gelb Material: Kunststoff	402265
PITreader key ye 5 service	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1, 2, 3, 4 und 5 (Service) Farbe: gelb Material: Kunststoff	402269

16.4 Transponder-Karten

Produkttyp	Merkmale	Artikel-Nr.
PITreader card ye g	Transponder-Karte für Authentifizierungssystem PITreader Card, Berechtigungen frei konfigurierbar Farbe: gelb Material: Kunststoff	402330
PITreader card ye 1	Transponder-Karte für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1 Farbe: gelb Material: Kunststoff	402331
PITreader card ye 2	Transponder-Karte für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1 und 2 Farbe: gelb Material: Kunststoff	402332

Produkttyp	Merkmale	Artikel-Nr.
PITreader card ye 3	Transponder-Karte für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1, 2 und 3 Farbe: gelb Material: Kunststoff	402333
PITreader card ye 4	Transponder-Karte für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1,2,3 und 4 Farbe: gelb Material: Kunststoff	402334
PITreader card ye 5	Transponder-Karte für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1, 2, 3, 4 und 5 Farbe: gelb Material: Kunststoff	402335
PITreader card ye 5 service	Transponder-Karte für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1, 2, 3, 4 und 5 (Service) Farbe: gelb Material: Kunststoff	402339

16.5 Transponder-Sticker

Produkttyp	Merkmale	Artikel-Nr.
PITreader sticker ye g	Transponder-Sticker für Authentifizierungssystem PITreader Card, Berechtigungen frei konfigurierbar Farbe: gelb Material: Kunststoff	402340
PITreader sticker ye 1	Transponder-Sticker für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1 Farbe: gelb Material: Kunststoff	402341
PITreader sticker ye 2	Transponder-Sticker für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1 und 2 Farbe: gelb Material: Kunststoff	402342
PITreader sticker ye 3	Transponder-Sticker für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1, 2 und 3 Farbe: gelb Material: Kunststoff	402343
PITreader sticker ye 4	Transponder-Sticker für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1, 2, 3 und 4 Farbe: gelb Material: Kunststoff	402344
PITreader sticker ye 5	Transponder-Sticker für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1, 2, 3, 4 und 5 Farbe: gelb Material: Kunststoff	402345
PITreader sticker ye 5 service	Transponder-Sticker für Authentifizierungssystem PITreader Card, Berechtigung für Betriebsart 1, 2, 3, 4 und 5 (Service) Farbe: gelb Material: Kunststoff	402349

16.6 Zubehör

Produkttyp	Merkmale	Artikel-Nr.
PIT es wrench	Montageschlüssel für PIT es Taster	400222
PITreader card holder	Kunststoffhalter für PITreader (S) card [402320/21] für Transponder-Karten und Transponder-Schlüssel als optionales Zubehör	402323

17 EG-Konformitätserklärung

Diese(s) Produkt(e) erfüllen die Anforderungen folgender Richtlinien des europäischen Parlaments und des Rates.

- 2014/53/EU über Funkanlagen

Die vollständige EG-Konformitätserklärung finden Sie im Internet unter www.pilz.com/downloads.
Bevollmächtigter: Pilz GmbH & Co. KG, Felix-Wankel-Str. 2, 73760 Ostfildern, Deutschland

18 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

Technische Unterstützung von Pilz erhalten Sie rund um die Uhr.

Amerika
Brasilien
+55 11 97569-2804
Kanada
+1 888 315 7459
Mexiko
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asien
China
+86 400-088-3566
Japan
+81 45 471-2281
Südkorea
+82 31 778 3390

Australien und Ozeanien
Australien
+61 3 95600621
Neuseeland
+64 9 6345350

Europa
Belgien, Luxemburg
+32 9 3217570
Deutschland
+49 711 3409-444
Frankreich
+33 3 88104003
Großbritannien
+44 1536 460866
Irland
+353 21 4804983
Italien, Malta
+39 0362 1826711
Niederlande
+31 347 320477
Österreich
+43 1 7986263-444
Schweiz
+41 62 88979-32
Skandinavien
+45 74436332
Spanien
+34 938497433
Türkiye
+90 216 5775552

Unsere internationale Hotline erreichen Sie unter:
+49 711 3409-222
support@pilz.com

Pilz entwickelt umweltfreundliche Produkte unter Verwendung ökologischer Werkstoffe und energiesparender Techniken. In ökologisch gestalteten Gebäuden wird umweltbewusst und energiesparend produziert und gearbeitet. So bietet Pilz Ihnen Nachhaltigkeit mit der Sicherheit, energieeffiziente Produkte und umweltfreundliche Lösungen zu erhalten.

BLUEcoMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

German Standards
BRAND OF THE CENTURY 2022

Qualitätsmanagement ISO 9001:2015 REG. NR. 2462
Umweltmanagement ISO 14001 REG. NR. 2462
Energiemanagement ISO 50001 REG. NR. 2462

1004806-DE-17, 2026-03 Printed in Germany

Wir sind international vertreten. Nähere Informationen entnehmen Sie bitte unserer Homepage www.pilz.com oder nehmen Sie Kontakt mit unserem Stammhaus auf.

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

PILZ
THE SPIRIT OF SAFETY