UniLock
System 10

Manual til
gateway
CV72 v2

Projekt	PRJ149
Version	2.0
Revision	240716

CV72 er en højsikker Ethernet til RS485 gateway, som giver mulighed for at tilslutte låsecomputernes RS485-net direkte til et Ethernet netværk.

UniLock programmet kommunikerer direkte med CV72 i lokaliteten via en TCP/IP forbindelse, der er sikret efter højeste krypteringsstandarder mod aflytning, manipulation, replay og hijacking.

CV72 kan forsynes via Power over Ethernet (PoE) og kan eventuelt strømforsyne en låsecomputer.

Konfiguration foretages med det meget brugervenlige Windows program CV-Config.

Indholdsfortegnelse

1. Produktbeskrivelse

Anvendelse

Er en virksomhed spredt over et større geografisk område, kan adgangskontrolsystemet opdeles i lokaliteter. Disse lokaliteter kan hver især forbindes til en CV72 gateway, hvorved låsecomputere i lokaliteten kan holdes opdateret over det lokale pc-netværk og internettet.

UniLock programmet kommunikerer direkte med CV72 i lokaliteten via en TCP/IP forbindelse, der er sikret efter højeste krypteringsstandarder mod aflytning, manipulation, replay og hijacking.

CV72 kan forsynes via Power over Ethernet (PoE) og kan eventuelt strømforsyne en låsecomputer.

Beskrivelse

CV72 er en højsikker Ethernet til RS485 gateway, som giver mulighed for at tilslutte låsecomputernes RS485-net direkte til et Ethernet netværk.

CV72 understøtter automatisk tildeling af IP-adresse (DHCP) og automatisk registrering af hostnavn i DNS-server.

For at sikre dataintegriteten, forhindre manipulation af data, replay af beskeder og hijacking af enheder, er de vitale dele af kommunikationen sikret efter højeste krypteringsstandarder. Endvidere kan enheden beskyttes med adgangskode.

CV72 kan forsynes over Ethernet via PoE, fra en låsecomputer eller med en almindelig netadapter. Der er fuld galvanisk adskillelse mellem Ethernet og RS485 nettet, så problemer med fejl- og jordstrømme undgås.

Forskellige lysdioder viser driftsinformationer, som kan være en god hjælp ved installation og kontrol. Detaljerede driftsinformationer og statistik kan aflæses via den indbyggede hjemmeside.

Konfiguration foretages med det meget brugervenlige Windows program CV-Config.

CV72 Open Frame
Funktionsmæssigt som CV72, dog kan en PoE forsynet CV72 Open Frame strømforsyne en låsecomputer. Forsynes en låsecomputer anbefales det, at anvende PoE+ for at have mest muligt effekt til rådighed. Er der ikke PoE til rådighed, kan enheden forsynes fra låsecomputeren.

CV72 Open Frame leveres som rå printplade beregnet til indbygning i låsecomputerens montagekasse.

Krav til pc-software

Opmærksomheden henledes på, at denne CV72 (v2) indeholder mange nye funktioner og nyeste højteknologiske krypteringsalgoritmer i forhold til den tidligere CV72 (v1). Derfor kræves følgelig også tilsvarende opdateret UniLock pc-program og CV-Config.

Krav:
UniLock version 2.0 minimum revision 2017-03-07, dog anbefales altid nyeste.
CV-Config revision 2016-09-02 eller nyere.

CV72 modtager automatisk softwareopdateringer fra UniLock pc-program, blandt andet derfor anbefales det generelt at holde pc-programmet opdateret.

2. Installations-vejledning

Dette afsnit indeholder information om konfiguration af CV72 samt eventuel nødvendig konfiguration af DHCP- og DNS-servere.

2.1 Valg af opsætning

Inden CV72 kan fungere i pc-netværket, skal den være konfigureret korrekt.

Konfiguration af CV72 og eventuelle ændringer i DHCP- og/eller DNS-serveren, bør altid foregå i samarbejde med den netværksansvarlige. Forkert opsætning kan i værste fald få alvorlige konsekvenser for pc-netværket i form af tabte data og driftsstop.

Inden der ændres i opsætningen for CV72, skal nedenstående skema udfyldes. En detaljeret beskrivelse af de enkelte felter findes i de efterfølgende afsnit.

Identifikation	
Hostnavn	
Domæne	(Valgfri)
Registreringsadresse	(Valgfri)
Netværk	
	☐ Fast IP-adresse ☐ DHCP
IP-adresse	(Kun ved fast IP-adresse)
Netmaske	(Kun ved fast IP-adresse)
Gateway adresse	(Kun ved fast IP-adresse)
DNS-server	Primær: (Kun ved fast DNS adresse)
	Sekundær: (Kun ved fast DNS adresse)
Port nummer	(default 7211)

Indtil det er fastlagt, hvordan skemaet skal udfyldes, er der ingen grund til at gå videre.

Identifikation

Enheden kan identificeres på netværket ved hjælp af et hostnavn enten gennem NetBIOS eller DNS.
Et NetBIOS-navn (hostnavn) kan kun anvendes indenfor samme subnet, det kræver ingen DNS-server, der skal blot vælges et hostnavn til enheden.
Et DNS-navn (hostnavn.domæne) kan anvendes i hele domænet på tværs af subnet, men det kræver en DNS-server, som skal være kendt og åben for registrering. Foruden hostnavnet bør domæne og eventuelt registreringsadresse angives. Afhængig af den aktuelle installation kan det dog udelades, hvis den primære eller sekundære DNS-server skal anvendes til registrering.

Hostnavn

Hostnavn kan bruges i stedet for en fast IP-adresse til at identificere enheden på netværket ved hjælp af NetBIOS eller DNS. Default hostnavn er: ”CV72-xxxxxx”, hvor xxxxxx er de sidste 6 cifre i enhedens MAC-adresse.

Et NetBIOS-navn kan maksimalt være på 15 karakterer. Indtastes et hostnavn på mere end 15 karakterer, anvendes enhedens default hostnavn som NetBIOS-navn og det indtastede hostnavn som DNS-navn. (max 63 karakterer).

Domæne

Domænet bruges når enheden skal registrere sit hostnavn i en DNS-server, og angiver hvilket domæne, enheden skal være en del af.

Angives intet domæne, vil enheden automatisk forsøge, at anvende det samme domæne som den primære eller sekundære DNS-server tilhører (omvendt DNS opslag).

Registreringsadresse

Som noget helt specielt har enheden mulighed for, at registrere sig i en anden DNS-server end den primære eller sekundære DNS-server. Dette kan anvendes i de situationer, hvor enheden skal installeres i en lokalitet med en anden DNS-opsætning end i ”hovedafdelingen”, og hvor enhedens hostnavn skal anvendes af fx Polleren.

Angives intet, bruges den primære eller sekundære DNS-server.

Netværk

Enheden kan anvende en fast netværkskonfiguration, eller automatisk hente den fra en DHCP-server.

Skal netværkskonfiguration automatisk hentes fra en DHCP-server, skal parametrene IP-adresse, Netmaske og Gateway-adresse ikke udfyldes. Ligeledes kan DNS-serveradresserne udelades, hvis disse tildeles af DHCP-serveren.

DHCP-serveren kan tildele CV72 en tilfældig IP-adresse indenfor sit adresseområde, eller en fast IP-adresse, hvis den ønskede IP-adresse er låst til enhedens MAC-adresse (statisk DHCP).

Hvis der i routeren anvendes port mapping (port forwarding) for at gøre enheden tilgængelig fra internet, kan det være nødvendigt at tildele enheden en fast IP-adresse, hvis den anvendte router ikke understøtter hostnavne.

IP-adresse

Hvis der vælges en fast IP-adresse skal (bør) denne ligge udenfor det område som DHCP-serveren tildeler IP-adresser ud fra.

Netmaske

Skal normalt være den samme som for andre ”apparater” på samme subnet. I et almindeligt klasse C netværk er netmasken 255.255.255.0.

Gateway-adresse

Den adresse der skal sendes til, hvis der sendes til en IP-adresse der ligger uden for subnettets adresseområde. Skal enheden anvendes på samme subnet som UniLock pc-programmet, er det ikke nødvendigt at konfigurere gateway adressen.

DNS-serveradresse

IP-adresse for den primære og den sekundære DNS-server, hvis ikke de tildeles af DHCP-serveren.

Port nummer

Den port som benyttes til at kommunikere på. Som default anbefales det at anvende port nummer 7211, men det kan i princippet være alle tal mellem 1024 og 65535. Det valgte port nummer, skal normalt være det samme som er valgt i det program der kommunikeres med (UniLock).

2.2 Konfiguration af CV72

Opsætning af CV72 udføres med Windows programmet CV-Config. CV-Config kan downloades fra Uniteks hjemmeside. Programmet kan afvikles direkte uden at installere noget software på pc'en.

Når enheden er konfigureret skal programmet ikke bruges mere. Det er derfor sjældent nødvendigt at installere det. Ønskes det alligevel at installere programmet, gøres det ved manuelt at kopiere programfilen til det ønskede drev/mappe.

2.2.1 Tilslutning

Den CV72 der skal konfigureres, skal tilsluttes det samme subnet som den pc hvorpå CV-Config afvikles.

CV-Config kommunikerer med enheder via broadcast, hvorved der kommunikeres uden brug af IP-adresser. Dette gør det muligt, at konfigurere CV72 på et andet netværk end der hvor den efterfølgende skal anvendes.

2.2.2 Søgning med CV-Config

Når CV-Config startes, søges der automatisk efter enheder på netværket. Alle fundne enheder vises i en sorteret liste. Som udgangspunkt er listen sorteret efter enhedernes oppetid, så den enhed der sidst blev tændt, står øverst på listen.

Har pc'en flere netværkskort vælges det korrekte netværkskort i listen.

Listen over fundne enheder kan opdateres ved at trykke på knappen [Søg].

2.2.3 Rediger indstillinger

For at ændre parametrene for en enhed, vælges den på listen, hvorefter der trykkes på knappen [Rediger indstillinger], eller der kan dobbeltklikkes på den i listen. Derved fremkommer en dialog hvor de ønskede parametre kan angives. Når der vælges [OK] sendes de nye parametre til enheden.

Når parametre er ændret i enheden, opdateres listen automatisk med de nye parametre. Parametre i listen er alle modtaget fra enhederne, så man kan være sikker på, at de viste parametre, også rent faktisk er de parametre, der er i de respektive enheder.

2.2.4 Adgangskode

CV72 kan beskyttes med en adgangskode på op til 32 karakterer. Adgangskoden gør det umuligt at ændre parametrene medmindre adgangskoden er kendt.

Et kort tryk på knappen i enheden nulstiller adgangskoden (adgangsnøgle).

For optimalt sikkerhed bør enheden tildeles en adgangskode på et lukket netværk, før den eventuelt flyttes til et offentligt netværk.

2.3 Konfiguration af pc-netværk

Afhængigt af netværkets opbygning og konfiguration kan der være behov for at ændre opsætningen af router og/eller DNS-server.

2.3.1 Opsætning af router

Kommunikationen mellem UniLock pc-programmet og CV72 foregår på den brugervalgte IP-port, default 7211. Det er pc-programmet, der skaber forbindelse til CV72. Det er derfor nødvendigt, at der kan kommunikeres med CV72 på den valgte port. Det vil sige, hvis CV72 og pc-programmet er adskilt af routere, firewalls og lignende, skal der i disse åbnes for den valgte IP-port, så pc-programmet kan få forbindelse til CV72.

Port mapping

CV72 tildeles normalt ikke en ”offentlig” IP adresse. Er CV72 og pc-programmet adskilt af fx en router, kan den lokale IP-adresse ikke bruges direkte, da lokale IP-adresser ikke kan routes over internet.

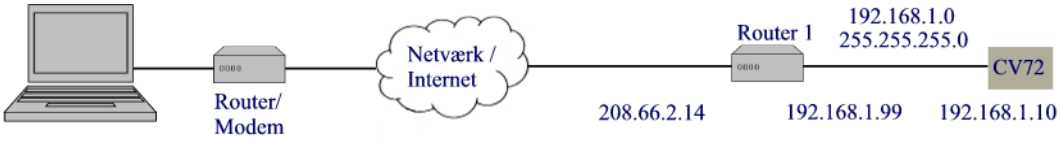
For at løse dette problem, kan der bruges en funktion i routeren som kaldes port mapping eller port forwarding. Port mapping er en funktion under NAT (Network Address Translation).

NAT giver mulighed for, at flere lokale IP-adresser kan deles om én offentlig IP-adresse, men her skal alle forbindelser startes af den lokale enhed.

Port mapping betyder, at udefra kommende trafik der sendes til routeren på en specifik port, altid videresendes til én specifik lokal IP-adresse, der vælges i routeren.

Routeren har altså en offentlig IP-adresse (WAN adresse), som bruges til at komme i kontakt med routeren. I routeren sættes port mapping op sådan, at når der kommer kommunikation til en bestemt IP-port på WAN-siden, oversættes den til en ny adresse på LAN-siden. Det er WAN adressen, der skal indtastes i Adgangseditoren.

Eksempel:



1. CV72 skal placeres i et "internt" netværk med netværksadresse 192.168.1.0 og netmaske 255.255.255.0.
2. Pc'en sidder i et andet netværk med en vilkårlig netværksadresse.
3. Router 1 har en offentlig WAN IP-adresse 208.66.2.14.
4. IP-adressen for lokaliteten i UniLock pc-programmet sættes så til 208.66.2.14 og port 7211
5. Port mapping i router 1 sættes sådan, at kommunikation der kommer til adresse 208.66.2.14 på port 7211 routes til den interne IP-adresse 192.168.1.10 på port 7211.

CV72 opsættes til:

- IP-adresse: 192.168.1.10
- Netmaske: 255.255.255.0
- Gateway adresse: 192.168.1.99
- Port: 7211

Gateway adressen skal være den gateway adresse som router 1 er konfigureret til. I eksemplet er det 192.168.1.99, men det kan være andre adresser, blot skal adressen være indenfor netværkets adresseområde.

I pc-programmet opsættes CV72 data til:

- IP-adresse: 208.66.2.14
- Port: 7211

Bemærk at den IP-adresse der opsættes i pc-programmet, ikke er den samme som den IP-adresse der opsættes for CV72.

2.4 Registrering af hostnavn i DNS-server

CV72 kan registrere sit hostnavn i en DNS-server (hostnavn.domæne). Dette giver mulighed for at tilgå CV72 med hostnavnet uden nødvendigvis at være på samme subnet som CV72.

Registrering af hostnavnet i DNS-serveren kan enten foretages automatisk af enheden eller manuelt af den IT-ansvarlig.

Vær opmærksom på, at det kan tage lang tid, før hele netværket er opdateret med tilføjelser og ændringer af navne. Korrekt rækkefølge er yderst vigtig for at minimere tiden, inden de korrekte navne er anvendelige.

Tiden, inden netværket er fuldt opdateret med ændringer skyldes, at svar fra en DNS-server gemmes (caches) af DNS-klienter (pc, mellemliggende DNS-servere og routere) i en given tid, hvorefter de automatisk slettes igen. Svarer en DNS-server, at det forespurgte DNS-navn ikke findes, gemmer DNS-klienter dette svar i en given tid, fra få sekunder til flere døgn afhængig af DNS-serverens konfiguration.

Dette betyder, at man skal være særligt opmærksom på, at navnet er registreret inden det anvendes af en pc, da der ellers kan gå yderligere tid, inden pc'en kan finde enheden.

Almindeligvis sænker man levetiden for svar (time to live) i DNS-serveren i god tid inden, der foretages ændringer. Ved at sænke levetiden, skal man vente kortere tid på, at ugyldige informationer udløber.

2.4.1 Automatisk registrering

CV72 kan automatisk registrere sit navn i en DNS-server (A-record). Til denne registrering er det nødvendigt at kende navnet på domænet. Hvis domænet ikke er angivet, eller ikke kan hentes gennem DHCP, er automatisk registrering ikke mulig.

Hentes IP-adressen automatisk via DHCP forsøger CV72 at foretages registreringen gennem DHCP-serveren (option 81). Er det ikke muligt at registrere gennem DHCP-serveren så forsøges det i stedet at foretage registreringen direkte i DNS-serveren.

Hvis der er angivet et domæne ved konfiguration af CV72 anvendes dette, alternativt bruges det domæne som DHCP-serveren angiver.

Anvendes en fast IP-adresse er det kun muligt, at registrere navnet direkte i DNS-serveren med det angivne domæne.

Registreringer direkte i DNS-serveren forudsætter at DNS-serveren tillader [Ikke sikrede dynamiske opdateringer] for den pågældende [Forward Lookup Zone].

Registrering foretages eller fornyes på baggrund af følgende kriterier:

- Ved opstart af enheden
- Ved ændring af enhedens opsætning.
- Ved fornyelse af dynamisk IP-adresse eller en gang i døgnet for en statisk IP-adresse.

2.4.2 Manuel registrering

Manuel registrering anvendes typisk hvis automatisk registrering ikke er muligt fx hvis DNS-serveren ikke tillader dynamiske opdateringer.

Ved manual registrering kan enheden ikke selv holde registreringen opdateret, og den IT-ansvarlige er derfor ansvarlig for dette. DNS-registreringen holdes nemmest korrekt opdateret ved, at tildele enheden en fast IP-adresse eller via statisk DHCP.

Vær opmærksom på, at enhedens statushjemmeside kun angiver status for registreringer, som enheden selv har anmodet om eller udført. Det vil sige, at statushjemmesiden i dette tilfælde vil angive fejl under registrering af hostnavn, da enheden ikke selv har kendskab til den manuelle registrering.

2.4.3 Test af DNS-registrering

For at teste registreringen i DNS-serveren kan bruges følgende fremgangsmåde:

1. Åbn statushjemmesiden med IP-adressen (http://ip-adresse) og verificer at det registrerede DNS-navn er korrekt.
2. Åbn hjemmesiden med DNS-navnet (http://hostnavn.domæne). Giver dette den samme statushjemmeside som i pkt. 1, er navnet registreret korrekt og klar til brug.
3. Indtast nu hostnavnet i UniLock programmet.

2.5 Kommunikation med andre enheder

Til kommunikation med andre IP-enheder (LS10-IP og CV72v2) anvendes multicast på IP-adresse 239.255.72.11, UDP-port 7211 med default TTL=2, hvorved enheder kan kommunikere på tværs af lokale netværk adskilt af max en router (forudsat korrekt router-konfiguration).

Anvender netværket IGMP snooping til at minimere netværkstrafik, skal der være konfigureret en IGMP querier til periodisk at sende forespørgsler om at opretholde multicast IP-adresse registreringer til IP-enheder. Dette er et krav i IGMP for at sikre at netværkstrafik altid routes korrekt. Det henvises til undervisningsmateriale for IGMP snooping.

En søgefunktionalitet findes på enhedernes hjemmesides fane [Find enheder], hvor søgningen kan synliggøre hvilke andre enheder, den enkelte enhed kan kommunikere med.

I større IT-installationer kan der være behov for at overstyre TTL-værdien hvis:

1. Enheder kan ikke finde hinanden pga. for mange routere mellem dem. TTL hæves.
2. Enheder kan finde hinanden få tværs af for mange routere. TTL sænkes.

Overstyring af multicast TTL gøres med en producentspecifik DHCP-option:

DHCP Vendor Class:	”UniLock” (Hexadecimal: 55 6E 69 4C 6F 63 6B)
Option Code:	1
Option Datatype:	1 byte
Option Value:	TTL-værdien (1-255)

2.6 Hjemmeside

LS10-IP har en indbygget hjemmeside, hvorfra man kan se status og søge efter andre enheder på Ethernet (CV72, LS10-IP) og RS485 (LS10-230V). Med hjemmesiden kan man således verificere at denne LS10-IP kan se andre enheder, samt finde andre enheders IP-adresse og ID-numre.

Adgang på standard web port 80 testes med web-browser ved at skrive IP-adressen for enheden (http://[adresse]).

Adgang på den valgte kommunikationsport testes med web-browser ved at skrive adressen og port-nummeret for enheden (http://[adresse]:[port]).

Er enheden placeret bag en router med port-mapping, kan der oprettes en http-forbindelse ved at skrive "http://[adresse]:[port]", hvor [adresse] angiver routerens adresse, og [port] angiver den port på routeren der er mappet til kommunikationsporten på enheden (default 7211).

2.7 Tilslutning

Diagram over tilslutning kan ses på Figur 1 og Figur 2.

CV72 kan forsynes af Power over Ethernet (PoE) eller af ekstern VDC forsyning.

Data

Funktioner:	DHCP (inkl. option 81), Statisk IP, Hostnavn, NetBIOS, DNS, TCP, UDP, ARP, HTTP, Ping, Firmware opdatering
Sikkerhed:	Rabbit 128bit-kryptering, HMAC, SipHash, Password
Netværk (J5):	10/100BaseT - RJ45

CV72

IP:	IPv4 (IPv6 forberedt), ikke galvanisk adskilt
Seriel (J1):	2-ledet RS485, half-duplex, galvanisk adskilt, transientbeskyttet
Forsyning ind:	
PoE/PoE+ (J5):	36-57 VDC (eget forbrug: 1,2W)
VDC (J6):	11-57 VDC (eget forbrug: 1,1W)
Størrelse:	160 x 80 x 39 mm, 209 g

CV72 Open Frame

IP:	IPv4 (IPv6 forberedt), galvanisk adskilt
Seriel (J1):	2-ledet RS485, half-duplex, ikke galvanisk adskilt, transientbeskyttet
Forsyning ind:	
PoE/PoE+ (J5):	36-57 VDC, 2,1W (eget forbrug)
VDC (J6):	7-34 VDC, 1,2W (50 mA@24V)
Forsyning ud ved (J6):	
PoE	24 VDC, max 8W (lige lidt nok til LS10)
PoE+	24 VDC, max 18W (anbefales til LS10)
Størrelse:	101 x 80 x 20 mm, 72 g

2.7.1 CV72 forsyning til eksterne enheder

Når CV72 Open Frame forsynes med Power over Ethernet, kan den levere fuld galvanisk adskilt 24 VDC til eksterne enheder. Effekten til rådighed for eksterne enheder afhænger af PoE typen, som CV72 tilsluttes.

Trækkes for meget effekt fra den router/switch som leverer PoE forsyningen vil den sandsynligvis lukke for power på den pågældende port. Nogle strømforsynende enheder kan konfigureres til automatisk at åbne for power igen efter en given tid.

Høje startstrømme kan få nogle strømforsynende enheder til at lukke for power. I de situationer frarådes det, at batterier og andre enheder med stor kapacitiv belastning forsynes på denne måde.

Test altid inden drift.

PoE type	PoE effekt (PSE)	PoE effekt (PD)	Effekt eksternt
PoE	15,4 W	12,9 W	Max 8 W
PoE+	30,0 W	25,5 W	Max 18 W

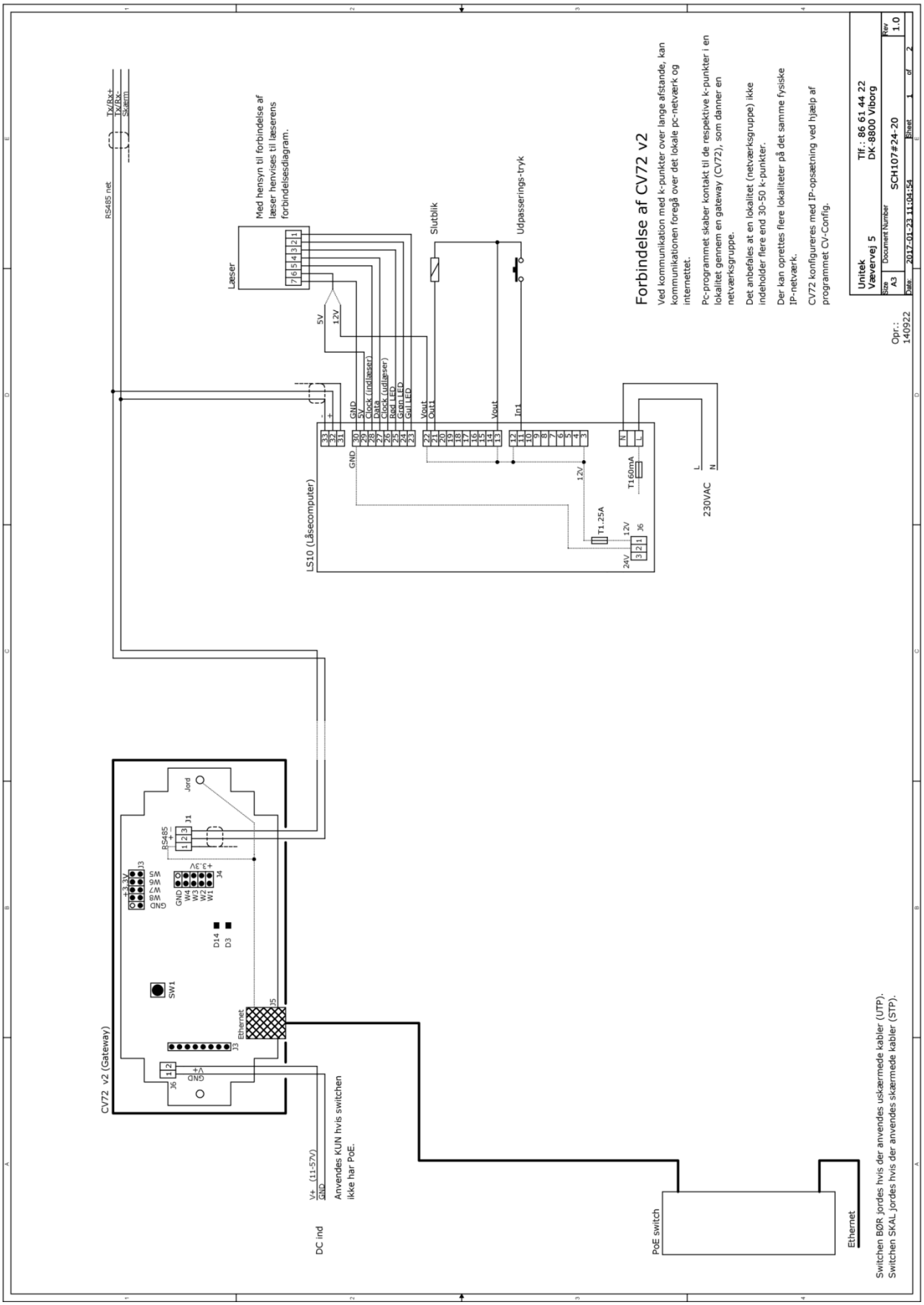
Som det ses af ovenstående tabel er der max ca. 8W (18 W) til rådighed for eksternt forbrug ud over enhedens egetforbrug (en LS10 låsecomputer har et egetforbrug på ca. 5 W). Forsynes en låsecomputer anbefales det, at anvende PoE+ for at have mest muligt effekt til rådighed.

2.7.2 Lysdioder

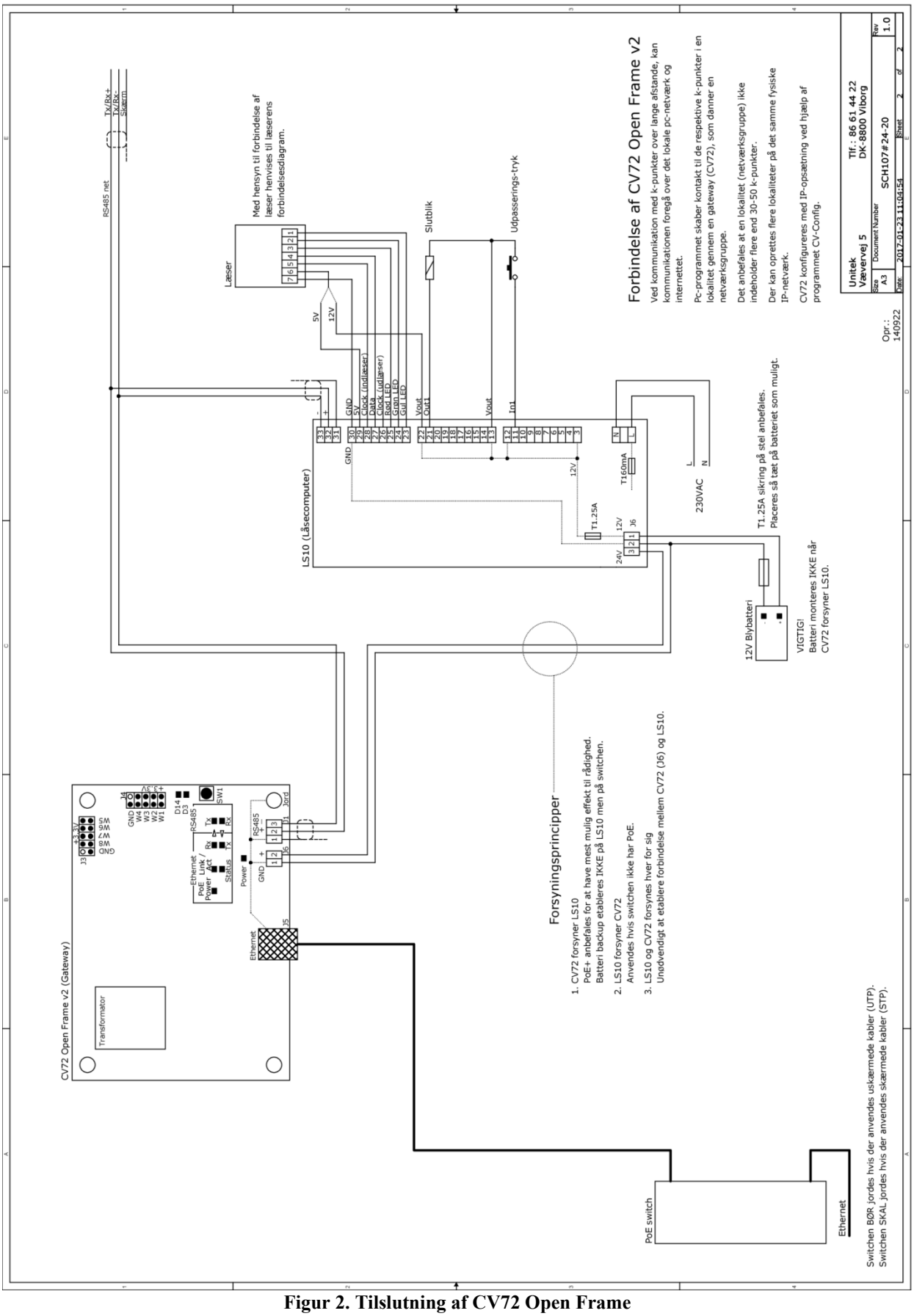
Lysdioderne viser driftsinformationer for enheden, som kan være en god hjælp ved installation og kontrol.

Lysdiode	Beskrivelse
[PoE Power] **D17**	Rød konstant Power over Ethernet forsyning tilsluttet.
[Power] **D9**	Rød konstant Forsyning tilsluttet.
[Status] **D8**	Grøn = 0,025 sek. Off = 0,025 sek. Softwareopdatering i gang. Grøn = 0,1 sek. Off = 2,9 sek. IP fejl/ IP ikke klar. Grøn = 0,5 sek. Off = 0,5 sek. Klar Grøn konstant Der er etableret en TCP/IP forbindelse til Polleren
[Ethernet Link/Act] **D10**	Off konstant Der er ikke en Link forbindelse. Grøn konstant Der er en Link forbindelse til Ethernet. Grøn = 0,025 sek. Off = 0,025 sek. Der er aktivitet på Ethernet, uanset om data er til denne enhed.
[Ethernet Rx] **D7**	Lyser når der modtages data fra Ethernet på den valgte IP-port
[Ethernet Tx] **D6**	Lyser når der sendes data ud på Ethernet på den valgte IP-port.
[RS485 Tx] **D5**	Lyser når der sendes data til RS485.
[RS485 Rx] **D4**	Lyser når der modtages data fra RS485.
D14	Off konstant CPU kører ikke. Grøn = 0,1 sek. Off = 0,1 sek. i 3 sek. Enhed er netop nulstillet efter 5 sek. tryk på knap. Grøn = 0,1 sek. Off = 0,4 sek. CPU kører korrekt med default opsætning. Grøn = 0,1 sek. Off = 1,9 sek. CPU kører korrekt.
D3	Anvendes ikke.

2.7.3 Forbindelsesdiagram



Figur 1. Tilslutning af CV72



Figur 2. Tilslutning af CV72 Open Frame

3. Test og fejlfinding

Ved idriftsættelse eller kommunikationsproblemer bør forbindelsen til og opsætning af CV72 verificeres.

I nogle af de efterfølgende afsnit skal enhedens adresse anvendes for at kontakte enheden. Feltet [adresse] kan være en af adressetyperne:

- IP-adresse i formatet "n.n.n.n"
- NetBIOS-navn i formatet "hostnavn"
- DNS-navn i formatet "hostnavn.domæne"

3.1 Test af forbindelse til CV72

Forbindelsen til CV72 kan testes med ping eller ved at åbne enhedens hjemmeside.

3.1.1 Hjemmeside

Adgang på port 80 testes med web-browser ved at skrive adressen for CV72 (http://[adresse]).

Adgang på den valgte kommunikationsport testes med web-browser ved at skrive adressen og portnummer for CV72 (http://[adresse]:[port]).

Er CV72 placeret bag en router med port-mapping, kan der oprettes en http-forbindelse ved at skrive "http://[adresse]:[port]", hvor [adresse] angiver routerens adresse, og [port] angiver den port på routeren der er mappet til kommunikationsporten på CV72 (default 7211).

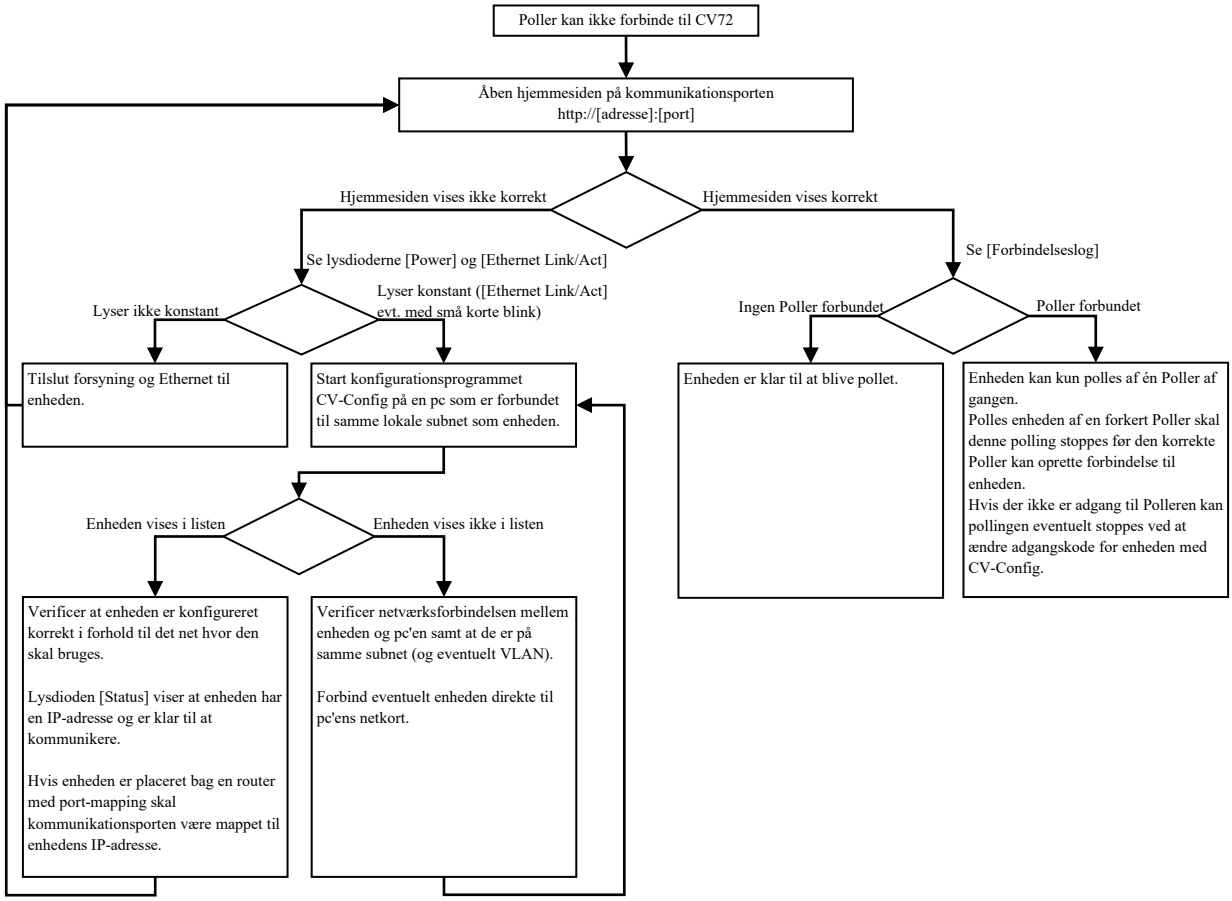
3.1.2 Ping

Start en kommandoprompt (”DOS vindue”) og skriv ”ping [adresse]” hvor [adresse] er adressen på CV72. Pinges et hostnavn vil Ping-kommandoen først oversætte dette til en IP-adresse, hvorefter den fundne IP-adresse anvendes.

Ping kan ikke anvendes til at teste forbindelsen til en enhed, hvis enheden er placeret bag en router med port mapping, da routeren selv vil svare på ping-forespørgsler.

3.2 Fejlfinding

Skulle der opstå problemer med kommunikation til CV72, er det vigtigt at gå systematisk frem for lettest at lokalisere fejlen.



Med hensyn til opsætning af routere, switche, firewalls mv., er opsætningen af disse helt forskellig fra fabrikat til fabrikat, så der henvises til den enkelte fabrikats brugervejledning.

3.3 Specielt om udskiftning af CV72

Hvis en CV72 skal udskiftes med en anden CV72, er der en række netværksmæssige udfordringer man skal være opmærksom på, for hurtigst muligt at få den nye CV72 i drift.

De følgende afsnit beskriver hvad man skal være særligt opmærksom på afhængigt, af hvordan CV72 adresseres i fx UniLock.

Adresseret med IP-adresse

Bruger den nye CV72 samme IP-adresse som den tidligere CV72, skal alle involverede pc'er, routere, mv. have deres ARP-tabeller opdateret.

ARP-tabellen bruges til at bestemme en MAC-adresse ud fra en IP-adresse.

Det er essentielt for korrekt kommunikation, at ARP-tabellen er opdateret, da al kommunikation på et Ethernet foregår ved hjælp af MAC-adresser og ikke ved hjælp af IP-adresser.

Routere, pc'er mv. vil normalt automatisk holde deres ARP-tabeller opdateret. Afhængig af deres opsætning kan der gå fra få sekunder til flere timer, før de opdaterer deres ARP-tabeller.

Hvis man ikke ved hvordan ARP-tabellen skal fornys i routere mv., må man vente til de automatisk opdaterer. På en pc kan ARP-tabellen tvangsopdateres ved at slettes tabellen med kommandoen ”arp -d” skrevet i kommandoprompten.

Alternativt kan den nye CV72 tildeles et andet IP-nummer, hvis IP-nummerplanen tillader dette.

Adresseret med hostnavn

Hvis den nye CV72 bruger samme hostnavn (NetBIOS-navn eller DNS-navn) som den tidligere CV72, og de ikke anvender samme IP-adresse, skal man være opmærksom på, at pc'en gemmer disse informationer i en cache i en given tid. Det betyder, at et gemt navn vil referere til den gamle IP-adresse og ikke den nye.

Hvis man ikke har adgang til at opdatere cachen lokalt, og i eventuelle mellemliggende DNS-servere, sker det automatisk efter en given tid. Det vil typisk ske indenfor 20 min, men det afhænger af pc'ens konfiguration.

Den lokale cache kan manuelt tømmes for hostnavne ved at skrive en kommando i kommando-prompten. Kommandoen for at fjerne NetBIOS-navne er "nbtstat -R" og kommandoen for at fjerne DNS-navne er "ipconfig /flushdns".

Vær dog opmærksom på, at mellemliggende DNS-servere ligeledes vil gemme navnet i deres cache, hvorved vi vil få det samme gamle IP-adresse.

Alternativt kan den nye CV72 gives samme hostnavn og IP-adresse som den tidligere CV72, eller bare gives et andet hostnavn, hvorved disse problemstillinger elimineres.

Da et hostnavn relaterer til en IP-adresse kan det være nødvendigt at opdatere ARP-tabellen som beskrevet i forrige afsnit.

3.4 Nulstilling af opsætning

Adgangskoden (adgangsnøglen) nulstilles ved et kort tryk på knappen [SW1] på CV72’s print.

Opsætningen kan nulstilles til fabriksindstilling, hvis knappen holdes nede i 5 sekunder indenfor de første 30 sekunder efter power-opstart.

Lysdioden D14 vil blinke (Grøn = 0,1 sek. Off = 0,1 sek.) i 3 sek. efter nulstilling af opsætning.

4. Sikkerhed

Dette afsnit beskriver overordnet hvordan kommunikation til og fra enheden beskyttes.

4.1 Netværkssikkerhed

For at sikre dataintegriteten, forhindre manipulation af data, replay af strenge og hijacking af enheder, er de vitale dele af kommunikationen sikret ved hjælp af kryptering og adgangskode.

Udover adgangskode og krypteringsnøgle anvendes yderligere en offentligt nøgle til overførsel af krypteringsnøglen i forbindelse med opstart af en enhed, dog kun hvis adgangskoden ikke allerede er sat i enheden.

For at forstærke krypteringen anvendes en ændringsnøgle i krypteringen. Populært sagt kan man sige, at ændringsnøglen sammen med krypteringsnøglen gør, at den samme krypteringsnøgle aldrig anvendes igen.

For at forhindre replay af en datastreng indsættes en tidskode (challenge), som krypteres i selve datastrengen.

For at verificere at en streng er dekrypteret korrekt, og at der ikke er manipuleret med data, beregnes et kryptografisk hashtal af alle data. Dette hashtal kan betragtes som en digital underskrift, der verificerer autenticiteten af en given datastreng.

4.1.1 Algoritmer

Til kryptering anvendes krypteringsalgoritmen Rabbit. Rabbit er en stream krypterings-algoritme med en 128 bit nøgle og en 64 bit ændringsnøgle (initialiseringsvektor). Ændringsnøg-len sikrer, at den samme streng krypteres forskelligt, hver gang den sendes.

Til integritetstjek anvendes en HMAC (Hash-based Message Authentication Code). Denne HMAC genereres vha. algoritmen SipHash, som er en kryptografisk 128 bit nøgleafhængig hash-algoritme (HMAC) der genererer et 64 bit hashtal. Dette hashtal er at betragte som en digital underskrift.

Begge overnævnte algoritmer anses for at være ubrydelige, og har ingen kendte svagheder. Et brute-force angreb mod en 128 bit symmetrisk krypteringsalgoritme vil ikke være praktisk muligt med nutidens computerteknologi, så det vil tage et par fantasiliarder år at prøve dem alle.

4.1.2 Adgangskode/adgangsnøgle

Ud fra brugerens adgangskode beregnes en adgangsnøgle i form af et hashtal, som efterfølgende anvendes og lagres i enhederne. Altså: Adgangskoden opbevares ikke i enheden eller sendes til enheden.

Adgangsnøglen bruges kun for at forhindre, at uautoriserede personer kan ændre i opsætningen af enheden, fx via pc-programmet CV-Config. Ligeledes beskytter adgangsnøglen mod, at en anden Poller kan overtage enheden (hijacking).

Altså: Adgangsnøglen låser enhederne til dette netværk, så enhederne ikke kan flyttes til et andet netværk uden at adgangsnøglen nulstilles eller videregives. Selv om der ikke er en adgangsnøg-le, så kan Polleren udmærket oprette en sikker krypteret kommunikationsforbindelse til enheden.

Et kort tryk på en knap i enheden nulstiller adgangsnøglen.

4.1.3 Krypteringsnøgle

Krypteringen sikrer, at data ikke kan aflyttes, og at data når sikkert og umanipuleret frem til enheden.
Krypteringsnøglen er den symmetriske nøgle, der anvendes af Polleren og enheder under normal drift.

4.1.4 Offentlig nøgle

Den offentlige nøgle anvendes kun i initialiseringsfasen til at kryptere overførslen af den første symmetriske krypteringsnøgle eller adgangsnøgle. Den offentlige nøgle anvendes ikke, og kan ikke anvendes, når der er sat en adgangsnøgle i enheden.

4.1.5 Ændringsnøgle

Formålet med ændringsnøglen (nonce) er at sikre, at de samme data aldrig giver samme krypterede resultat. Populært sagt kan man sige, at ændringsnøglen sammen med krypterings-nøglen gør, at den samme krypteringsnøgle aldrig anvendes igen.

4.1.6 Tidskode

For at forhindre replay af data indeholder hver streng en tidskode (challenge). Når den anvendte challenge er en tidskode, kan data overføres direkte uden forudgående kommunikation til overførsel af en challenge.
At anvende en tidskode som challenge giver endvidere mulighed for at anvende broadcast.
Hvis tiden i enheden ikke er kendt, eller den er ude af synkronisering, kan man bede enheden om at oplyse dens tid (challenge).

4.1.7 Integritetstjek

For at verificere at data er konsistente, indeholder strengen en digital underskrift i form af et kryptografisk hashtal (HMAC). Dette tal sikrer, at strengen er sendt fra en afsender, der er tillid til, og at der ikke er manipuleret med indholdet. Hashtallet beregnes ved hjælp af en kryptografisk nøgleafhængig hash-algoritme på baggrund af hele datastrengen. Altså: Såvel af den krypterede som den ukrypterede del.
Hashtallet krypteres efterfølgende ind i den krypterede del af datastrengen.

4.1.8 Reset knap

I enheden findes en trykknap. Ved et kort tryk nulstilles adgangsnøglen i enheden (altså ikke krypteringsnøglen).
Efterfølgende vil Polleren automatisk tildele enhederne den korrekte adgangsnøgle igen.