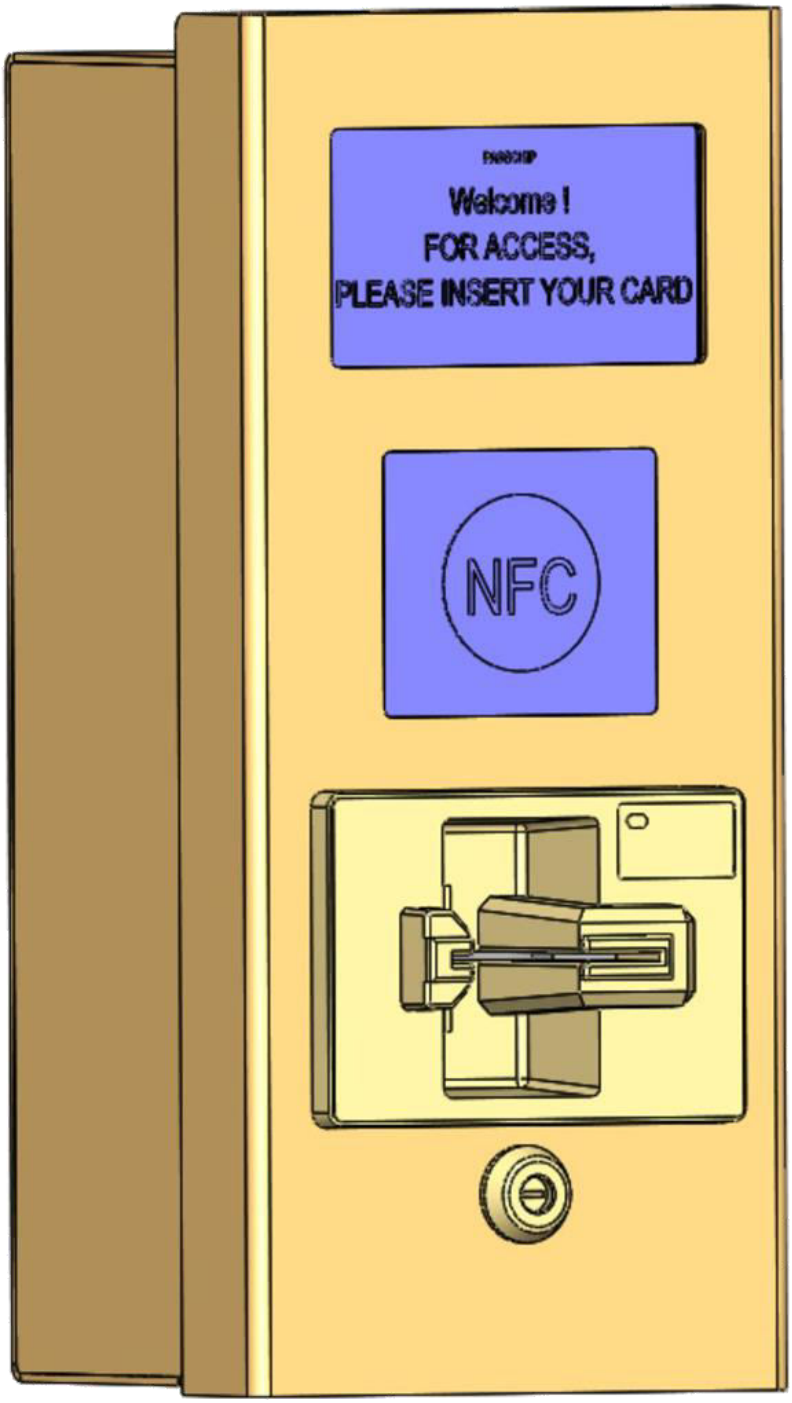


PASSCHIP®

Geräte zum Lesen und Auswerten von Bankkartenchips integrierbar in Zutrittskontrollsysteme mit Kommunikationsprotokoll Wiegand

PASSCHIP TECHNOLOGY SRL

a. **PRODUKT: Gerät zum Lesen und Auswerten von Bankkartenchips integrierbar in Zutrittskontrollsysteme mit Wiegand Kommunikationsprotokoll**

b. **TECHNISCHER BEREICH ABGEDECKT VON DER PASSCHIP TECHNOLOGIE**: die Technologie bezieht sich auf die elektronische Sicherheitssysteme, insbesondere die Zutrittskontrollsysteme. Es ist in erster Linie für den Bankbereich, für die Zugangskontrolle zu sehr wichtigen oder Hochsicherheitsbereichen bestimmt.

c. **STAND DER TECHNIK:**

Die Zutrittskontrollsysteme erlauben den selektiven Zugriff auf einen bestimmten Bereich oder eine Ressource. Die Auswahl erfolgt auf der Grundlage der vorgelegten Authentifizierungselemente, der "Zugang" bedeutet: Eingang, Verbrauch oder zur Verwendungserlaubnis. Der Zugriffserlaubniss auf eine Ressource wird "Ermächtigung" genannt.

Die traditionelle Zutrittskontrollsysteme bestehen aus den folgenden Grundelementen:

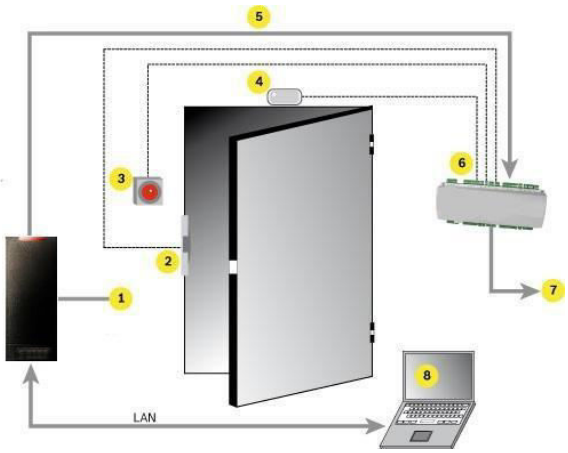
-Authentifizierungselemente: Passwörter, Karte, biometrische Elemente oder eine Kombination von zwei oder mehr solcher Elemente

-Leselemente: Tastaturen, berührungslose oder Kontaktleser (Magnetstreifen oder Computer-Chip) oder Kombinationen von Tastaturen und Leser

-Auswerteeinheit: Einheit für die Analyse Computer mit Datenbank oder Zusammenbau der beiden Elemente

-Zugangsbeschränkungselement: mechanische Verriegelung, elektrische Sperre, rotierendes Zugangselement des Types Drehkreuz

Schematische Darstellung der Funktionsweise von den Zugriffssystemen:



Legende:

1 = Leser; 2 = Sperre; 3 = Exit Taste; 4 = Kontakt zur Statusbestätigung der Tür;
5 = Kommunikation zwischen dem Leser und dem Zugangsmodul; 6 = örtliche Evaluationseinheit;
7 = Zentraleinheit zur Auswertung/Computer;
8 = Computer mit Parametrierungs- und Verwaltungssoft (OPTIONAL JE NACH DER LESERSART)

Auf den Karten sind Elemente gespeichert, die die Personen in dem System identifizieren. Alle Entscheidungen werden dann von den Authentifizierungselementen (Zahlen, Koden, Serien, etc.) ausgehend getroffen, in den meisten Fällen wird ein Code zu einer Person zugeordnet.

Beim Lesen der Karten von dem Leser, sendet dieser die Benutzerinformationen zu der Auswerteeinheit, welche die gelesene Information mit der Liste vergleicht, und die Entscheidung den Zugang zu erlauben oder verweigern trifft und das Ergebnis der Entscheidung der Geschichte vom internen Ereignisse übermittelt, die durch den Systemadministrator eingesehen werden können. Wenn die von der Karte gelesene Information in der Datenbank gefunden wird, aktiviert die Auswerteeinheit automatisch ein Relais das elektrische Öffnungsmechanismus, andernfalls wird dieses Relais nicht betrieben. Die meisten Zugangsleser bieten eine primäre Information über den Zugriff und eine grüne LED leuchtt bei der Zulassung bzw. eine rote LED bei der Verweigerung der Zulassung.

DIE NÄCHSTGEEGENE LÖSUNGEN FÜR DIE VORGESCHLAGENE AUSRÜSTUNG :

Die aktuellen Lösungen für Zutrittskontrolle gegründet auf Bankkartenleser sind die folgenden:

- Magnetband Leser von Karten, die die Informationen auf dem Magnetband werten und den Zugang je nachdem zulassen
- Leser, der alle Arten von Chips von Karten (Smart Card) erkennen und den Zugriff in Abhängigkeit von der Anwesenheit oder Abwesenheit von diesem Chip zulassen.

d. TECHNISCHE PROBLEME, DIE WIR MIT HILFE DER PASSCHIP PLATFORM LÖSEN WOLLEN: „Gerät zum Lesen und Auswerten von Bankkartenchips integrierbar in Zutrittskontrollsysteme mit Wiegand Kommunikationsprotokoll”:

- Autorisierung auf Grund von Informationen in Chips von Smartcard Bankkarten enthalten (nicht durch Erkennung des Chips)

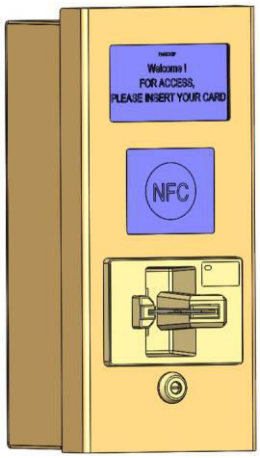
- Möglichkeit, die Arten von Karten zu wählen, die Zugang haben können, je nach Kartenherausgeber (Beispiel: Visa, Mastercard, American Express, etc.).

- Interaktion mit den Kartennutzern / -inhaber durchTextnachrichten und Symbole in jeder zu Zeit bekannten Sprache der Welt

- Geschichte von interne Ereignissen mit hoher Kapazität nutzen und Aufzeichnung von Fingerabdrücken für alle Ereignisse im System

- Integration mit jeder Art von Zugriffskontrolle unter Verwendung bekannter Kommunikationsprotokolle: Wiegand (am meisten verwendet), RS485, Datumsuhr, Ethernet.

e. PRODUKTBILD:



f. VORTEILE VON PASSCHIP IM VERGLEICH ZU DEM AKTUELLEN STAND DER TECHNIK:

1. Autorisierung auf Grund der Informationen in den Chips von Smartcard Bankkarten (nicht durch ihre Anerkennung) hat den großen Vorteil der Lektüre von Chipkarten. Die Lesensart der Chip von Bankkarten ist eine viel sicherere Alternative gegen unbefugtes Lesen und das Klonen von Karten im Vergleich zum Leseverfahren von Magnetstreifenkarten.

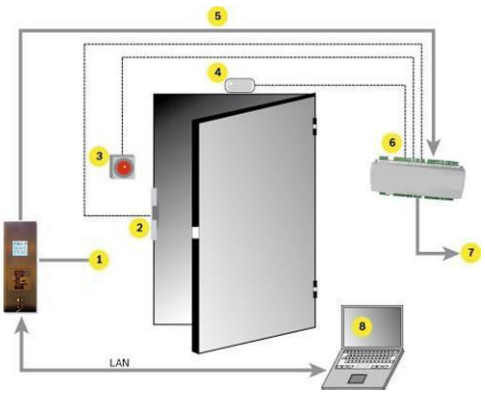
   Zugangswahl wird nach einem oder mehreren Kriterien, je nach Applikation, gemacht:

   * Vor- / Nachname geschrieben auf Bankkarten (Sie können schwarze Listen definieren)
   * Nummer der Bankkarte
   * Art der Kreditkarte (Visa, Visa Electron, Visa Business, Visa Gold, Maestro ....)
   * Bank (nur Kunden der entprechenden Bank werden Zugang haben)
   *Ablaufdatum

2. Interaktion mit den Kartennutzern / -inhabern durch Textnachrichten und Symbole in jeder in diesem Moment bekannten Sprache in der Welt ist ein wesentlicher Fortschritt, um das Gerät in jedem Land der Welt zu verwenden; die derzeitig ähnlichen Systeme sind auf Textnachrichten mit lateinische Schriftzeichen beschränkt. Ein weiterer Vorteil ist, dass die Geräte gleichzeitig Textnachrichten in mehreren Sprachen anzeigen können; die bestehende Begrenzung ist durch die Bildschirmgröße und der Art der verwendeten Zeichen gegeben.
3. Verwendung von Informationen in der internen Geschichtenspeicher von Hochleistungs- zusammen mit spezifischen Zeitstempeln (Datum / Zeit) ist ein großer Vorteil im Vergleich zu ähnlichen bestehenden Anlagen, die aktuellen Ereignisse übertragen, um diese in der externen Evaluationseinheiten oder Datenbank von Computern zu speichern.
4. Integration mit jeder Art von Auswertung für Zugriffskontrolle mit bekannten Kommunikationsprotokollen stellt einen großen Vorteil im Vergleich zu ähnlichen bestehenden Anlagen, die unabhängig arbeiten oder die Integration mit anderen Sicherheits-Ausrüstung über Standardprotokolle: Wiegand, RS232, Clock Daten, Ethernet nicht ermöglichen. Dieses Gerät ermöglicht es, jede Zutrittskontrolle, unabhängig von Generation mit dem Wiegand-Protokoll zu integrieren.

g. ABBILDUNGEN, ZEICHNUNGEN

1. Schematische Darstellung der Bedienung von der Ausrüstung zum Lesen und Auswertung des Bankkartenhips integrierbar in Zutrittskontrollsysteme mit Wiegand Kommunikationsprotokoll:
2.



Legende:

1 = Ausrüstung zum lesen von Bankkarten; 2 = elektrische Sperre; 3 = Exit-Taste; 4 = Kontakt zur Statusbestätigung der Tür;
5 = Kommunikation zwischen dem Leser und dem Evalationsmodul;
6 = örtliche Evaluationseinheit; 7 = Zentraleinheit zur Auswertung/Computer; 8 = Computer mit Parametrierungs- und Verwaltungssoft

Terminologie:

ID = Chip-Code-Liste, spezifisch für jeden Emittenten von Kreditkarten (Beispiel: Visa, MasterCard, American Express, etc.)

BLK = schwarze Liste: Liste der Karten, die aus Sicherheitsgründen beim Lesen laut Systemadministrator abgelehnt werden können

LOG = innere Geschichte der Ereignisse

NTP = Network Time Protocol (wird verwendet, um Datum und Uhrzeit zwischen zwei Geräten / Computern zu synchronisieren)

DNS = Domain Name System (wird verwendet, um Vorrichtungen in einem Kommunikationsnetz zuadressieren) LAN = Local Area Network

Betrieb der Geräte stützt sich auf der Verbindung von elektronischen Komponenten und der Interaktion mit geeigneter Software, entwickelt zur Ausführung von logischen Sequenzen, die in dem Flussdiagramm der Betrieb des Gerätes beschrieben sind, wie folgt:

Im Standby vor das -Einstecken der Karte, leuchtet das System mit grünem Licht , auf dem LCD Display erscheint die Anzeige die: **FÜR ZUGANG STECKEN SIE DIE KARTE EIN**

Wenn vollständige Einführung der Karte erkannt wird, wird der Verriegelungsmechanismus für die Karte betätigt, das Licht blinkt igrün, es beginnt das Lesen der Chipkarte und wird die Nachricht: **KARTELESEN** angezeigt

Das Lesen der Karte kann 4 mögliche Ergebnisse haben:

- Zugang gestattet – Karten-Typ ist SmartCard
- Lesefehler
    - Kartentyp ist nicht SmartCard – Beispiel: Karte ausgestellt durch einen Dienstleister für Transport oder Kommunikation oder Karte für normale Zugangskontrolle-
    - die Karte wurde (Zwangs-) entfernt bevor sie gelesen werden konnte
- Karte abgelehnt – Kartentyp ist SmartCard und:
    - Abgelaufene Karte – Karten-Typ ist SmartCard Karten, die im aktuellen Monat ablaufen gelten nicht als abgelaufen

Nach dem Lesen der Karte leuchtet das grüne Led und die Meldung :**ZIEHEN SIE DIE KARTE AUS**

wird angezeigt

Wenn 1 Minute nach Anzeige der obigen Meldung und die Karte nicht ausgezogen wurde, startet das rote Licht zu blinken gehen, es wird das Zutrittskontrollsystem benachrichtigt mit Nachricht "4", zeigt es die folgende Meldung: **VERGESSENE KARTE; RUFEN SIE……AN** und warten Extraktion
Karte

Nach dem Ausziehen der Karte, geht es zurück zu der Phase: **FÜR ZUGANG STECKEN SIE DIE KARTE EIN**, ohne das Lesergebniss in Betract zu ziehen.

Wenn die Karte binnen 1 Minute nach der Anzeige **ZIEHEN SIE DIE KARTE AUS** ausgezogen wurde, wird es zu der weiteren Phase entsprechend dem Leseergebnis gegangen(für 2 Sekunden), und dann geht es zurück zu der ursprünglichen Phase **FÜR ZUGANG STECKEN SIE DIE KARTE EIN**.

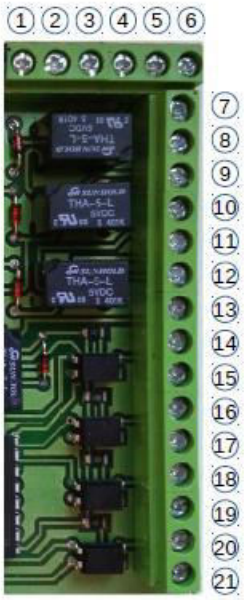
- Zugang gestattet: das grüne LED leuchtet, der Summer wird gestellt, um einen kurzen Ton (1,5 KHz - 160ms) zu produzieren, es wird die Nachricht "1" an die Zutrittskontrolle gesendet, und folgende Mitteilung angezeigt: **ZUGANG GESTATTET**

- Lesefehler: das rote LED leuchtet, der Summer wird gestellt, um einen kurzen Ton (2.5 KHz – 2 Sek) zu produzieren, es wird die Nachricht "0" an die Zutrittskontrolle gesendet, und folgende Mitteilung angezeigt: **LESEFEHLER**

- Karte abgelehnt: das rote LED leuchtet, der Summer wird gestellt, um einen kurzen Ton (2.5 KHz – 2 Sek) zu produzieren, es wird die Nachricht "2" an die Zutrittskontrolle gesendet, und folgende Mitteilung angezeigt: **KARTE ABGELEHNT**

- Karte abgelaufen: das rote LED leuchtet, der Summer wird gestellt, um einen kurzen Ton (2.5 KHz – 2 Sek) zu produzieren, es wird die Nachricht "3" an die Zutrittskontrolle gesendet, und folgende Mitteilung angezeigt: **KARTE ABGELAUFEN**

Shield pinout:



PIN	Description
1	Wiegand Data0
2	Wiegand Data1
3	Wiegand GND
4	INT BAT GND
5	INT BAT +5V
6	Not Connected
7	Door Relay NO
8	Door Relay NC
9	Door Relay COM
10	Fault Relay NO
11	Fault Relay NC
12	Fault Relay COM
13	Not Connected
14	GND
15	Inactive (Fire) (NO)
16	GND
17	PIR (NC)
18	GND
19	Exit Button (NO)
20	GND
21	CM (NC)
22	- 12V
23	+12V

Cable

Position	Description	Color
R1	Wiegand Data0	
R2	Wiegand Data1	
R3	Wiegand GND	
R4	- 12V	
R5	+12V	
R6	Not Connected	
R7	Door Relay NO	
R8	Door Relay NC	
R9	Door Relay COM	
R10	Fault Relay NO	
R11	Fault Relay NC	
R12	Fault Relay COM	
R13	Not Connected	
R14	GND1	verde
R15	Inactive / Fire (NO)	a-verde
R16	GND2	albastru
R17	PIR (NC)	a-albastru
R18	GND3	maro
R19	Exit Button (NO)	a-maro
R20	GND4	portocaliu
R21	Magnetic Contact (NC)	a-porto
R22	TAMPER	
R23	TAMPER	
R24	GROUND	

POWER SOURCE
12 V DC, 3A

RELAY 1A 30V DC

--- PASSCHIP®
1 Piata Presei Libere, Sektor 1, 013888, Bukarest, Rumänien
Tel: 0040745342887, Fax: 004 0378 104 216, office@passchip.com

Gedrückt in Rumänien
www.passchip.com

Wir behalten uns das Recht zu Änderungen vor

Allgemeine Spezifikationen :

i. ID ist auf eine bestimmte Anzahl von Karten-Typen

ii. BLK ist auf 1000 Datensätze beschränkt (der Wert kann erhöht werden, wenn keine Speicherkarte mehr auf die Liste geladen werden, aber das kann zue Erhögung der benötigten Zeit führen, um die Karte zu lesen und zu validieren)

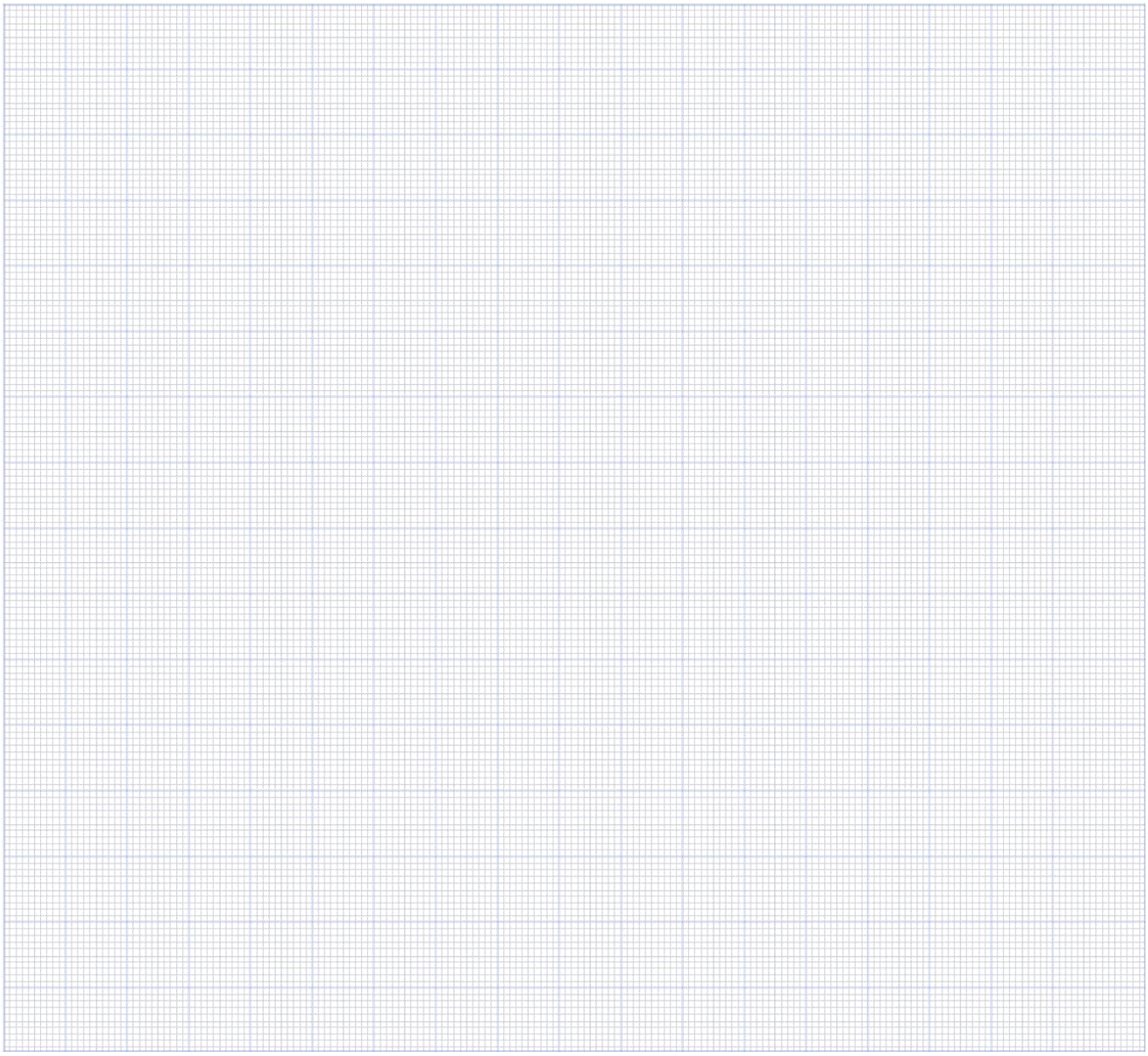
Für eine richtige Bewertung der Informationen in der LOG und für die Validierung der Karten (Vergleich Verfallsdatum – aktuelle Datum) ist es möglich, den Leser mit einem NTP-Server (vorzugsweise in LAN) zu synchronisieren - in dem internen DNS-kann einen Eintrag definiert warden, tock.usno.navy.mil oder time.windows.com nutzt, um den Leser auf die NTP-Server zu lenken.

Kommunikation	Ethernet 100 Base-TX/10Base-T RS232 bis 115200 Bit/Sek Zeit und Datum Wiegand bis 64 bit
Speicher	Inneres DRAM 64 MB , aufnehmen von mind 50 ID- profile laut EMV oder non EMV, Port SD, 1xSDA Echtzeituhr mit Li-Ion Batterie wartungsfre
Referenzstandards	ISO 7816 cu T=0 and T=1, EMVCo Level 1, ISO 7810, ISO 7811, JIS X6301, JIS X6302I
Prozessor	ARM 64-bit, 1.2 GHz,
Betriebssystem	Quad Linux OS
Software	On line, während des Betriebs
AktualisierungenSpeisung	85-264 VAC, 45-65 Hz, Cold Start,
Verbrauch	Max. 11 W
Innere Geschichte	5MB, aprox.10 000 Ereignisse mit Zeitstempel
Geschätzte Lebensdauer	Mind 125 000 Betriebsstunden Mind 500 000 Steckzyklen
Fügegeschwindigke	8-127 cm/Sek
Aufbau	Gehäuse in Edelstahl oder lackiert, antiskimming Metallbau, vandalensicher LCD-Bildschirm geschützt
Anzeige	4,3” TFT LCD Touchscreen-Typ, Helligkeit konfigurierbare Software Auflösung 480x272 Pixel Kontrast 300:1, Helligkeit mind 250cd/sqm Farben QVGA 65 000 farben oder monochrome 32 Graustufen
Konformitäten	Konformität CE
Umgebungsbedingungen	Betrieb:-30 C +50 C Lagerung:-35 C +60 C Feuchtigkeite: 10-95%
Größe (Breite x Höhe x Tiefe)	150 x 350 x 150 mm
Gewicht	3.90 Kg
Schutzklasse	IP65
Interaktion mit dem Benutzer	Eigentlich alle verfügbare bekannte schriftliche Sprache und multiton interner
Schwarze Liste	JA, online programmierbar für maximal 10 Kartenprofile
NFC	OPTIONAL

--- PASSCHIP®
1 Piata Presei Libere, Sektor 1, 013888, Bukarest, Rumänien
Tel: 0040745342887, Fax: 004 0378 104 216, office@passchip.com

Gedrückt in Rumänien
www.passchip.com

Wir behalten uns das Recht zu Änderungen vor



--- PASSCHIP®
1 Piata Presei Libere, Sektor 1, 013888, Bukarest, Rumänien
Tel: 0040745342887, Fax: 004 0378 104 216, office@passchip.com

Gedrückt in Rumänien

www.passchip.com

Wir behalten uns das Recht zu Änderungen vor