UniLock
System 10

Manual
Interface til
berøringsfri biometri læsere fra Idemia

Projekt	PRJ199
Version	1.0
Revision	240517

Denne biometrilæser giver hygiejnisk berøringsfri aflæsning af fingre sammen med anvendelse af berøringsfrie kort, QR-koder og PIN-koder.

Hånden skal blot bevæges forbi læsefeltet og på under et sekund er fingrene aflæst. Hastigheden gør læseren velegnet ved speedgates og lignende.

Biometrilæseren tilsluttes låsecomputeren via et interfaceprint. Når en person identificerer sig ved biometrilæseren, sendes data via interfaceprintet til låsecomputeren som en standard UniLock nøglekode. Når låsecomputeren signalerer adgang givet/nægtet eller PIN-kode krævet, sender interfaceprintet dette til biometrilæseren, som viser dette displayet.

Indholdsfortegnelse

Indholdsfortegnelse 2

1. Produktbeskrivelse 3

2. Operatør-vejledning 5

2.1 Oprette personer i UniLock 5
2.2 Oprette nøglekort med biometri til MorphoWave 5

3. Bruger-vejledning 7

3.1 Indtastning af pinkode 7

4. 3D fingeraftrykslæser (MorphoWave) 8

4.1 Adgangskode 8
4.2 Aktivering af hjemmeside 8
4.3 Grundopsætning 8
4.4 Placering af biometrisk data 14
4.5 Krav til kontrol af personer 15

5. Installationsvejledning 18

5.1 Tilslutning 18
5.2 Lysdioder på interfaceprintet 19
5.3 Tilbagemelding til biometrisk læser 19
5.3 Forbindelsesdiagram 20

1. Produktbeskrivelse

Læser til Biometri, RFID og PIN

Muligheder:
- ✓ Hygiejnisk 3D aflæsning af fingre
- ✓ 100% berøringsfri 2-faktor godkendelse
- ✓ Robust overfor lys, støv og fugt.
- ✓ Berøringsfri læser for Prox, Mifare, Iclass
- ✓ QR læser
- ✓ PIN-kode via touchdisplay

Teknik:
- ✓ Tilsluttes UniLock med interfaceprint

Anvendelse

Denne biometrilæser giver hygiejnisk berøringsfri aflæsning af fingre sammen med anvendelse af berøringsfrie kort, QR-koder og PIN-koder.

Hånden skal blot bevæges forbi læsefeltet og på under et sekund er fingrene aflæst. Hastigheden gør læseren velegnet ved speedgates og lignende.

Høj sikkerhed for korrekt aflæsning opnås via tredimensional (3D) aflæsning af en hånds fire fingre.

Høj brugervenlighed opnås via den animerede brugervejledning og simple betjening på læserens 4.3" touch-display.

Beskrivelse

Biometrilæseren understøtter person identifikation i form af biometri (fingre), berøringsfri kort (Mifare, Prox, Iclass), QR-kode og PIN.

Læseren kan skifte mellem forskellige krav til kombination af identifikationsformerne som fx kort + fingeraftryk udenfor arbejdstiden og fingeraftryk, QR-kode eller PIN-kode i arbejdstiden. Kombinationen kan være det samme altid eller styres fra UniLock låsecomputer.

Læserens fingeraflæsning er robust i forhold til lys, støv og fugt (våde/tørre fingre) og har håndtering af skadede/indbundne fingre.

Læseren kan bruges indendørs og udendørs (under tag eller monteret beskyttelsesvisir). Der er tilkøbsmulighed for monteringsstander og beskyttelsesvisir mod kraftig sollys og kraftig regn. Læseren forsynes via Ethernet (PoE+) eller 12/24 VDC.

Idemia præsentationsvideo: https://www.youtube.com/watch?v=q3TaHVvT8Fc

Biometrilæseren tilsluttes låsecomputeren via et interfaceprint. Når en person identificerer sig ved biometrilæseren, sendes data via interfaceprintet til låsecomputeren som en standard UniLock nøglekode. Når låsecomputeren signalerer adgang givet/nægtet eller PIN-kode krævet, sender interfaceprintet dette til biometrilæseren, som viser dette displayet.

Interfaceprintet kan via den fysiske dataforbindelse overvåges for at alarmere, når læsning ikke fungerer korrekt, som fx ikke-funktionel biometrilæser, kabelbrud mv.

Interfaceprintet forsynes direkte fra låsecomputeren og kan indbygges i samme montagekassen som låsecomputeren. Interfaceprintet indeholder flere lysdioder til at vise aktuel status og kommunikation.

Varenumre

UniLock interfaceprint:	PCB168-PIC165
Idemia fingeraftrykslæser:	MorphoWave XP, model: MPH - AC004B
Idemia ansigtslæser:	VisionPass (ikke afprøvet af Unitek)

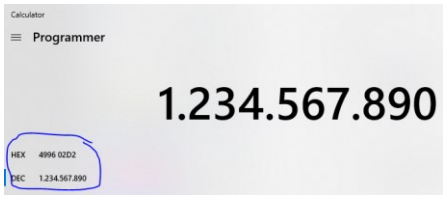
2. Operatør-vejledning

2.1 Oprette personer i UniLock

I UniLock Adgangseditor oprettes en person, og som nøgledata anvendes personens Morpho-Wave User ID.
Anbefalingen til MorphoWave er at anvende personens berøringsfrie korts CSN som User ID, hvor personens berøringsfrie kort blot kan indlæses UniLock (bordlæser eller læser ved en dør).

QR-kode eller MorphoWave User ID andet end anbefaling

Anvendes QR-kode eller er personers MorphoWave User ID andet end berøringsfri kort CSN skal QR-kode data eller User ID konverteres fra decimal-tal til hexadecimal-tal. Konvertering kan udføres med Windows lommeregner indstillet til ”Programmer”, hvor fx User ID decimal ”1234567890” konverteres til hexadecimal ”499602D2”. I UniLock oprettes personen med [Nøgledata]: ”499602D2” og [Nøgletype]: ”Standard (Hex)”.



I samspillet mellem MorphoWave og UniLock skal hexadecimal tals længde være 8 cifre eller 14 cifre, hvor der tilføjes foranstillede ”0” som:

- ”1234567” (decimal) => ”12D687” (hexadecimal) => ”0012D687” (nøgledata)
- ”112233445566” (decimal) => ”1A21A278BE” (hexadecimal) => ”00001A21A278BE”

2.2 Oprette nøglekort med biometri til MorphoWave

Anbefalingen er at personers biometriske template lagres i det personlige berøringsfrie nøglekort fremfor i læserens database og at personers User ID er det personlige berøringsfrie korts CSN (Card Serial Number). Se afsnit ”4.3 Grundopsætning”.

Nøglekort kan programmeres med biometrisk template direkte på MorphoWave læserens touch-display eller via læserens hjemmeside.

Oprettelse fra touch-display

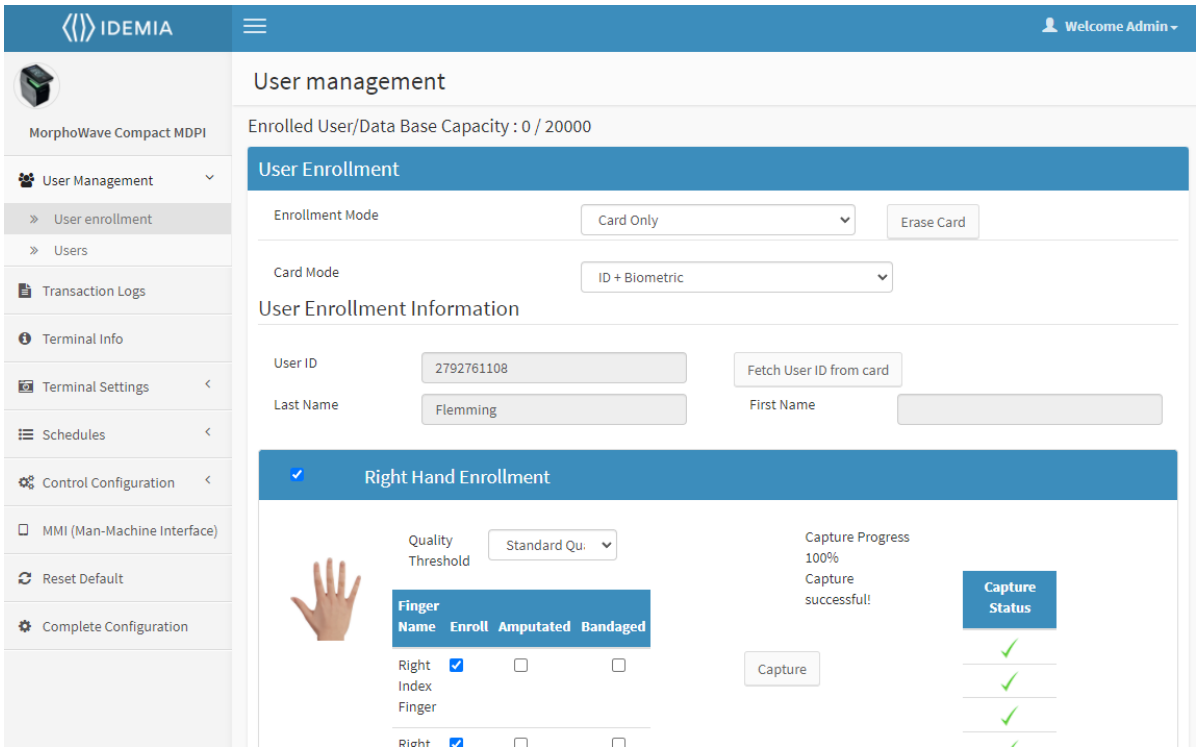
På MorphoWave touch-display logges ind med adgangskode. Der kan oprettes login som kun kan tilføje personer.

Fra touch-display programmeres nøglekort under menupunktet [User Menu], [Add/Enroll User], [Card Only], [ID + Template]. Følg vejledningen i læserens display.

Oprettelse fra hjemmeside

Fra læserens hjemmeside programmeres kort under menupunktet: [Hjemmeside], [User Management]:

1. [User Enrollment]:
   a) Enrollment Mode: Card only (Andre muligheder er: ”Db only”, ”Db + Card”).
   b) Card Mode: ID + Biometric
   c) Last Name: Brugernavn (som i praksis ikke bruges).
2. [User Enrollment information]: Indlæs nøglekort CSN
   a) Tryk på [Fetch User ID from card]
   b) Følg vejledning på hjemmeside og touch-display.
3. [Right Hand Enrollment]: Indlæs højre hånd
   a) Aktiver med flueben
   b) Vælg indstillinger og tryk på [Capture].
   c) Følg vejledning på hjemmeside og touch-display.
4. [Left Hand Enrollment]: Indlæs venstre hånd
   a) Aktiver med flueben
   b) Vælg indstillinger og tryk på [Capture].
   c) Følg vejledning på hjemmeside og touch-display.
5. [Finger to Encode On Card]
   a) Marker de fingre som skal gemmes i personens nøglekort.
   b) Tryk på [Submit], for at gemme
   c) Gem template på koret ved at følge vejledningen på hjemmeside og touch-display.



3. Bruger-vejledning

Følg vejledningen i læserens display for at få adgang.

3.1 Indtastning af pinkode

Når adgang kræver pinkode vil læserens display automatisk vise et pinkode-tastatur.

Indtastning af pinkode afsluttes med tasten '#'. Indtastes "#" ikke vil indtastningen automatisk afsluttes ca. 4,5 sekunder efter seneste ciffertryk.

Pinkodetastaturet forsvinder når der trykkes på  eller  men har ikke nogen betydning for indtastning af pinkode.

4. 3D fingeraftrykslæser (MorphoWave)

Interfaceprintet er testet med Idemia MorphoWave XP 3D fingeraftrykslæser (firmware version 2.7.2), og fungerer sandsynligvis også med sammenlignelige biometriske læsere af samme fabrikat.
Dette afsnit omhandler grundopsætning og indeholder informationer fra MorphoWave manualen "Administration Guide for Access & Time Terminals", som er nødvendig eller relevant opsætning efter fabriksindstilling.

Opsætning af MorphoWave foretages på touch-display, via læserens hjemmeside eller Idemia pc-program MorphoBioToolBox. I nogle tilfælde skal MorphoWave genstartes før ændringer træder i kraft.

4.1 Adgangskode

Adgang til læseren er beskyttet med adgangskode, hvor default adgangskode er angivet i manualen. Som altid bør adgangskode hurtigst muligt ændres væk fra default.

Skal personer selv kunne oprette sig fra læserens touch-display, anbefales det at begrænse rettigheder til kun at kunne oprette personer.

1. Opret en person i MorphoWave. Password (fx "1298") tilføjes som Login Identifier.
2. Password (fx "1298") tilføjes som LCD Login Password.
3. Personens administrator rettigheder sættes til "Limited Database Admin": [Touch-display], [User Menu], [Edit User], [Administration rights]: Limited Database Admin.
4. Fra hjemmeside sættes parameter "misc.LCD_login_option = 1", så der skal anvendes ID+Password til login på display.

4.2 Aktivering af hjemmeside

Meget opsætning kan foretages fra læserens touch-display, hvor hjemmesiden er et godt alternativ. Hjemmesiden skal aktiveres fra touch-display og af sikkerhedsmæssige årsager anbefales det at deaktivere hjemmesiden efter endt brug eller som minimum anvende SSL/TLS og indstille hvilke IP-adresser der kan kommunikere med læseren.

1. Er læseren tilsluttet et netværk med DHCP-server bør DHCP aktiveres først:
    - [Touch-display], [Communication], [Network Interface], [Ethernet], [IP Settings], [IPv4], [IP Mode]: DHCP
2. Aktivering af hjemmeside (Webserver):
    - [Touch-display], [System Menu], [Miscellaneous], [Web Server]: On

4.3 Grundopsætning

I Webbrowser indtastes læserens Hostnavn eller IP-adresse som findes via touch-displayet.

- IP-adresse: [Information menu], [Communication], [Ethernet], [IPV4]: IP Address
- Hostnavn: [Information menu], [Communication]: Hostname

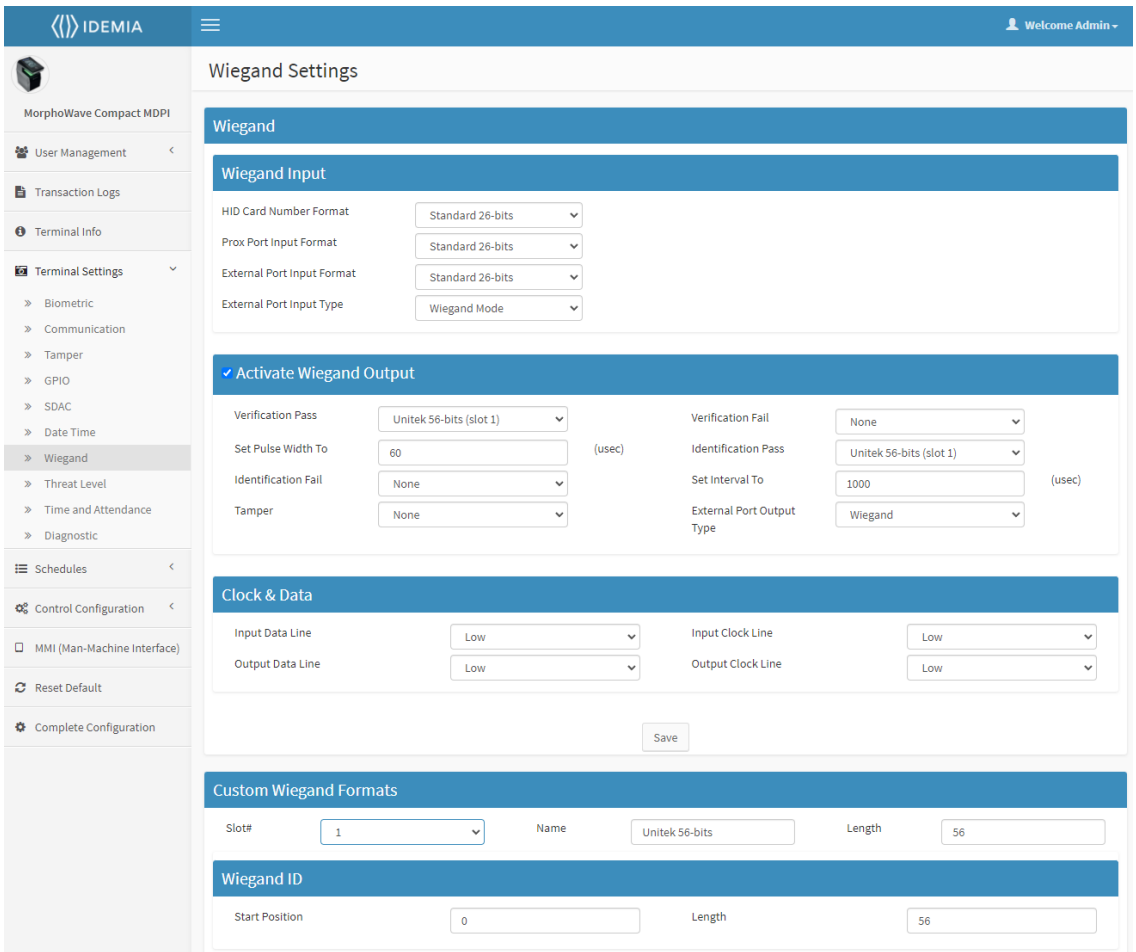
Dataformat (Wiegand)

Interfaceprintet modtager 56bit Wiegand data fra læseren, hvor 56bit Wiegand formatet først skal oprettes i læseren.

[Hjemmeside], [Terminal settings], [Wiegand Settings]:

1. [Custom Wiegand Formats]:
   d) Slot#: Vælg et ledigt
   e) Name: Unitek 56-bits
   f) Length: 56
   g) Wiegand ID:
      - Start position: 0
      - Length: 56
   h) Tryk på [Save the selected slot] for at gemme.

2. [Wiegand], [Activate Wiegand Output]:
   a) Activate Wiegand Output: Aktiv (flueben)
   b) Verification Pass: Unitek 56-bits
   c) Tamper: None
   d) Identification Pass: Unitek 56-bits
   e) Set Interval To: 1000 (us)
   f) Tryk [Save] for at gemme.

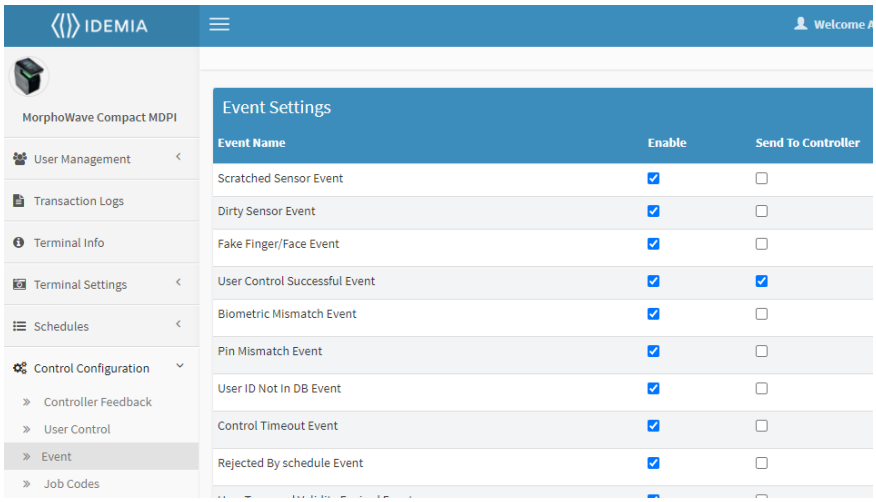


Sende data til interfaceprint

Læseren skal konfigureres til at afsende personers identifikation eller QR-kode-data via Wiegand til interfaceprintet.

[Hjemmeside], [Control Configuration], [Event], [Event Settings]:

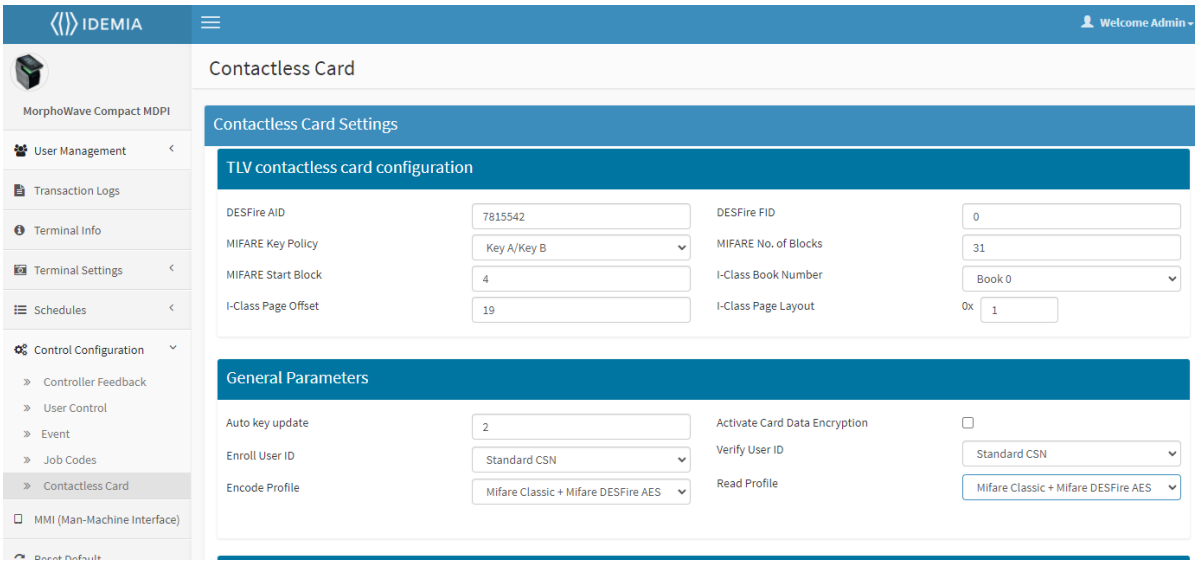
1. [User Control Successful Event]:
   a) Enable: Aktiv
   b) Send To Controller: Aktiv
   c) Tryk [Save] for at gemme



Identifikation af personer

Når personers identifikation skal anvendes i flere systemer, er det lettest at anvende samme identifikation i alle systemer. Personers berøringsfrie kort er det oplagte valg, da alle systemer til adgangskontrol, printere, kantiner, vaskerier mv. understøtter dette. MorphoWave indstilles således også til at anvende berøringsfrie kort som personers identifikation.
[Hjemmeside], [Control Configuration], [Contactless Card], [Contactless Card Settings]:

1. [General Parameters]:
   a) Enroll User ID: Standard CSN
   b) Verify User ID: Standard CSN
   c) Encode Profile: Vælg de korttyper som anvendes i installationen
   d) Decode Profile: Samme som Encode Profile
   e) Tryk [Save] for at gemme



Gemmes data (biometrisk template) på det berøringsfrie kort som anbefalet, bør man aktivere kort data kryptering og tildele alle biometriske læsere i installationen samme DESFire AID og krypteringsnøgler (pc-program Idemia MorphoBioToolBox).

Når personer oprettes via læserens touch-display kan man som standard indtaste Bruger ID. Manuel indtastning af bruger ID deaktiveres (og samtidig tvang om brug af det berøringsfrie korts ID) ved at ændre læserens parameter [misc.user_id_edit] fra ”0” til ”1”.

[Hjemmeside], [Complete Configuration], [Configurations], [Parameter Key]:

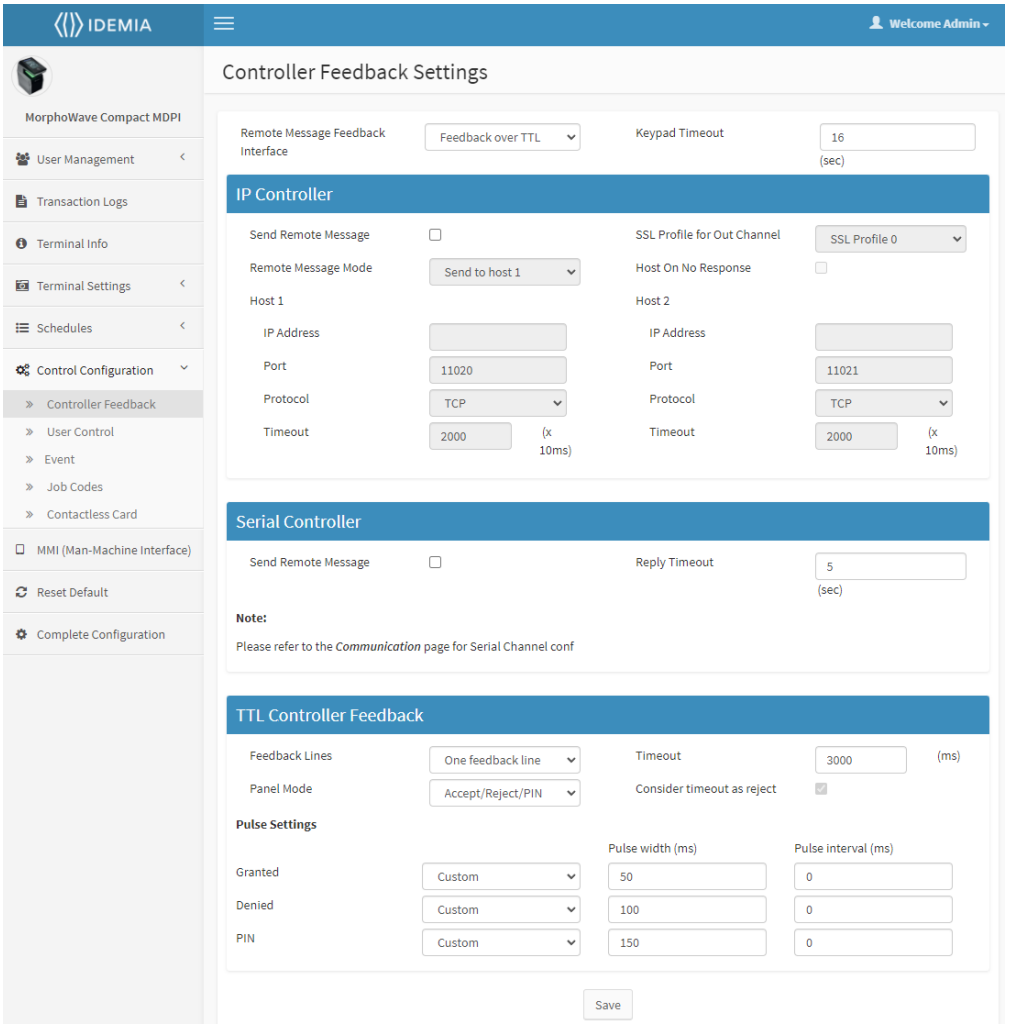
1. misc.user_id_edit
   a) Parameter Key: Aktiv
   b) Parameter Value: 1
   c) Tryk [Save] for at gemme

Tilbagemelding for adgangsforsøg (Controller feedback)

Efter et adgangsforsøg kan MorphoWave display vise om adgang nægtes eller tillades, hvilket interfaceprintet signalerer via en digital indgang på læseren.

[Hjemmeside], [Control Configuration], [Controller Feedback], [Controller Feedback Settings]:

1. [Remote Message Feedback Interface]: Feedback over TTL
2. [Keypad Timeout]: 16 sec. (maksimal tid for indtastning af pinkode)
3. [TTL Controller Feedback]:
   a) Panel Mode: Accept/Reject/PIN
   b) Pulse Settings
      - Granted:
        - Pulse width (ms): 50
        - Pulse interval (ms): 0
      - Denied:
        - Pulse width (ms): 100
        - Pulse interval (ms): 0
      - PIN:
        - Pulse width (ms): 150
        - Pulse interval (ms): 0
   c) Tryk [Save] for at gemme



Biometrisk følsomhed (sikkerhed)

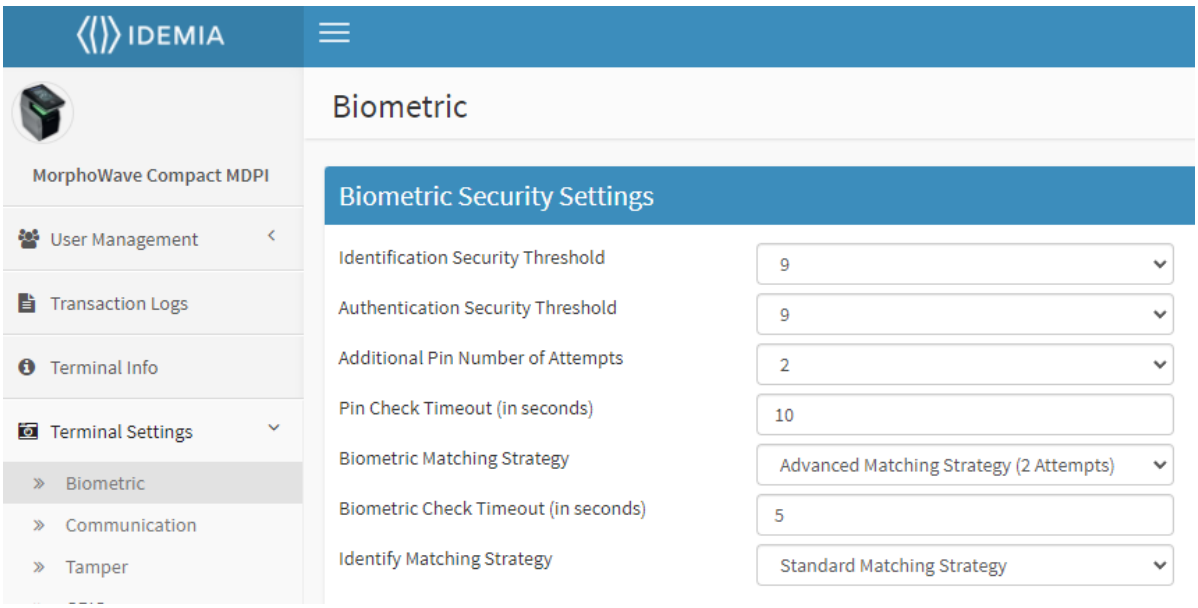
Biometrisk følsomheden i læseren kan justeres, så sandsynligheden for afvisning af en registreret bruger er lav (False Rejection Rate (FRR)), men det er på bekostning af en større sandsynlighed for accept af uregistrerede brugere (False Acceptance Rate (FAR)). Disse to er modsatrettede parametre og det glemmer mange at tage med i deres sikkerhedsbetragtninger.

fejlraten for falske accepterede læsninger (FAR) kan justeres [Hjemmeside], [Terminal settings], [Biometric]:

1. Fejlraten for identifikation af brugere med biometri oprettet i terminalens database:
   a) Identification Security Threshold: 9 (anbefales)
2. Fejlraten for verificering af personer med biometri oprettet på personens nøglekort:
   b) Authentication Security Threshold: 9 (anbefales

Værdi	Beskrivelse
1	FAR < 1 %
2	FAR < 0,5 %
3	FAR < 0,1 % (standard)
4	FAR < 0,05 %
5	FAR < 0,01 %
6	FAR < 0,001 %
7	FAR < 0,0001 %
8	FAR < 0,00001 %
9	FAR < 0,0000001 %
10	Ikke anbefalet af producenten grundet for mange falske afvisninger

Sikkerhedsmæssigt bør man være meget forsigtig med at sætte niveauet for lavt, da man sjældent bliver gjort opmærksom på falske positive (adgang til uregistreret person), hvorimod man altid bliver gjort opmærksom på falske afvisninger (nægtet adgang til registreret person).



4.4 Placering af biometrisk data

Identifikation af fingeraftryk fungerer ved at personens fingeraftryk først indlæses som personlig template, hvor læseren efterfølgende kan identificere personen ved at sammenligne template med scanning af fingre når en person ønsker adgang.

Personens fingeraftryk-template kan gemmes lokalt i læserens database eller i personens berøringsfrie kort.

Vi anbefaler at gemme template i det berøringsfrie kort, da dette kombinerer højere sikkerhed[1] ved at kombinere to faktorer (kort og biometri) og lettere administration da man så undgår at skulle oprette hver template i alle MorphoWave læsere i installationen.

Husk at beskytte template på kort med krypteringsnøgle. Krypteringsnøglen og lignende skal være identisk i alle biometriske læsere i installationen. Krypteringsnøgler til berøringsfrie kort kan ændres med pc-programmet Idemia MorphoBioToolBox og via læserens touch-display [User Menu], [Card Manager].

[1] Højeste sikkerhed opnås når hver kunde har egne krypteringsnøgler til at beskytte template-data i kortene.

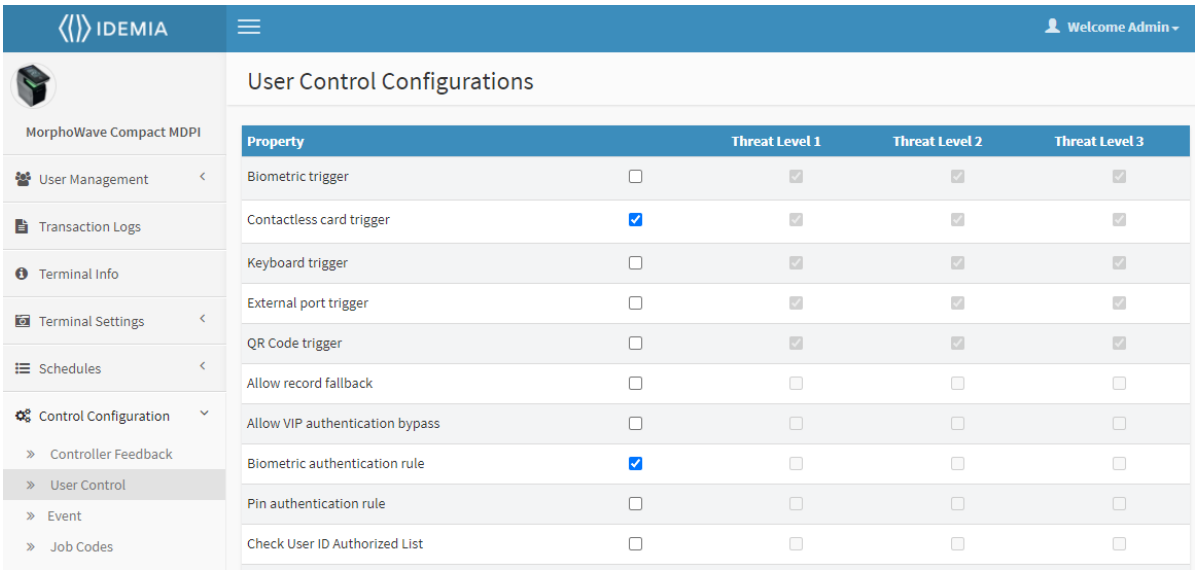
4.5 Krav til kontrol af personer

Biometrilæseren har sine egne krav til kontrol af personers identifikation, som kan indstilles til noget fast eller styres via læserens indgange (Threat Level).

Biometrilæseren understøtter person identifikation i form af biometri, berøringsfri kort, QR-kode (MorphoWave XP) og PIN. Identifikationsformerne kan kombineres.

[Hjemmeside], [Control Configuration], [User Control], [User Control Configurations], [Property]:

Krav til identifikation	**Indstillinger**	**Handling ved læser**
Berøringsfri kort indeholdende biometrisk personlig template (anbefalet).	a) Contactless card trigger: Aktiv b) Biometric authentication rule: Aktiv	a) Vis kort. b) Vis hånd.
Biometri[1)] eller berøringsfri kort indeholdende biometrisk personlig template (standard).	a) Biometric trigger: Aktiv b) Contactless card trigger: Aktiv c) Biometric authentication rule: Aktiv	a) Vis kort eller hånd. b) Vis hånd hvis startvisning var kort.
Biometri[1)] eller berøringsfri kort.	a) Biometric trigger: Aktiv b) Contactless card trigger: Aktiv	a) Vis kort eller hånd.
Biometri[1)]	a) Biometric trigger: Aktiv	a) Vis hånd.
QR-kode[2)]	b) QR Code trigger: Aktiv	a) Vis QR-kode.



Figur 1 Opsætning for anbefalet krav til identifikation (Identificer med berøringsfri kort og autentificer med biometri)

[1)] Forudsætter at personers biometriske template er gemt i læserens database.

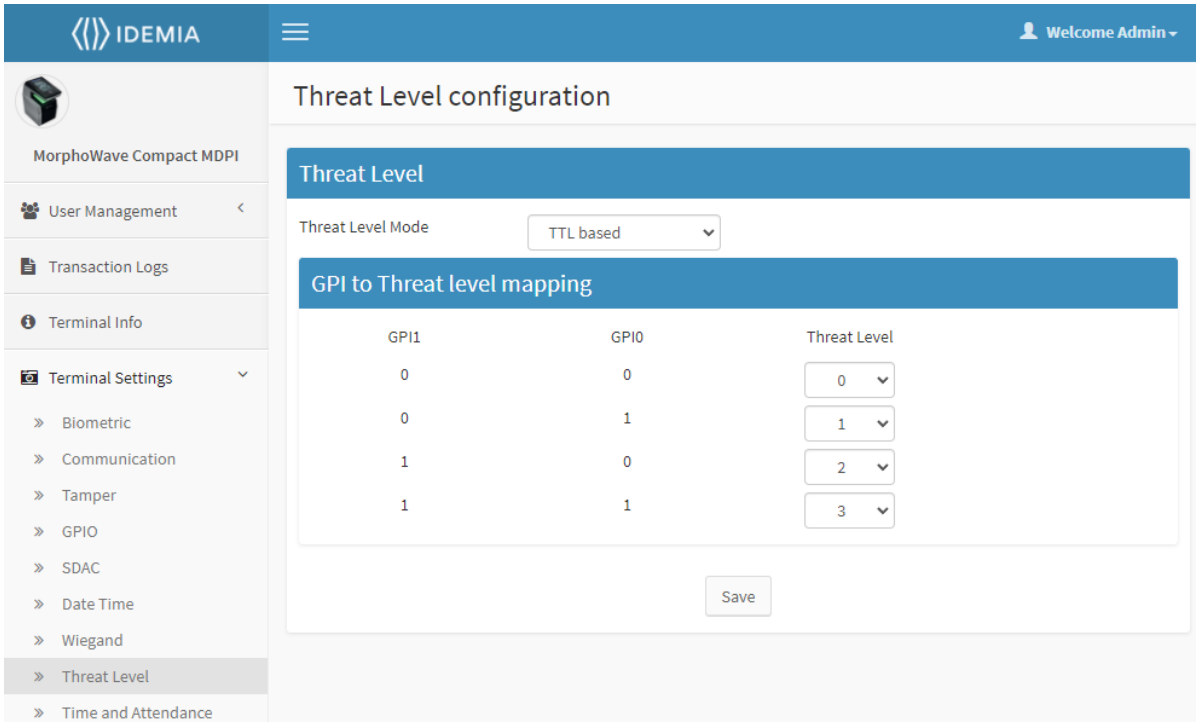
[2)] QR-kode data konverteres fra decimal-tal til hexadecimal-tal ”1234567890” => ”499602D2” fx med Windows lommeregner og oprettes i UniLock som nøgledata med [Nøgletype]: ”Standard (Hex).

Det er muligt at skifte mellem at tillade forskellige krav til personers identifikation, som fx at tillade QR-koder på nogle tidspunkter af døgnet, mens andre tidspunkter kræver kort + biometri.

Læseren kan skifte mellem fire forskellige sikkerhedsniveauer (Threat Level) via læserens indgange (GPI 0 og GPI 1), som kan styres fra UniLock låsecomputerens udgange. Udgange tilsluttes læserens indgange og på låsecomputeren monteres en pull-up modstand (fx 1 kΩ) fra hver udgang til 5VDC.

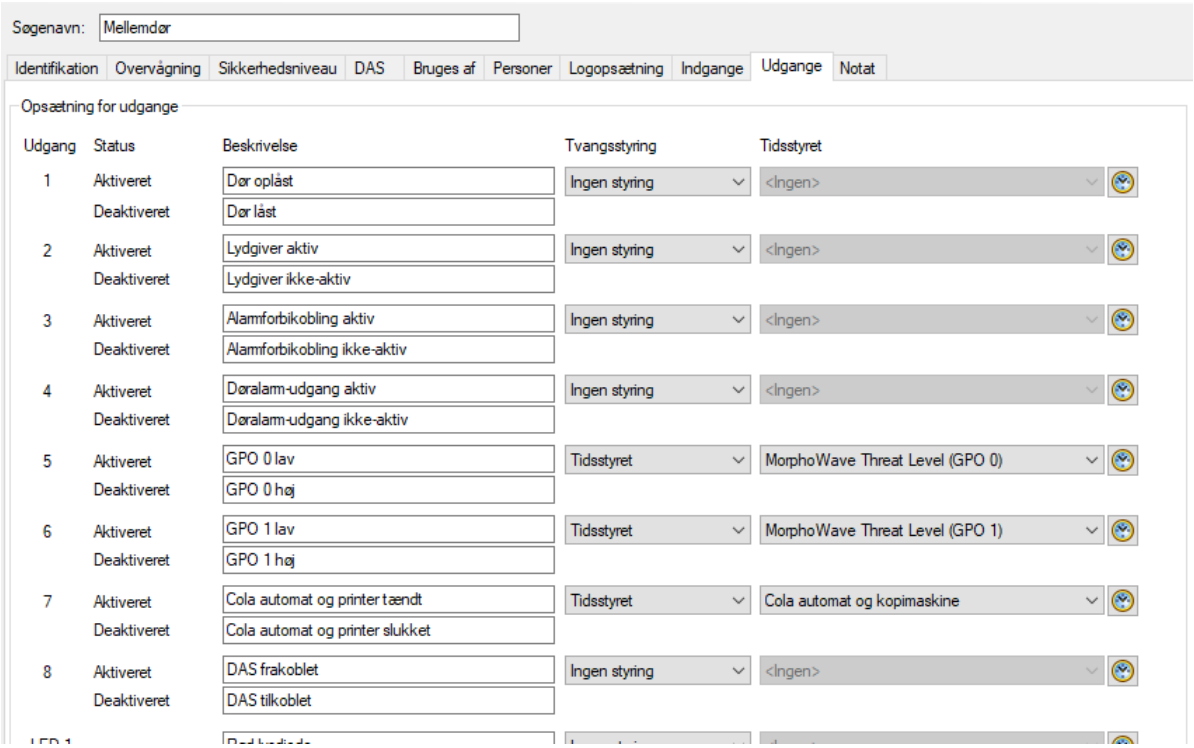
Læserens indganges funktion indstilles fra [Hjemmeside], [Terminal Settings], [Threat Level]:

1. [Threat Level]:
   a) Threat Level Mode: TTL based
   b) Tryk [Save] for at gemme.

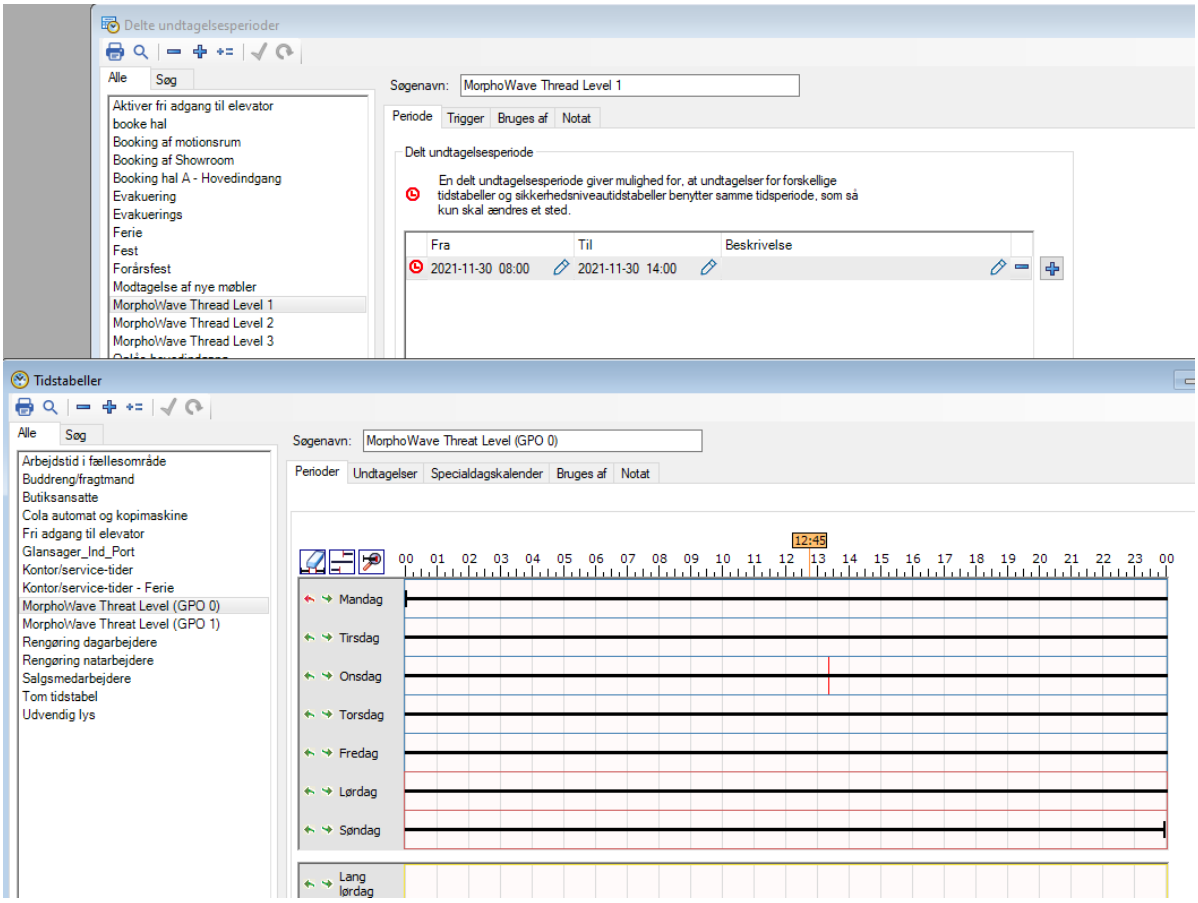


I UniLock adgangseditor indstilles k-punktets (låsecomputerens) udgang til at følge en tidstabel, som skifter mellem to af læserens fire Thread Level.

Vil man skifte mellem alle læserens fire sikkerhedsniveauer (avanceret) anvendes to udgange som styres af hver sin tidstabel, hvor udgangskombinationerne styres ved at have tre delte undtagelser til at kombinere on/off i de to tidstabeller.



Figur 2 K-punktets udgange styrer læserens fire Thread Levels (avanceret)



Figur 3 Tidstabeller og Delte undtagelser til at styre læserens fire Thread Levels (avanceret)

5. Installationsvejledning

5.1 Tilslutning

Interfaceprintet monteres mellem låsecomputeren og den biometriske læser.

Elektriske forbindelser

Interfaceprintet forbindes fra J3 og J11 til låsecomputeren med et 7-ledet kabel. Interfaceprintet forbindes fra J7 til læserens fastmonteret kabel. Forbindelsesdiagram ses på Figur 4.

Data

Interfaceprint	PCB168-PIC165
Interface 1 (J3)	
Forsyning:	8-14 VDC, 90 mA
Interface 2 (J11)	Til LS10
Indgange:	3 stk. TTL (lysdioder)
Udgange:	2 stk. åben kollektor (data)
Interface 4 (J7)	Til biometrilæser
Udgange:	3 stk. TTL
Indgange:	2 stk. intern pull-up til 5 VDC
Særligt:	Overvåget dataforbindelse
	Overvåget biometrilæser
Størrelse:	110 x 80 x 30 mm, 60 g
Fingeraftryklæser	Idemia MorphoWave XP
Forsyning ind:	
PoE+:	Max 25W
VDC:	12-24 VDC, 2,5A@12VDC
Kabel (fastmonteret):	<30cm kabel
Beskyttelsesklasse:	IP65
Størrelse:	152 x 250 x 220 mm, ca. 2 kg

5.2 Lysdioder på interfaceprintet

Lysdiode	Beskrivelse
D13 (Power)	Rød konstant. Forsyning tilsluttet.
D17 (Ok/Error)	Rød = 0,1 sek. off = 0,1 sek.: Initialisering. Rød = 0,1 sek. off = 1,9 sek.: Klar.
D16 (Rød/Grøn)	Som lysdiode i læser. Se UniLock manual til Windows program.
D19 (Gul)	Som DAS-lysdiode i læser. Se UniLock manual til Windows program.
D10 (Rx)	Gul: Data modtages fra læseren
D9 (Tx)	Gul blink (0,25 sek.): Data sendes til låsecomputeren.
D12 (Tx)	Gul: Feedback signal til læser aktiveret.

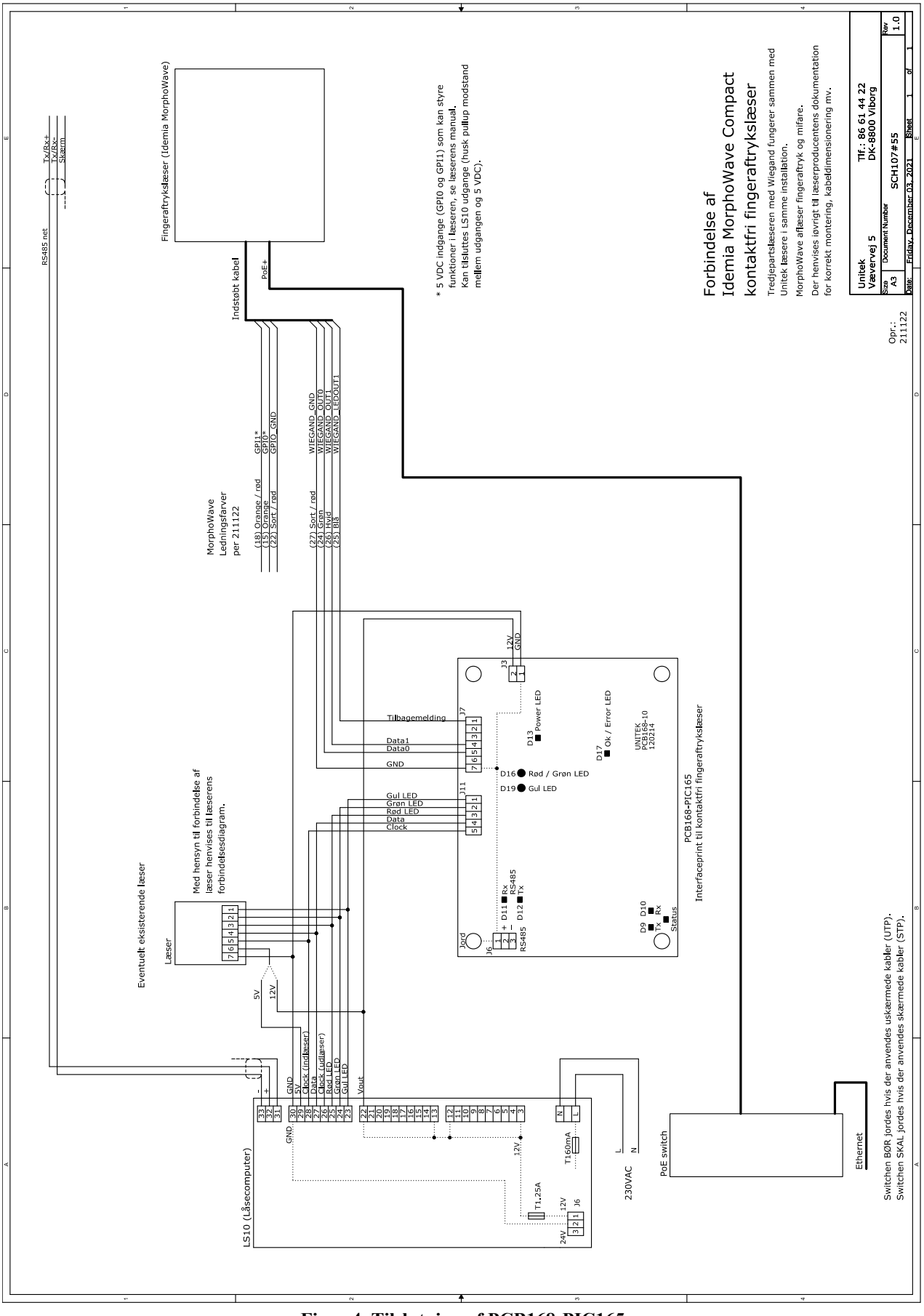
5.3 Tilbagemelding til biometrisk læser

Interfaceprintet giver tilbagemelding fra adgangsforsøget på digital udgang J7 terminal 1[2], som forbindes til læseren. Den biometriske læsers display viser adgang givet eller afvist baseret på tilbagemeldingen.

LS10 status	Feedback signal	Indikation på terminalens display
Bruger accepteret	50ms puls	”Access granted”
Bruger afvist	100ms puls	”Access denied”
Behov for pinkode	150ms puls	Tastatur til indtastning af pinkode

[2] Interfaceprintet baserer adgang givet/afvist på låsecomputerens statusindikation til læser (rød/grøn lysdiode).

5.3 Forbindelsesdiagram



Figur 4. Tilslutning af PCB168-PIC165