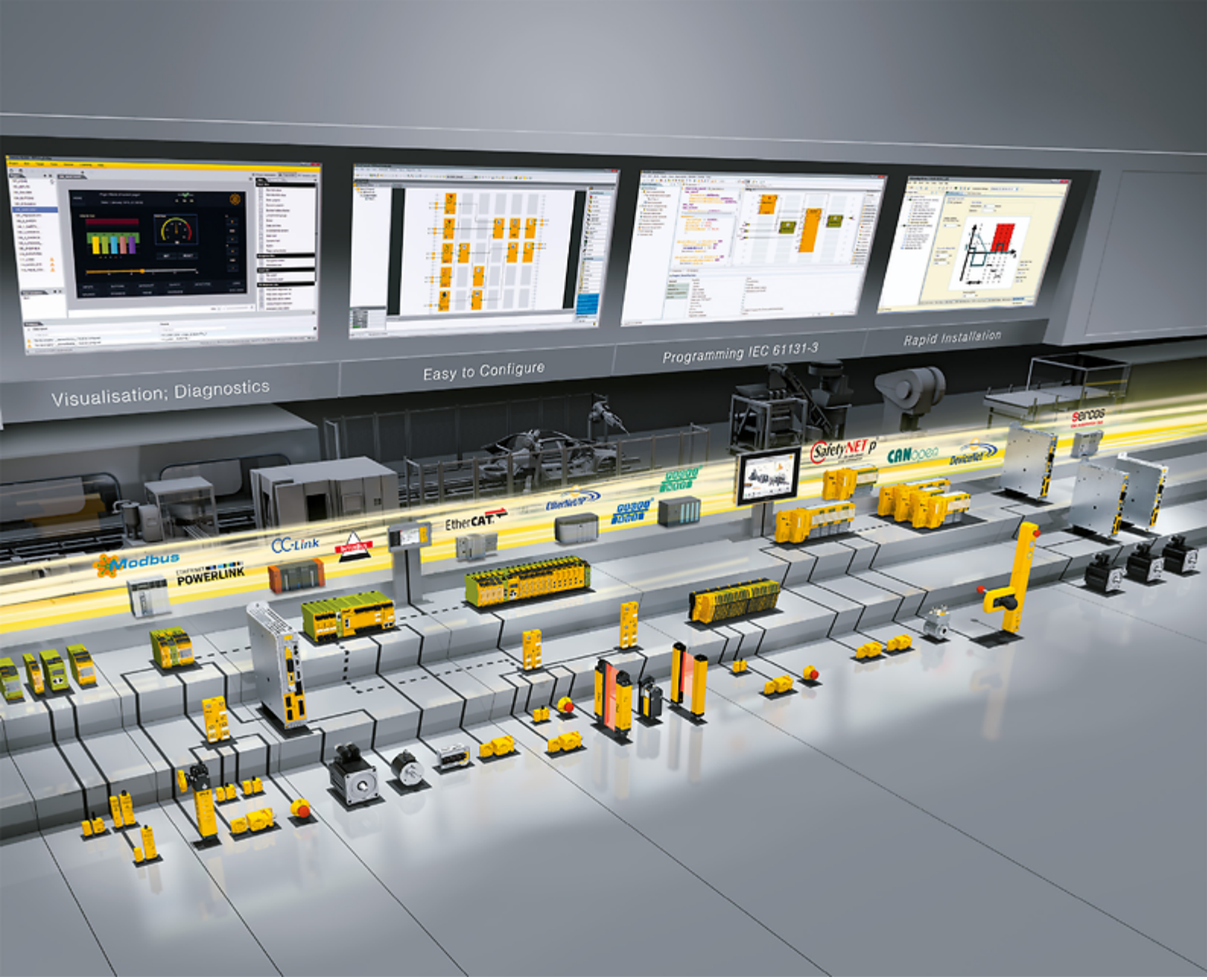


PITreader

PILZ
THE SPIRIT OF SAFETY

- Befehls- und Meldegeräte

Bedienungsanleitung-1004806-DE-06

Dieses Dokument ist das Originaldokument.

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 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.

1.4 Fremdhersteller-Lizenzinformationen

Dieses Produkt enthält Open Source-Software verschiedener Lizenzen.

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

Die zugehörigen Quellcodes können über opensource@pilz.de angefordert werden.

Ihre Anfrage sollte Folgendes beinhalten: (a) den Namen der Firmware, (b) die Version der Firmware, (c) Ihren Namen, (d) Ihren Firmennamen (falls zutreffend), (e) Ihre Rückantwortadresse und (f) Ihre E-Mail-Adresse (falls möglich).

Pilz kann eine Gebühr für den Datenträger und den Versand erheben.

Die Anforderung des Quellcodes muss spätestens 3 Jahre nach Erhalt der zugehörigen MPL eingehen. Unabhängig von diesem Zeitraum senden wir Ihnen, solange Pilz für dieses Gerät Ersatzteile oder technischen Support anbietet, eine komplette, maschinenlesbare Kopie des Quellcodes zu.

2 Übersicht

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

- Transponder-Schlüssel (PITreader key) 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, Bestell-Nr. 402 250) zur sicheren Betriebsartenwahl (nur bei PITreader Basiseinheit)

2.1 Gerätemerkmale

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

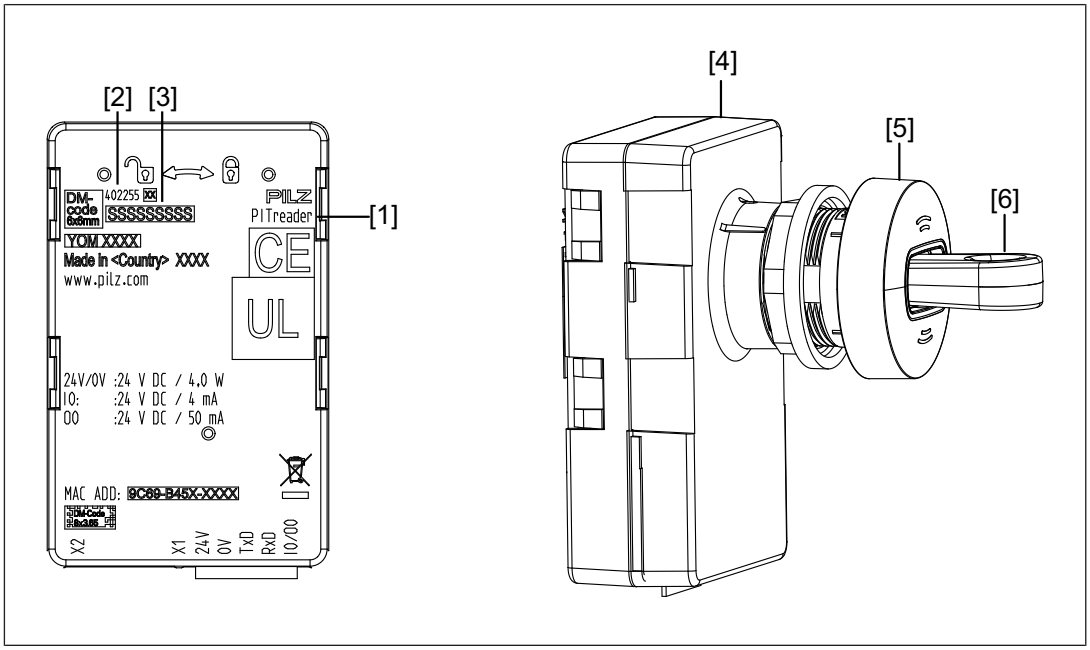
Nur bei PITreader Basiseinheit:

- Schnittstelle für den Anschluss einer sicheren Auswerteeinheit (SEU) zur Betriebsartenwahl
- Für Einbauöffnungen D22 (Durchmesser 22,3 mm +0,4 mm/-0,0 mm) gemäß EN 60947-5-1 mit Verdrehsicherung

Nur PITreader vom Typ PITreader S base unit und die Varianten des PIT gb mit der Ergänzung "X" im Gerätenamen (z B. PIT gb XLLE y up ETH, PIT gb XLLE y down ETH):

- integrierter OPC Server UA

2.2 Geräteansicht PITreader mit Basiseinheit



Legende

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

X2 Ethernet-Schnittstelle

[1] Gerätebezeichnung

[2] Bestellnummer

[3] Seriennummer

[4] PITreader base unit, inklusive Federkraftklemme (Bestell-Nr. 402 255)

[5] PITreader key adapter h (Bestell-Nr. 402 308)

[6] PITreader key (siehe auch Transponder-Schlüssel [📖 19])

3 Sicherheit

3.1 Bestimmungsgemäße Verwendung

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

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 [51]) 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.

3.2 Sicherheitsvorschriften

3.2.1 Zusätzlich geltende Dokumente

Lesen und beachten Sie auch folgende Dokumente:

- Bedienungsanleitung des verwendeten PITreaders
  (z. B. PIT gb RLLE y up ETH, PIT gb RLLE y down ETH)
- Bedienungsanleitung PITreader REST API
- Bedienungsanleitung PITreader OPC Server UA

3.2.2 Qualifikation des Personals

Aufstellung, Montage, Programmierung, Inbetriebsetzung, Betrieb, Außerbetriebsetzung und Wartung der Produkte dürfen nur von 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 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).

3.2.4 Entsorgung

- Beachten Sie bei der Außerbetriebsetzung die lokalen Gesetze zur Entsorgung von elektronischen Geräten (z. B. Elektro- und Elektronikgerätegesetz).

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.
- Stellen Sie sicher, dass das Produkt durch einen Router (Layer-3 Switch oder Firewall) vom Firmennetzwerk getrennt ist.
- Vergeben Sie nur sichere Kennwörter. Beachten Sie bei der Vergabe von Kennwörtern:
  - Das Kennwort sollte mindestens 8 Zeichen lang sein.
  - Das Kennwort sollte aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen.
  - Das Kennwort sollte möglichst nicht in Wörterbüchern vorkommen.
  - Das Kennwort sollte nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen (also nicht: 1234abcd).
  - Nutzen Sie einen Kennwort-Manager, um komplexe Kennwörter gut verwalten zu können.
  - Sprachabhängige Zeichen sind nicht in jeder Tastatursprache vorhanden.

  - Ändern Sie regelmäßig die Kennwörter der auf dem System angelegten Anwenderkonten bzw. fordern Sie die Anwender auf, ihre Kennwörter selbst zu ändern.
  - Weisen Sie die Anwender auf den verantwortungsvollen Umgang mit Ihren Zugangsdaten hin.
- Beschränken Sie Modbus/TCP-Verbindungen auf das maschineninterne Netzwerk. Sichern Sie die Verbindung gegenüber externen Netzwerken ab.
- Installieren Sie zeitnah Firmware-Updates, die von Pilz für das Produkt zur Verfügung gestellt werden.
- Bewahren Sie die Transponder-Schlüssel an einem sicheren Ort auf und schützen Sie sie vor unbefugten Zugriffen. Weisen Sie die Anwender auf die Sicherheitsrisiken durch die Weitergabe von Transponder-Schlüsseln hin.
- Protokolldaten können personenbezogene Daten enthalten. Legen Sie exportierte Protokolle 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.

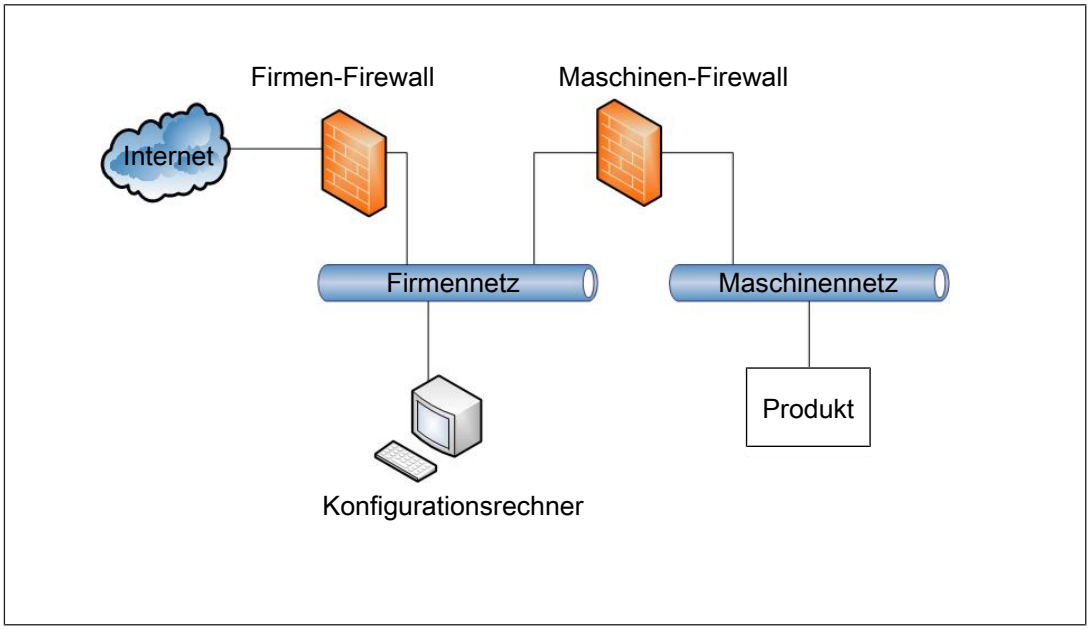


Abb.: Beispiel Netzwerktopologie

- Beachten Sie die Netzwerkdaten [53] für die Risikoanalyse und die Security-Maßnahmen.

5 Funktionsbeschreibung

5.1 Ablauf der Authentifizierung

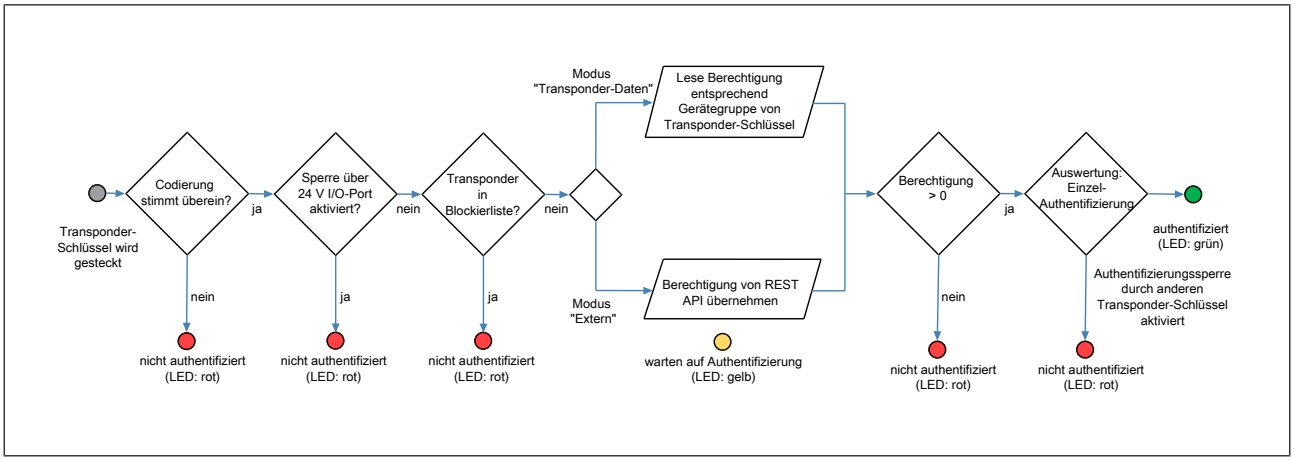


Abb.: Ablauf der Authentifizierung

5.2 Authentifizierungsmodi

Der PITreader unterstützt zwei Authentifizierungsmodi:

- Transponder-Daten [📖 14]
  Vordefinierte, gruppenbasierte Authentifizierung im Transponder-Schlüssel
- Extern [📖 16]
  Authentifizierung erfolgt extern, z. B. über PLC, HMI

Im Auslieferungszustand ist der Authentifizierungsmodus Transponder-Daten eingestellt. Der Authentifizierungsmodus kann in der Web-Anwendung geändert werden.

5.2.1 Transponder-Daten

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

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

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

INFO

Bitte beachten Sie, dass im Authentifizierungsmodus Transponder-Daten die Authentifizierung allein vom Besitz des Transponder-Schlüssels abhängt. Der Verlust eines Transponder-Schlüssels kann daher zu einem Security-Risiko führen.
Wir empfehlen Ihnen, die Security-IDs aller herausgegebenen Transponder-Schlüssel in eine Liste einzutragen, um diese bei Verlust in die Blockierliste [25] übernehmen zu können.

5.2.1.1 Gerätegruppen

Es gibt 32 auswählbare Gerätegruppen, G0 bis G31.

In einer Gerätegruppe werden PITreader zusammengefasst. Ein Anwender (ein Transponder-Schlüssel) 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 [38].

Pro Gerätegruppe kann auf einem Transponder-Schlüssel 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 [54].

Im PITreader ist immer nur eine Berechtigung gültig. Zusätzliche Berechtigungen, die auf dem Transponder-Schlüssel 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-Schlüssel können die Berechtigungen für die Gerätegruppen 0 ... 31 gespeichert werden und zusätzlich für maximal 48 weitere Gerätegruppen im Bereich 32 ... 9999. Siehe Anwenderdaten [20].

5.2.2 Extern

Im Authentifizierungsmodus Extern kann sich ein Anwender durch das Einbringen eines Transponder-Schlüssels in den Lesebereich des PITreader am verbundenen Steuerungssystem oder auf dem HMI authentifizieren.
Es stehen folgende Verbindungsmöglichkeiten zur Verfügung:

Externe Authentifizierung (Modbus/TCP)

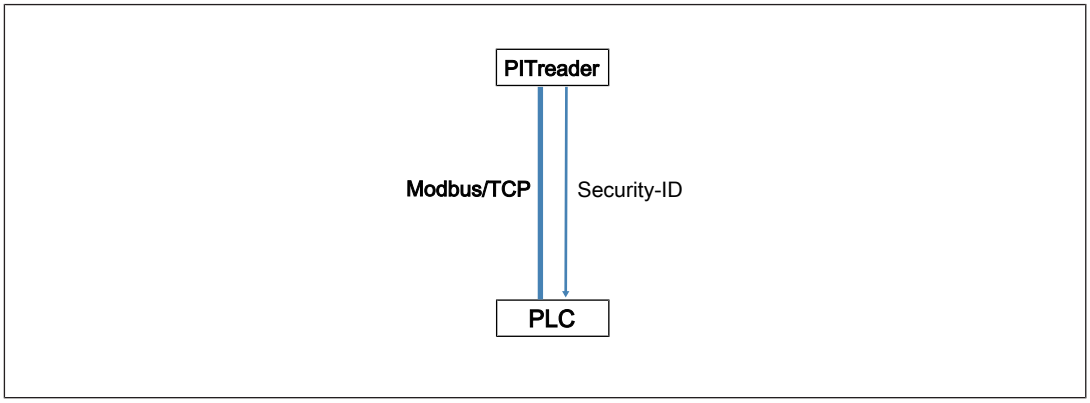


Abb.: Externe Authentifizierung (Modbus/TCP)

Der PITreader stellt die Daten des Transponder-Schlüssels über die Modbus/TCP-Verbindung zur Verfügung.
Mithilfe einer Berechtigungsdatenbank (auf der PLC) und der Daten des Transponder-Schlüssels (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 gestecktem Transponder-Schlüssel rot.
Zur Anzeige des extern ermittelten Authentifizierungszustands über die Geräte-LED können Farbe und Blinkmodus über die Modbus/TCP-Schnittstelle überschrieben werden (siehe auch Modbus/TCP [26]).

INFO

Im Authentifizierungsmodus Extern über Modbus/TCP kann **keine** sichere Auswerteeinheit (z. B. PIT m4SEU) eingesetzt werden.

Externe Authentifizierung (REST API)

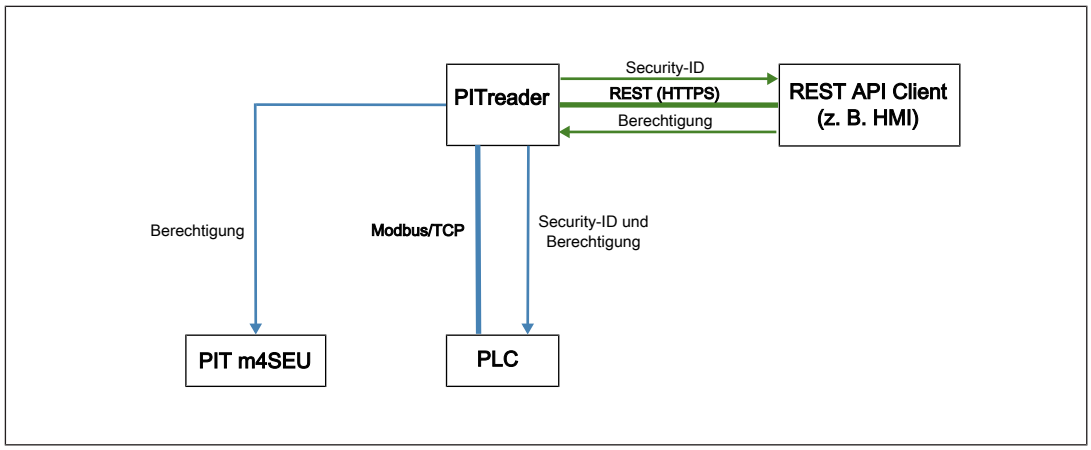


Abb.: Externe Authentifizierung (REST API)

Mithilfe einer Berechtigungsdatenbank (auf dem HMI) und der Daten des Transponder-Schlüssels (z. B. die Security-ID) kann die Berechtigung für den Anwender ermittelt werden.
Die Authentifizierung erfolgt im PITreader und der Authentifizierungsstatus wird über die Geräte-LED angezeigt.

Externe Authentifizierung (OPC UA)

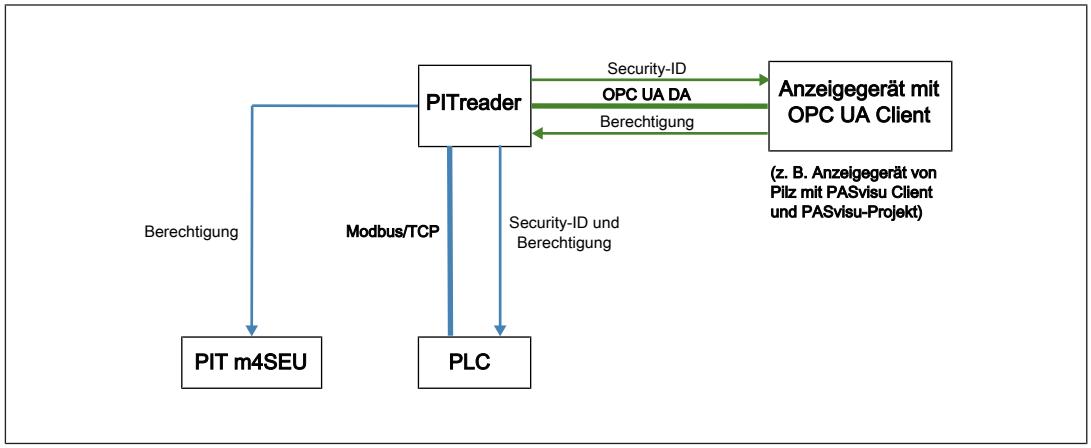


Abb.: Externe Authentifizierung (OPC UA)

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

Die Authentifizierung erfolgt im PITreader und der Authentifizierungsstatus wird über die Geräte-LED angezeigt.

5.3 Authentifizierungstypen "Basis" und "Einzelauthentifizierung"

Der PITreader unterstützt folgende Authentifizierungstypen:

- Basis

  Der Authentifizierungstyp "Basis" umfasst die Authentifizierungsmodi "Transponder-Daten" und "Extern" mit allen ihren Funktionen und Möglichkeiten (siehe Authentifizierungsmodi [📖 14]).

- 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-Schlüssel an einem Gerät anmelden, um eine Authentifizierungssperre für alle anderen Transponder-Schlüssel zu aktivieren. Die Authentifizierungssperre bleibt aktiviert, bis die Abmeldung mit demselben Transponder-Schlüssel erfolgt. Bei aktiver Authentifizierungssperre leuchtet die Geräte-LED rot.

  Authentifizierungssperre aktivieren:

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

  Authentifizierungssperre deaktivieren:

  Die Authentifizierungssperre wird erst durch die Abmeldung mit demselben Transponder-Schlüssel deaktiviert. Für die Abmeldung muss derselbe Transponder-Schlüssel erneut gesteckt 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.

5.4 Transponder-Schlüssel

Die Transponder-Schlüssel sind in folgenden Varianten verfügbar (siehe auch Bestelldaten [📖 56]):

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

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

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

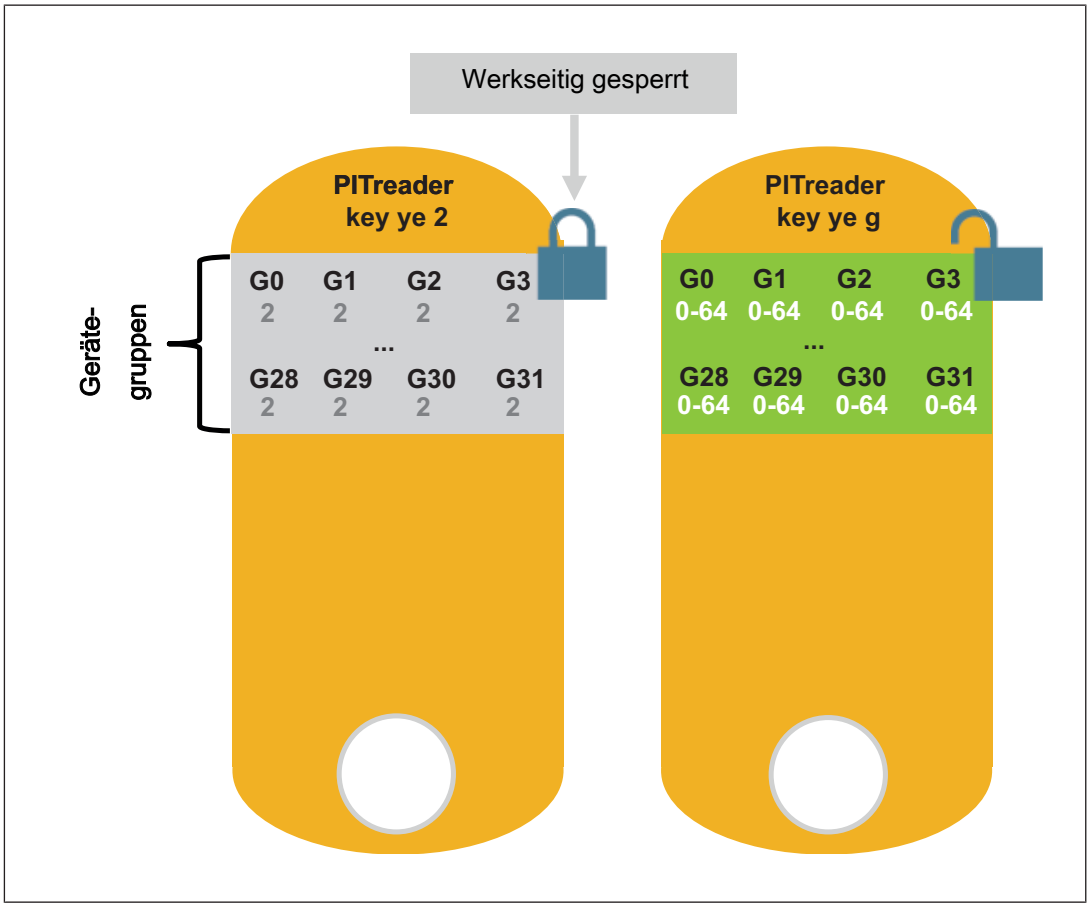


Abb.: Beispiel "PITreader key ye 2" und "PITreader key ye g"

WICHTIG

Achten Sie beim Stecken des Transponder-Schlüssels in den PITreader darauf, dass der Transponder-Schlüssel spürbar einrastet.

5.4.1 Seriennummer der Transponder-Schlüssel

Die Seriennummer der Transponder-Schlüssel 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 Security-ID (SID) der Transponder-Schlüssel

Alle Transponder-Schlüssel sind werkseitig mit einer Security-ID (SID) vorprogrammiert. Die Security-ID eines Transponder-Schlüssels ist nicht änderbar. Bei der Security-ID eines Transponder-Schlüssels handelt es sich um eine eindeutige Kennung, die ausschließlich für diesen einen Transponder-Schlüssel gilt.

Die Security-ID dient zur eindeutigen Identifikation eines Transponder-Schlüssels am PITreader; d. h. mithilfe der Security-ID wird ein Transponder-Schlüssel beim PITreader authentifiziert. Die Berechtigungen, die für einen Transponder-Schlüssel 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 Transponder-Schlüssels in eine Blockierliste eingetragen wird, kann die Authentifizierung gesperrt werden (siehe Blockierliste verwenden [📖 42]).

5.5 Anwenderdaten

Auf den Transponder-Schlüsseln 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 [📖 22].

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

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 [📖 22]).
Wie Sie Anwenderdaten konfigurieren, ist hier beschrieben: Anwenderdaten konfigurieren [📖 43]

Die Werte der Parameter werden auf dem Transponder-Schlüssel gespeichert. Auf dem Transponder-Schlüssel 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, um so weniger Gerätegruppen sind möglich. In der Web-Anwendung wird die Auslastung des Speichers auf dem Transponder-Schlüssel 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-Schlüssel schreiben, ist hier beschrieben: Werte der Anwenderdaten bearbeiten [📖 41].

Die Anwenderdaten können über Modbus/TCP, über REST API oder über den OPC Server UA vom Transponder-Schlüssel 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-Schlüssel vorhanden sein, wird der Initialwert des Datentyps zurückgegeben.
Ist der Parameter auf dem Transponder-Schlüssel 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-Schlüsseln beschränkt werden.

Es gibt zwei verschiedene Codierungen:

- Basis-Codierung [24]
- OEM-Codierung [25]

Auf einem PITreader können die Kennungen für beide Codierungen gespeichert werden. Auf dem Transponder-Schlüssel kann nur die Kennung für eine der Codierungen gespeichert werden.

Die Wirkung der Codierungen ist gleich, aber sie unterscheiden sich darin, wie die Kennungen auf dem PITreader geändert und gelöscht werden und wie die Transponder-Schlüssel eingelernt werden.

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

Einlernen eines codierten Transponder-Schlüssels

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

INFO

Wenn ein (noch) nicht codierter Transponder-Schlüssel in den Lesebereich des PITreader eingebracht wird oder PITreader und Transponder-Schlüssel mit unterschiedlichen Kennungen codiert sind, wird der Transponder-Schlüssel nicht ausgelesen und der PITreader zeigt einen Fehler an (LED blinkt rot). In diesem Fall sind die Daten des Transponder-Schlüssels auch nicht über die Modbus/TCP-Verbindung auslesbar und es kann keine (externe) Authentifizierung des Transponder-Schlüssels stattfinden.

Schutz vor unbefugtem Auslesen eines codierten Transponder-Schlüssels

An einem nicht codierten PITreader funktionieren sowohl codierte, als auch nicht codierte Transponder-Schlüssel; d. h. die Daten eines codierten Transponder-Schlüssels können auch von einem nicht codierten PITreader ausgelesen werden. Um dies zu verhindern, kann ein codierter Transponder-Schlüssel zusätzlich so konfiguriert werden, dass das Auslesen auf identisch codierte PITreader beschränkt ist (siehe Transponder-Schlüssel auf identisch codierte PITreader beschränken [41]).

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 oder die REST API kann die Prüfsumme ausgelesen werden. Die Prüfsumme wird außerdem in der Web-Anwendung angezeigt (siehe Basis-Codierung setzen [📖 41] und OEM-Codierung setzen [📖 42]).

5.6.1 Basis-Codierung

Durch die Basis-Codierung können PITreader ausschließlich Transponder-Schlüssel erkennen, die mit der gleichen Basis-Kennung versehen sind oder ggf. mit einer OEM-Kennung (siehe OEM-Codierung [📖 25]).

Die Basis-Codierung kann z. B. genutzt werden, um eine „Unternehmenskennung“ zu codieren, dadurch werden nur noch intern codierte Transponder-Schlüssel erkannt.

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.

Die Basis-Codierung erfolgt durch die Konfiguration des PITreader mit einer Basis-Kennung (siehe Basis-Codierung setzen [📖 41]). Transponder-Schlüssel werden auf eine Basis-Kennung eingelernt, wenn an einem codierten PITreader Berechtigungen auf den Transponder-Schlüssel geschrieben werden (siehe Transponder-Schlüssel auf Basis-Codierung einlernen [📖 39]).

5.6.2 OEM-Codierung

Durch die OEM-Codierung kann im PITreader eine zweite Kennung zur Prüfung von Transponder-Schlüsseln hinterlegt werden. PITreader mit OEM-Codierung akzeptieren Transponder-Schlüssel, mit der gleichen OEM-Kennung oder mit der passenden Basis-Kennung (siehe Basis-Codierung [24]).

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

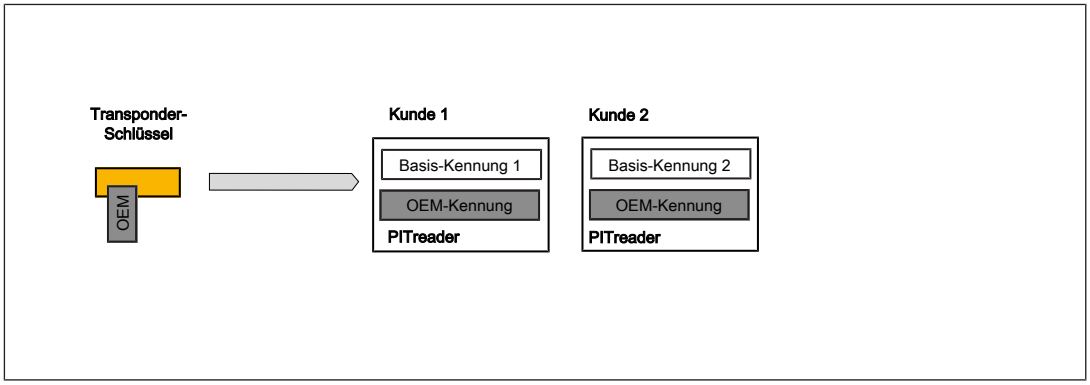


Abb.: OEM-Codierung

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 auch OEM-Codierung setzen [42].

Neue Transponder-Schlüssel mit der 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-Schlüssel auf OEM-Codierung einlernen [40].

5.7 Blockierliste

Sie können die Authentifizierung bestimmter Transponder-Schlüssel sperren. Ein in der Blockierliste enthaltener Transponder-Schlüssel kann sich nicht mehr am PITreader authentifizieren. Diese Funktion kann beispielsweise nützlich sein, wenn ein Anwender seinen Transponder-Schlüssel verloren hat. Somit kann verhindert werden, dass sich unbefugte Personen am PITreader authentifizieren.
Die Blockierliste kann in jedem Authentifizierungsmodus verwendet werden.
Siehe auch Blockierliste verwenden [42].

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 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.

5.9.1 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)

5.9.2 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)

Function Code	Funktion	
16	Write Multiple Registers	Der Client einer Verbindung schreibt auf mehrere Wort-Daten im Server der Verbindung, Datenlänge ≥ 1 Wort, (Daten senden nach 4x)

5.9.3 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 bitte 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 Transponder-Schlüssels)

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

Adresse	Inhalt
3x0001 … 3x0002	PITreader Bestellnummer (codiert) Bits 31 bis 24: Produktgruppe (00 = leer, 01 = G1) Bits 23 bis 20: Revision (00 = leer) Bits 19 bis 0: Produktnummer Beispiele: PITreader base unit (402255): 0x 00 0 6234F 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 [26])
3x0010	LED-Blinkmodus (siehe auch Steuerung der LED [26])
3x0011	Diagnose-Status (Alle Diagnosemeldungen werden einem Schweregrad zugeordnet, Schweregrad 3 = Störung, Schweregrad 8 = Warnung, Schweregrad 13 = Statusinformation)
3x0013 … 3x0016	PITreader Bestellnummer (ASCII)
3x0017	PITreader Revision (ASCII)
3x0019	SEU-Statusinformation (siehe auch Bedienungsanleitung PIT m4SEU, Kapitel 5.5) Standardwert wenn keine SEU angeschlossen ist: 0x00F0 (dezimal: 240)
3x0025 … 3x0028	Security-ID (Daten des Transponder-Schlüssels)
3x0029 … 3x0030	reserviert
3x0031 … 3x0032	Berechtigung (Codewort)
3x0033	Berechtigung (Ganzzahl, 0 bis 64)

Adresse	Inhalt
3x0034	Authentifizierungsstatus (0 = nicht authentifiziert, 1 = Transponder erfolgreich authentifiziert)
3x0035 … 3x0036	Bestellnummer (Transponder-Schlüssel)
3x0037 … 3x0038	Seriennummer (Transponder-Schlüssel) (siehe auch Seriennummer der Transponder-Schlüssel [20])
3x0039	reserviert
3x0040	reserviert
3x0059 … 3x0060	Gruppe 0
3x0061 … 3x0062	Gruppe 1
3x0063 … 3x0064	Gruppe 2
3x0065 … 3x0066	Gruppe 3
3x0067 … 3x0068	Gruppe 4
3x0069 … 3x0070	Gruppe 5
3x0071 … 3x0072	Gruppe 6
3x0073 … 3x0074	Gruppe 7
3x0075 … 3x0076	Gruppe 8
3x0077 … 3x0078	Gruppe 9
3x0079 … 3x0080	Gruppe 10
3x0081 … 3x0082	Gruppe 11
3x0083 … 3x0084	Gruppe 12
3x0085 … 3x0086	Gruppe 13
3x0087 … 3x0088	Gruppe 14
3x0089 … 3x0090	Gruppe 15
3x0091 … 3x0092	Gruppe 16
3x0093 … 3x0094	Gruppe 17
3x0095 … 3x0096	Gruppe 18
3x0097 … 3x0098	Gruppe 19
3x0099 … 3x0100	Gruppe 20
3x0101 … 3x0102	Gruppe 21
3x0103 … 3x0104	Gruppe 22
3x0105 … 3x0106	Gruppe 23
3x0107 … 3x0108	Gruppe 24
3x0109 … 3x0110	Gruppe 25
3x0111 … 3x0112	Gruppe 26
3x0113 … 3x0114	Gruppe 27
3x0115 … 3x0116	Gruppe 28
3x0117 … 3x0118	Gruppe 29

Adresse	Inhalt
3x0119 … 3x0120	Gruppe 30
3x0121 …3x0122	Gruppe 31
3x0159 … 3x0166	Prüfsumme der Basis-Codierung
3x0167 … 3x0174	Prüfsumme der OEM-Codierung
3x1000 … 3x1519	Anwenderdaten (siehe auch Info unten und Anwenderdaten [20])

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-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.

5.9.4 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 Register)	
Daten schreiben (Wort)	FC 06 (Write Single Register)	1 Wort
	FC 16 (Write Multiple Registers)	1 … 123 Worte

5.10 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-Schlüssel ausgelesen und beschrieben werden (siehe auch Kapitel Konfiguration [📖 36] und Firmware-Update [📖 47]).

5.11 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 Transponder-Schlüssels eingestellt werden, ab welcher der Ausgang eingeschaltet werden soll. Wenn die Berechtigung des Transponder-Schlüssels 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 "Basis" und "Einzelauthentifizierung" [📖 18]).

5.12 Verbindung der Basiseinheit mit einer sicheren Auswerteeinheit

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

6 Montage der Basiseinheit

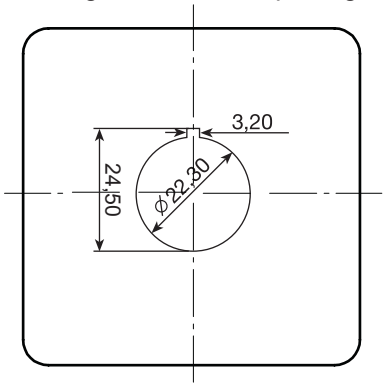
6.1 Allgemeine Hinweise zur Montage

WICHTIG

Beschädigung durch elektrostatische Entladung!

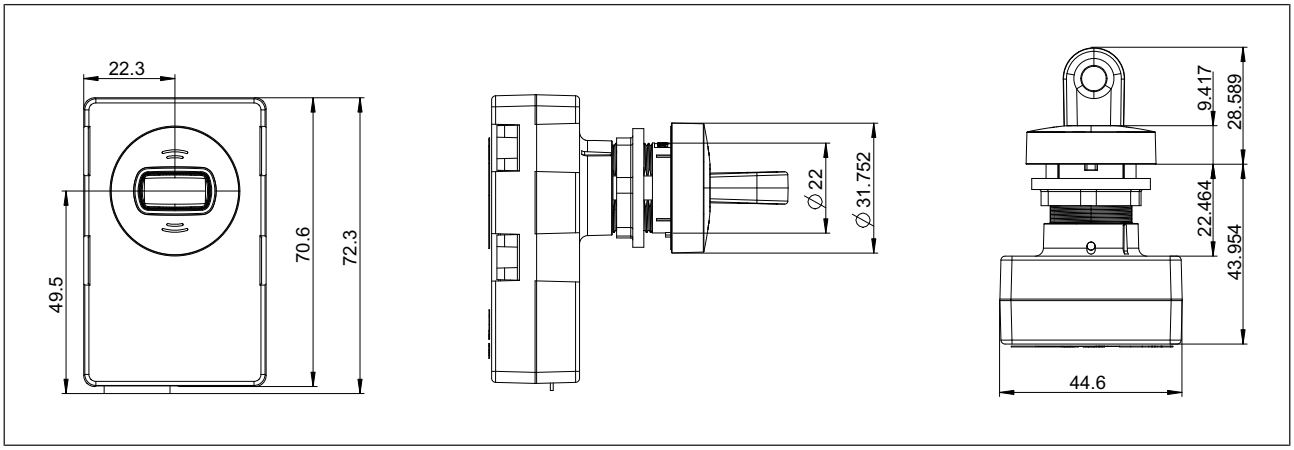
Durch elektrostatische Entladung können Bauteile beschädigt werden. Sorgen Sie für Entladung, bevor Sie das Produkt berühren, z. B. durch Berühren einer geerdeten, leitfähigen Fläche oder durch Tragen eines geerdeten Armbands.

- Montieren Sie das Gerät in die Frontplatte eines Schaltschranks oder in ein Bedienpult. Materialstärke:
  - nicht metallisch: 2 … 6 mm
  - Metall: 2 … 4 mm.
- 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 (zum Schutz gegen Verdrehen):



- Führen Sie den PITreader key adapter h (Bestell-Nr. 402 308) in die Einbauöffnung ein und befestigen Sie ihn von der anderen Seite mit der Kunstoffmutter (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 [📖 56]).
- Stecken Sie die PITreader base unit (Bestell-Nr. 402 255) auf den Hals des PITreader key adapter h (Bestell-Nr. 402 308) und drehen Sie sie im Uhrzeigersinn um 15°, bis sie einrastet.

6.2 Abmessungen in mm



7 Verdrahtung

7.1 Standalone

Gehen Sie wie folgt vor:

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

Gehen Sie wie folgt vor:

1. Verbinden Sie den PITreader mit einer sicheren Auswerteeinheit PIT m4SEU (siehe auch 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 Internet Explorer (IE), ab Version 10
- 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 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 [📖 37]).

   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 mit Basiseinheit [📖 9]).

   Nach 5 Fehlversuchen ist die Anmeldung für 5 Minuten gesperrt.

5. **Initialkennwort ändern**

   Die Meldung "Das Default-Kennwort wurde nicht geändert" wird angezeigt. Ändern Sie unter ***Anwender -> Kennwort ändern*** das Initialkennwort. Geben Sie ein sicheres Kennwort mit mindestens 8 Zeichen ein (Merkmale eines sicheren Kennworts siehe Security [📖 12]).

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.

8.3 Zertifikate verwalten

8.3.1 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 in den 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 PITreaders 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.

8.3.2 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 seinem 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)

8.4 Ortsbeschreibung

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

8.5 Datenprotokollierung mit personenbezogenen Daten

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

8.6 Gerätegruppe einstellen

Sie können in der Web-Anwendung unter ***Konfiguration -> Einstellungen -> Funktion*** dem PITreader eine Gerätegruppe zuweisen (siehe auch Gerätegruppen [📖 15]). 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 -> Funktion*** der entsprechende Name in der Auswahlliste angezeigt. Wenn kein Name eingetragen wurde, wird die Nummer der Gerätegruppe angezeigt.

8.7 Transponder-Schlüssel beschreiben/programmieren

8.7.1 Berechtigungen programmieren

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

WICHTIG

Beachten Sie:

- An einem gesperrten Transponder-Schlüssel 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-Schlüssel beim schreiben/programmieren der Berechtigungen automatisch auch auf die Basis-Codierung des PITreader eingelernt.

8.7.2 Gültigkeit des Transponder-Schlüssels konfigurieren

Sie können die Gültigkeit von Transponder-Schlüsseln auf einen bestimmten Zeitraum einschränken. Aktivieren Sie dafür unter ***Konfiguration -> Einstellungen -> Funktion*** 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 Transponder-Schlüssels eintragen.

8.7.3 Transponder-Schlüssel auf Basis-Codierung einlernen

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

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

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

8.7.4 Transponder-Schlüssel auf OEM-Codierung einlernen

Das Einlernen eines Transponder-Schlüssels auf die OEM-Codierung geschieht genau so, wie das Einlernen auf die Basis-Codierung, siehe Transponder-Schlüssel auf Basis-Codierung einlernen [📖 39]. Der Trick ist, dass die OEM-Kennung anstelle der Basis-Kennung eingetragen wird.

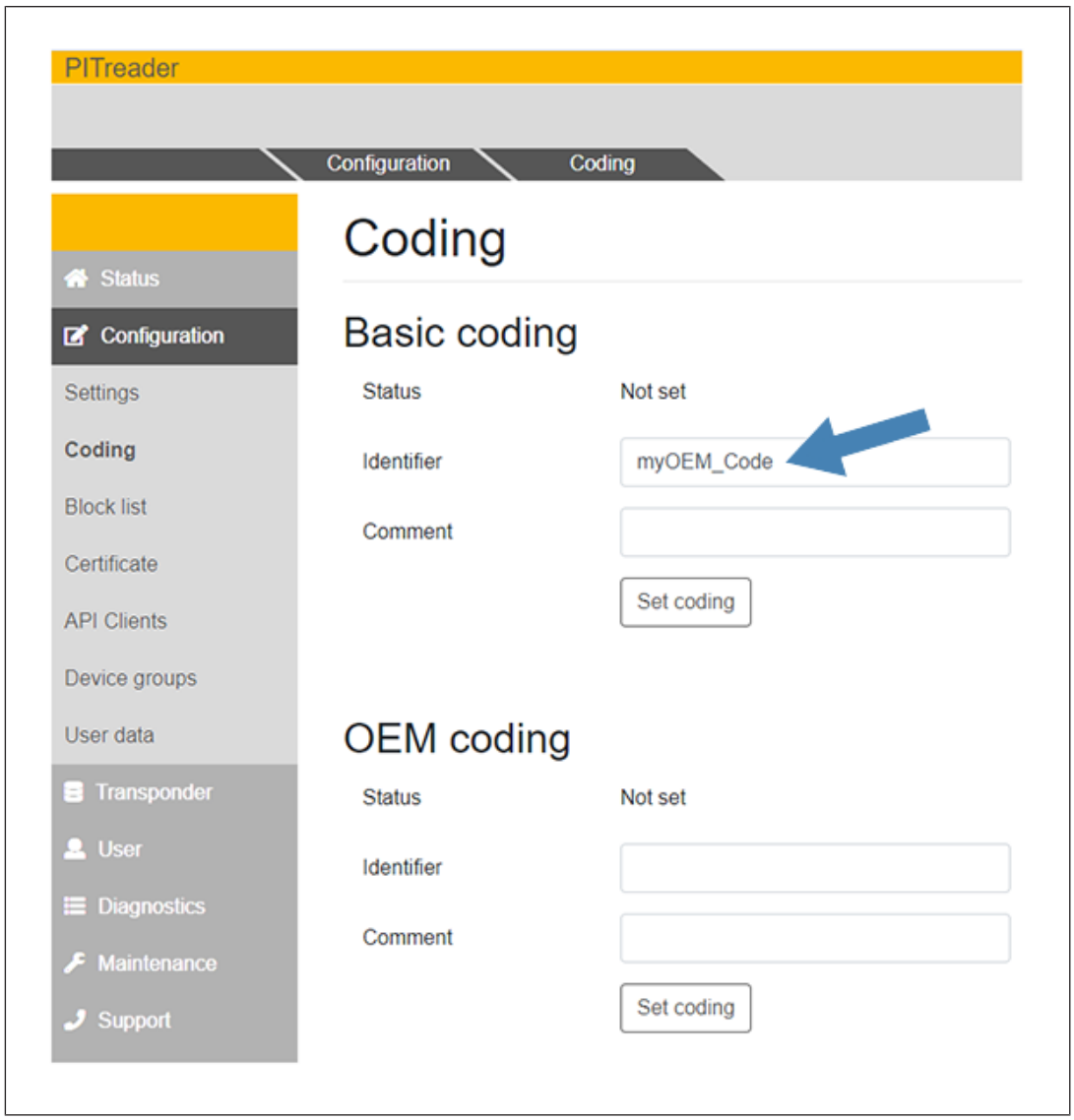


Abb.: Transponder-Schlüssel auf OEM-Codierung einlernen

Wenn Sie als Maschinenhersteller Transponder-Schlüssel für Service-Mitarbeiter codieren möchten, verwenden Sie dafür idealerweise einen PITreader, der nur diesem Zweck dient.

Auf diese Weise ist sichergestellt, dass neue Transponder-Schlüssel mit der OEM-Kennung nur von einer Person erstellt werden können, die die OEM-Kennung kennt oder die einen speziell für diesen Zweck konfigurierten PITreader verwendet.

8.7.5 Transponder-Schlüssel auf identisch codierte PITreader beschränken

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

Wenn Sie codierte Transponder-Schlüssel 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***.

8.7.6 Werte der Anwenderdaten bearbeiten

Mit der Web-Anwendung kann angezeigt werden, welche Werte die Parameter auf dem Transponder-Schlüssel haben. Die Werte können geändert 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 [📖 43]). Sollten auf dem Transponder-Schlüssel mehr Parameter vorhanden sein, so werden diese ignoriert. Sollten auf dem Transponder-Schlüssel weniger Parameter vorhanden sein, so wird für die fehlenden Parameter der Initialwert des Datentyps angezeigt.
  Beim Speichern der Anwenderdaten auf dem Transponder-Schlüssel, 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-Schlüssel 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.

8.8 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 [📖 23].

8.9 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.

Alle PITreader-Geräte, die Sie an Ihre Kunden ausliefern, müssen Sie ebenfalls mit dieser OEM-Kennung codieren.

Siehe auch Codierung [📖 23].

8.10 Blockierliste verwenden

Sie können die Authentifizierung bestimmter Transponder-Schlüssel sperren, in dem Sie die Security-IDs dieser Schlüssel (und optional einen Kommentar) unter ***Konfiguration -> 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.

Siehe auch Blockierliste [📖 25].

8.11 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.

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.

8.12 API-Clients

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

8.13 Konfiguration speichern 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 Blockierliste, die Namen der Gerätegruppen und die Anwenderdaten-Konfiguration. TLS-Zertifikate, OPC UA-Zertifikate und Codierungskennungen sind nicht in der Sicherung enthalten und können nicht wiederhergestellt werden.

8.14 Auf Werkseinstellungen zurücksetzen

Die PITreader Basiseinheit 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.

Kurzschluss an den Klemmen TxD/RxD

Es werden die Konfigurationsdaten (inklusive Codierung) und die Blockierliste zurückgesetzt.
Gehen Sie wie folgt vor:

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

WICHTIG

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

4. Wenn das Zurücksetzen auf Werkseinstellungen erfolgreich durchgeführt wurde, leuchtet die LED grün.
5. Entfernen Sie den Kurzschluss
   Die LED leuchtet nicht mehr gelb bzw. grün und der Boot-Vorgang wird fortgesetzt.

INFO

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

In der Web-Anwendung

In der Web-Anwendung kann ausgewählt werden, welche Daten zurückgesetzt werden sollen.

Folgende Daten können in der Web-Anwendung auf Werkseinstellungen zurückgesetzt werden:

- Gerätekonfiguration
- Diagnoseprotokoll
- Transponder-Blockierliste
- Namen der Gerätegruppen
- Konfiguration der Anwenderdaten

Gehen Sie wie folgt vor:

Klicken Sie unter ***Wartung -> Werksreset*** auf ***Auf Werkseinstellungen zurücksetzen*** und wählen Sie die Daten, die Sie zurücksetzen möchten.

9 Firmware-Update

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

Ein Update-Paket kann im Download-Bereich zum Gerät auf der Pilz Internetseite heruntergeladen werden. Es gibt zwei unterschiedliche Dateiendungen, .fw und .fwu. In der Web-Anwendung wird angezeigt, welches Update-Paket mit welcher Dateiendung für Ihr Gerät verwendet werden soll.

Es ist nicht möglich, eine ältere Firmware-Version einzuspielen, als momentan im PITreader aktiv ist.

WICHTIG

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

10 Betrieb

10.1 LED-Anzeige

Legende

 LED ein

 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 gesteckten Transponder-Schlüssel gesetzt
blau		Gerät ist betriebsbereit, es wurde kein Transponder-Schlüssel gesteckt
grün		Transponder-Schlüssel wurde als gültig erkannt
rot		Transponder-Schlüssel wurde als nicht gültig erkannt mögliche Gründe: ▸ Bei gestecktem Transponder-Schlüssel: Die Authentifizierung wird verweigert (z. B. Berechtigung = 0). ▸ Bei nicht gestecktem Transponder-Schlüssel: 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***
rot		Störung (z. B. Hardware-Fehler, Konfigurationsfehler, ungültiger oder nicht codierter Transponder-Schlüssel, …). Mögliche Abhilfen bei einem Konfigurationsfehler und 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 [📖 45].

10.2 PITreader sicher außer Betrieb setzen

Vor der Entsorgung muss der PITreader sicher außer Betrieb gesetzt werden. Dazu müssen alle Daten vom Gerät gelöscht werden.

Gehen Sie wie folgt vor:

- Setzen Sie die Konfiguration auf Werkseinstellungen zurück wie im Kapitel Auf Werkseinstellungen zurücksetzen [📖 45] beschrieben.

10.3 Diagnose

Die Diagnose des PITreader erfolgt über

- die LED
- die Diagnoseliste und das Diagnoseprotokoll

Sie können die Diagnoseliste und das Diagnoseprotokoll in der Web-Anwendung unter ***Diagnose*** auslesen.
Unter ***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.

11 Technische Daten

Allgemein	
Zertifizierungen	**CE, FCC, IC, UL/cUL**
Funktionsweise Sensor	**Transponder**
Transponder	
Energieversorgung des Transponders	**passiv (batterielos)**
Frequenzband	**13,24 - 13,88 MHz**
Max. Sendeleistung	**170 mW**
Elektrische Daten	
Versorgungsspannung	
Spannung	**24 V**
Art	**DC**
Art des Netzteils	**SELV/PELV**
Spannungstoleranz	**-15 %/+20 %**
Leistung des externen Netzteils (DC)	**4 W**
Externe Gerätesicherung F1	**4 A, Sicherungsautomat 24 V DC, Charakteristik B/C**
Statusanzeige	**LED**
Verlustleistung	**2,5 W**
Eingänge	
Signalpegel bei "1"	**15 - 30 V DC**
Eingangsstrombereich	**4 mA**
Galvanische Trennung	**nein**
Halbleiterausgänge	
Gesamtleistung ext. Last, Halbleiter	**1,2 W**
Anzahl	**1**
Schaltstrom pro Ausgang	**50 mA**
Galvanische Trennung	**nein**
Kurzschlussfest	**ja**
Ethernet-Schnittstelle	
Anzahl	**1**
IP-Adresse Werkseinstellung	**192.168.0.12**
Anschlussart	**RJ45**
Übertragungsrate	**10/100 Mbit/s**
Zeiten	
Überbrückung bei Spannungseinbrüchen der Versorgungsspannung	**10 ms**
Umweltdaten	
Umgebungstemperatur	
nach Norm	**EN 60068-2-14**
Temperaturbereich	**-20 - 55 °C**

Umweltdaten	
Lagertemperatur	
nach Norm	**EN 60068-2-1/-2**
Temperaturbereich	**-25 - 70 °C**
Feuchtebeanspruchung	
nach Norm	**EN 60068-2-78**
Feuchtigkeit	**93 % r. F. bei 40 °C**
Max. Betriebshöhe über NN	**2000 m**
EMV	**EN 301489-1 V2.1.1**
Schwingungen	
nach Norm	**EN 60068-2-6**
Frequenz	**5 - 8,4 Hz, 8,4 - 150 Hz**
Amplitude	**3,5 mm**
Beschleunigung	**max. 1g**
Schockbeanspruchung	
nach Norm	**EN 60068-2-27**
Beschleunigung	**15g**
Dauer	**11 ms**
Schutzart	
nach Norm	**EN 60529**
Gehäuse	**IP20**
Front	**IP65/IP67**
Einbauraum (z. B. Schaltschrank)	**≥ IP54**
Mechanische Daten	
Einbaulage	**beliebig**
Material	
Unterseite	**PC**
Front	**PC**
Anschlussart	**Federkraftklemme steckbar**
Befestigungsart	**steckbar**
Max. Anzugsdrehmoment Befestigungsschrauben	**1,3 - 2,1 Nm**
Leiterquerschnitt bei Federkraftklemmen: flexibel mit/ ohne Aderendhülse	**0,2 - 1,5 mm², 24 - 14 AWG**
Federkraftklemmen: Klemmstellen pro Anschluss	**1**
Abisolierlänge bei Federkraftklemmen	**8 mm**
Abmessungen	
Höhe	**54 mm**
Breite	**72 mm**
Tiefe	**45 mm**
Gewicht	**47 g**

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

12 Ergänzende Daten

12.1 Funkzulassungen

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.

12.2 Netzwerkdaten

Proto-koll	Rich-tung	Trans-port-protokoll	Port-Nr.	Deakti-vierbar	Beschreibung
HTTP	in	TCP	1 … 65535 Default: 80	nein	**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	**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**

12.3 Übersicht der Berechtigungen

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

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

13 Bestelldaten

13.1 Authentifizierungssystem

Produkttyp	Merkmale	Bestell-Nr.
PITreader base unit	RFID-Authentifizierungssystem, Basiseinheit. Notwendiges Zubehör: PITreader key adapter	402 255
PITreader S base unit	RFID-Authentifizierungssystem, Basiseinheit mit erweitertem Funktionsumfang. Notwendiges Zubehör: PITreader key adapter	402 256
PITreader key adapter h	1x PITreader Schlüsselaufnahme horizontal + 1x Mutter für PITreader base unit	402 308

13.2 Transponder-Schlüssel

Produkttyp	Merkmale	Bestell-Nr.
PITreader key ye 1	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1 Farbe: gelb Material: Kunststoff	402 261
PITreader key ye 2	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1 und 2 Farbe: gelb Material: Kunststoff	402 262
PITreader key ye 3	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1, 2 und 3 Farbe: gelb Material: Kunststoff	402 263
PITreader key ye 4	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1, 2, 3 und 4 Farbe: gelb Material: Kunststoff	402 264
PITreader key ye 5	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1, 2, 3, 4 und 5 Farbe: gelb Material: Kunststoff	402 265
PITreader key ye 5 service	Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigung für Betriebsart 1, 2, 3, 4 und 5 (Service) Farbe: gelb Material: Kunststoff	402 269
PITreader key ye g	Generischer Transponder-Schlüssel für Authentifizierungssystem PITreader, Berechtigungen frei konfigurierbar Farbe: gelb Material: Kunststoff	402 260

13.3 Zubehör

Produkttyp	Merkmale	Bestell-Nr.
PIT es wrench	Montageschlüssel für PIT es Taster	400 222

14 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: Norbert Fröhlich, Pilz GmbH & Co. KG, Felix-Wankel-Str. 2, 73760 Ostfildern, Deutschland

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 21 60880878-216
Japan
+81 45 471-2281
Südkorea
+82 31 778 3300

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 462203
Irland
+353 21 4804983
Italien, Malta
+39 0362 1826711
Niederlande
+31 347 320477
Österreich
+43 1 7986263-0
Schweiz
+41 62 88979-32
Skandinavien
+45 74436332
Spanien
+34 938497433
Türkei
+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.

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, Telefax: +49 711 3409-133, E-Mail: info@pilz.de, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY

1004806-DE-06, 2021-03 Printed in Germany