

# UniLock

## System 10

### Manual

### Windows-program

Projekt	PCS125
Version	2.0
Revision	2024-05-10

UniLock programmet er et Windows baseret pc-program til at oprette og vedligeholde et adgangskontrolsystem. UniLock programmet varetager den administrative del af adgangskontrollen, og kommunikerer med alle kontrol-punkterne via Ethernet eller et lokalt RS485 netværk, hvortil forbindelsen etableres via pc'ens USB-port, COM-port, telefonmodem eller pc-netværk/internettet.

Manualen giver en overordnet beskrivelse af systemet, og beskriver installationsproceduren for programmet. For en supplerende beskrivelse af, hvordan de enkelte programmoduler anvendes, henvises tillige til særskilte manualer, som også er inkluderet i programmet.

# Indholdsfortegnelse

- 1. Introduktion..... 4**
  - 1.1 Generel systembeskrivelse .....4
  - 1.2 Forudsætninger.....4
  - 1.3 Program .....5
  
- 2. Definitioner og begreber ..... 7**
  - 2.1 Indledning.....7
  - 2.2 Definitioner .....7
  
- 3. Adgangseditor ..... 11**
  - 3.1 Beskrivelse .....11
  - 3.2 Generelt for alle objektvinduer.....11
  - 3.3 Login/ud .....12
  - 3.4 Personer.....14
  - 3.5 Grupper.....17
  - 3.6 Tidstabeller.....18
  - 3.7 Sikkerhedsniveautidstabeller.....20
  - 3.8 Specialdagskalendere .....23
  - 3.9 Delte undtagelser.....25
  - 3.10 K-punkter .....26
  - 3.11 DAS-grupper .....39
  - 3.12 Lokalteter .....41
  - 3.13 ID-kort design og produktion.....44
  - 3.14 Videoserver og kamera.....45
  - 3.15 Områder.....47
  - 3.16 Operatører.....48
  - 3.17 Operatørgrupper .....50
  - 3.18 Integrationer (Import/Eksport) .....52
  - 3.19 Licens .....53
  - 3.20 Systemoversigt .....55
  - 3.21 Logsøgning.....56
  - 3.22 Poller .....58
  - 3.23 Alarmoversigt.....62
  - 3.24 K-punkt oversigt.....63
  - 3.25 Tyverialarmstyring .....67
  - 3.26 Videoafspilning .....68
  - 3.27 Web-Adgangseditor.....69
  - 3.28 Områdevisning .....72
  - 3.29 Øvrige indstillinger.....73

---

<b>4.</b>	<b>Programmoduler .....</b>	<b>74</b>
4.1	Indledning.....	74
4.2	Modul oversigt.....	74
4.3	Modul beskrivelser .....	75
<b>5.</b>	<b>Licens.....</b>	<b>88</b>
5.1	Indledning.....	88
5.2	Licensbestilling.....	88
5.3	Ansvarsfraskrivelse .....	89
<b>6.</b>	<b>Installation / opdatering.....</b>	<b>90</b>
6.1	Indledning.....	90
6.2	Forudsætninger .....	90
6.3	Systemkrav .....	90
6.4	Installationsprogram .....	92
6.5	Netværksinstallation .....	93
6.6	Database .....	94
6.7	Efter installation .....	96
6.8	Opdatering .....	97
6.9	Aktivering af licens .....	97
6.10	Programfejl.....	97
<b>A.</b>	<b>Backup af data.....</b>	<b>99</b>
<b>B.</b>	<b>Lysdiode i læser.....</b>	<b>101</b>

# 1. Introduktion

## 1.1 Generel systembeskrivelse

UniLock system 10 er et pc-styret adgangskontrolsystem til at begrænse hvem der har adgang hvor og hvornår, og til registrering af hvem der kommer og går i fx en virksomhed.

### Decentralt system

Ved hver dør (k-punkt) sidder en låsecomputer. Låsecomputerne kommunikerer med pc'en på netværk eller via konverter til 2-ledet kabel (RS485, som kan være op til flere kilometer langt).

Alle parametre til styring af adgangskontrollen ligger decentralt i låsecomputerne. Det betyder, at systemet stadig fungerer, selv om pc'en bryder ned eller kommunikationsnettet afbrydes.

Decentral styring er ligeledes en fordel, hvis nogle k-punkter er placeret i en ekstern lokalitet, disse k-punkter kan så fungere helt selvstændigt uafhængig af pc'en. Når disse k-punkter skal opdateres, eller loggen skal tømmes, kan de fx via et modem sættes i forbindelse med pc'en.

Pc'en skal dog være i forbindelse med låsecomputerne, hvis der benyttes pc-styret alarm, områdevisning, transaktionsregistrering, bookinger og andre realtidsfunktioner.

## 1.2 Forudsætninger

Formålet med denne manual er at give brugeren et overblik over funktionerne i UniLock, og forberede brugeren på at anvende og installere pc-programmet til UniLock.

Erfaringen viser, at en god start og et godt "fundament" holder i mange år og giver mindre administrativt arbejde i længden.

### Sikkerhedspolitik

Programmet er et værktøj til administration af firmaets sikkerhedspolitik, programmet kan ikke give firmaet en sikkerhedspolitik. Derfor er det vigtigt at firmaets sikkerhedspolitik defineres før indtastning af programdata starter.

Sikkerhedspolitikken må derfor indeholde "hvem har adgang til hvilke døre og hvornår", og "hvilket sikkerhedsniveau skal hver dør anvende på forskellige tidspunkter".

Som det ses, kan leverandøren eller programmet ikke løse disse opgaver, men bør være specificeret af installationsstedets sikkerhedsansvarlige før programmet tages i brug.

Skriftet "Skemaer og eksempler til adgangskontrol" bør læses, og medfølgende skemaer bør være udfyldt før indtastning af programdata.

### Programinstallatøren

Programinstallatøren bør have et indgående kendskab til adgangskontrolsystemets opbygning og funktionalitet. Endvidere kræves det at programinstallatøren har et større kendskab til Windows end dagligdagsbrugeren. Skal programmet installeres i netværk, skal program-

installatøren have et indgående kendskab til det benyttede netværk. En netværksinstallation bør altid laves i samarbejde med installationsstedets IT-ansvarlige.

### **Operatøren**

Det forudsættes at operatøren har et indgående brugerkendskab til Windows, og er bekendt med normale udtryk og begreber indenfor Windows. Det falder uden for denne manuals rammer at undervise brugeren i grundlæggende Windows-funktioner – her må henvises til Microsofts manualer.

### **Definitioner og begreber**

Det anbefales at læse afsnittet ”Definitioner og begreber”, der beskriver betydningen af ord og vendinger, som er specielt for dette adgangskontrolsystem, og som må formodes at være nye ord for brugeren.

### **Pc-udstyr**

Der stilles selvfølgelig visse tekniske krav til det pc-udstyr der skal bruges, men mange af de krav er igen afhængig af en selv – hvor tålmodig er jeg? Hvor længe vil jeg vente før skærmen er opdateret? Hvor stor en skærm kræver jeg? Hvilket operativsystem skal anvendes? mv.

Generelt kan siges, at det anbefales at købe den pc der var topmodellen for ½ år siden, da den kan erhverves for en rimelig pris sammenlignet med tidens topmodel. Dog må et minimumskrav være en god skærm med stor opløsning. Se afsnittet ”Installation” for yderligere informationer.

### **Sikkerhed**

Adgangskontrolsystemets formål er at beskytte udvalgte områder mod uønsket indtrængen, men et system er ikke stærkere end det svageste led. Derfor er det selvfølgelig også vigtigt, at sikre den pc hvorpå programmet er installeret. Har man fuld kontrol over pc og UniLock programmet, har man reelt fuld kontrol over alle adgangsveje i bygningerne. Derfor bør pc'en placeres et sikkert sted og beskyttes med login, endvidere bør programmet beskyttes med adgangskode.

Det anbefales at oprette en ekstra systemoperatør med alle rettigheder. Denne ”Ny systemadministrator” bruges så i dagligdagen som systemoperatør. Gem derefter [Login navn] og [Adgangskode] for operatøren ”Systemadministrator” i en bankboks og brug kun denne operatør i nødstilfælde.

## **1.3 Program**

Pc-programmet er ét samlet program. Administration foregår i AdgangsEditor, data gemmes i en database, mens kommunikation varetages af PollerService (Windows Service).

Adgangseditoren er den del, som dagligdags-brugeren stifter bekendtskab med. I Adgangseditoren oprettes k-punkter (døre), personer, tidstabeller mv. og udføres overvågning, efterforskning og styring.

I Adgangseditoren findes en række andre programmoduler, som udfører specielle opgaver, se afsnittet for det pågældende programmodul for nærmere oplysninger.

## **Manualer**

Manualer kan læses ved at vælge menuen [Hjælp]. For at manualen altid skal være lige ved hånden, og for at manualen altid skal passe til den pågældende softwareversion/revision, findes programmanualerne ikke på papir. Såfremt manualen ønskes på papir, kan de ønskede kapitler udskrives.

## **Licens**

For at anvende programmet lovligt, skal der erhverves licens til de programmer og programmoduler, det ønskes at anvende. Programmerne er indrettet således, at licensen midlertidigt kan sættes ud af drift, hvis det ønskes at se eller teste programmer eller programmoduler, der endnu ikke er erhvervet licens til. Læs venligst afsnittet ”Licens”.

## **Backup**

Der bør med jævne mellemrum tages sikkerhedskopi af databasen, specielt før og efter der laves større ændringer. En backup bør altid gemmes et andet sted, end i det rum hvor pc'en er placeret og helst uden for huset. Backup-generering opsættes i Adgangseditor [Indstillinger], [Database], [Backup].

En udskrift specielt af alle personer kan også være en god løsning. Det vigtigste er at have nøglekoderne til alle personer. Ud fra disse nøglekoder vil det ved hårdt arbejde være muligt tilnærmelsesvis at rekonstruere databasen, uden at skulle have fat i alle personer og låne deres nøgle for at genindlæse nøglekoden.

## **Programmet**

Windows programmet til UniLock systemet er en naturlig videreudvikling af det ”gamle” DOS program, som har eksisteret siden 1993. UniLock systemet anvendes i mere end 3000 installationer med i alt over 60.000 døre. Program (og alt hardware) er 100 % dansk udviklet og derfor specielt tilpasset dansk behov og mentalitet. Windows programmet repræsenterer i dag en udviklingsindsats på mere end 170.000 timer (110 årsværk) og over 800.000 programlinjer, og videreudviklingen vil fortsætte, således at programmets funktionalitet løbende udbygges og tilpasses nye Windows operativsystemer.

## **Programfejl**

Der er gjort meget for at teste programmet og for at finde de fejl der evt. måtte være i programmet. Alligevel kan der være fejl i programmet som endnu ikke er opdaget. Hvis der opdages fejl, vil vi selvfølgelig gerne høre det. For at kunne rette fejlen, skal den kunne reproduceres. Det vil i de fleste tilfælde ikke være muligt at rette fejl der ikke kan reproduceres.

Alvorlige fejlrettelser har første prioritet i vores udviklingsafdeling, og derfor vil mange fejl også blive rettet med det samme, således at der i løbet af få dage er en ny release klar.

## 2. Definitioner og begreber

### 2.1 Indledning

I dette afsnit beskrives de ord og vendinger som er specielt for dette adgangskontrolsystem, og som formodes må være nye ord for brugeren.

### 2.2 Definitioner

#### Dato- og tidsformat

Dato og tid skrives de fleste steder alt efter hvordan Windows er opsat. Nogle steder er formatet dog fast og datoen skrives i henhold til Dansk Standard DS/ISO 8601 som ÅÅÅÅ-MM-DD. Hvis det fx er den 22. august 2019, skrives datoen som 2019-08-22, evt. 190822. Tiden angives som HH:MM:SS fx 10:27:42. Nogle steder angives der ikke sekunder, og tiden angives derfor som HH:MM, altså blot 10:27.

#### K-punkt

K-punkt er en forkortelse for kontrolpunkt, altså et punkt hvor der er kontrol af, hvem der kan passere og hvornår. Hvert k-punkt er styret af en decentral låsecomputer.

Et k-punkt behøver ikke være en dør, men kan også være fx er bom, port, turnstile ("per-sillehakker"), elevator mv.

#### ID-nummer

Alle k-punkter i et system anvender et kommunikationsnet som kan være Ethernet eller RS485. For at pc'en kan kommunikere med hver enkelt, skal de hver have et entydigt firecifret ID-nummer. ID-nummeret tildeles låsecomputeren med en Loader, eller det indtastes på kortlæseren i de første 20 sekunder efter at låsecomputeren er tændt (tast "\*nnnn#", hvor "nnnn" = ID-nummer). Alternativt kan låsecomputerne bestilles med ID-nummer. Ved oprettelse af et k-punkt skal dette ID-nummer angives.

#### Lokalitet

En lokalitet er et antal k-punkter der har forbindelse med hinanden på det samme kommunikationsnet.

Hvis der er langt til nogle k-punkter, kan disse derfor oprettes i en eller flere særskilte lokaliteter, hvor de enkelte k-punkter i hver lokalitet er koblet på samme kommunikationsnet. Forbindelsen til en lokalitet etableres med en gateway, som kan være USB, modem over telefonnettet (analog eller GSM) eller med COM Server (CV72, LS10-IP) over et IP-netværk (pc-netværk og/eller internettet). Systemet kan opsættes, så pc'en automatisk opretter forbindelse til disse lokaliteter på forskellige tidspunkter.

#### Person

En person er som navnet siger en person, men det kan dog også være andre former for nøgleindehavere. Fx kan en bil have adgang, uafhængig af hvem der kører i den, og bilen oprettes så som en person.

En person kan have op til fire nøgler, som fx en normalnøgle og en reservenøgle.

## Nøgle

En nøgle er det, der får låsecomputerne til at oplåse døren. Det kan være forskellige typer, ofte en berøringsfri brik. Det kan også være et magnetkort, et trådløst kort eller ID-brik (RFID, Mifare), Dallas Touch Memory, chipkort, radiosender, telefon, bilbrik, nummerplade mv.

## Gruppe

For at gøre det lettere at oprette og vedligeholde systemet, er der mulighed for at have grupper. Grupper er en samling af adgangsrettigheder til k-punkter. Det kan være k-punkter, der giver adgang til samme område, eller det kan være k-punkter som en bestemt personalegruppe har adgang til.

## Sikkerhedsniveau

Et k-punkt er altid på et sikkerhedsniveau. Sikkerhedsniveauet er bestemmende for, hvor stor sikkerheden er mod passage af et k-punkt. Jo højere sikkerhedsniveauet er, desto bedre er k-punktet sikret.

Følgende sikkerhedsniveauer kan anvendes:

- 0.0 Konstant oplåst (kan ikke låses med normal nøgle).
- 0.1 Konstant oplåst efter anvendelse af første nøgle.
- 1.0 Nøgle eller PIN-kode (skiftefunktion, starter med oplåst).
- 1.1 Nøgle eller PIN-kode (skiftefunktion, starter med låst).
- 1.2 Nøgle eller PIN-kode (oplåst i tid).
- 2.0 Gyldig nøgle (skiftefunktion, starter med oplåst).
- 2.1 Gyldig nøgle (skiftefunktion, starter med låst).
- 2.2 Gyldig nøgle (oplåst i tid).
- 3.0 Nøgle + PIN-kode (skiftefunktion, starter med oplåst).
- 3.1 Nøgle + PIN-kode (skiftefunktion, starter med låst).
- 3.2 Nøgle + PIN-kode (oplåst i tid).
- 4.0 Konstant låst efter anvendelse af første nøgle + PIN.
- 4.1 Konstant låst (kan ikke oplåses med almindelig nøgle).

## Sikkerhedsniveautidstabel

En sikkerhedsniveautidstabel er en række tider (op til 32), der bestemmer, hvornår et k-punkt skal skifte sikkerhedsniveau, og til hvilket niveau det skal skifte.

## Default sikkerhedsniveau

Hvis et k-punkt ikke har modtaget den sikkerhedsniveautidstabel som den skal anvende, er den på default sikkerhedsniveau. K-punktet er også på default sikkerhedsniveau, hvis der ikke anvendes nogen sikkerhedsniveautidstabel, den anvendte tabel er tom, eller uret ikke går.

## Tidstabel

En tidstabel indeholder op til 16 tidsperioder. En nøgle kan individuelt i hvert k-punkt anvende én af 50 forskellige tidstabeller.



Andre funktioner kan også anvende tidstabellerne. Fx kan en udgang følge en tidstabel, så den er aktiv i de perioder, der er angivet i tabellen.

## Undtagelse

Normalt gentager en tidstabel og sikkerhedsniveautidstabel sig selv uge efter uge, men i visse situationer kan det være ønskeligt at bryde denne monotoni. En undtagelse består af en tidsperiode, hvor der anvendes en anden valgbar funktion end den, der er angivet i tidstabellen.

Undtagelser er et kraftigt supplement til specialdagskalenderen. Modsat specialdage, der varer hele døgn, varer undtagelser i en valgbar tidsperiode.

## Specialdagskalender

Specialdagskalendere indeholder informationer om, hvilke dage der ikke er normale ugedage, fx helligdage, 1. maj, lang lørdag, åbent hus mv.

Der kan anvendes følgende angivelser i kalenderen:

- 0 Normal ugedag. Der er ingen afvigelse fra normalkalenderen.
- 1-7 Anvendes, hvis der skal benyttes en anden ugedag end den aktuelle. Hvis der fx anvendes "søndags drift" på helligdage, skrives 7 ud for disse dage (1=mandag, 7=søndag). Eller der kan måske anvendes "lørdags drift" (dag 6) 1. maj, 24. december osv.
- A-F Bruges, når der skal anvendes en af de fiktive specialdage A-F.

En fiktiv specialdag anvendes, hvis ingen af de andre dage (1-7) kan anvendes på den ønskede dato.

Hvis der fx skal anvendes helt specielle adgangskriterier den første lørdag i måneden, skrives fx "A" ud for første lørdag i hver måned.

I hver sikkerhedsniveautidstabel defineres det sikkerhedsniveau, som døren skal være på den aktuelle specialdag. Ligeledes bestemmes via tidstabellerne, hvem der har adgang på de enkelte specialdage, og hvornår.

Ved afslutning af en specialdag skiftes til sikkerhedsniveauet for den efterfølgende dag.

Sikkerhedsniveautidstabellen indeholder tider for skift til et andet sikkerhedsniveau, men hvis sikkerhedsniveautidstabellen ikke indeholder skift for den specialdag der anvendes, vil døren forblive på det sikkerhedsniveau den var på, før specialdagen startede kl. 00:00:00.

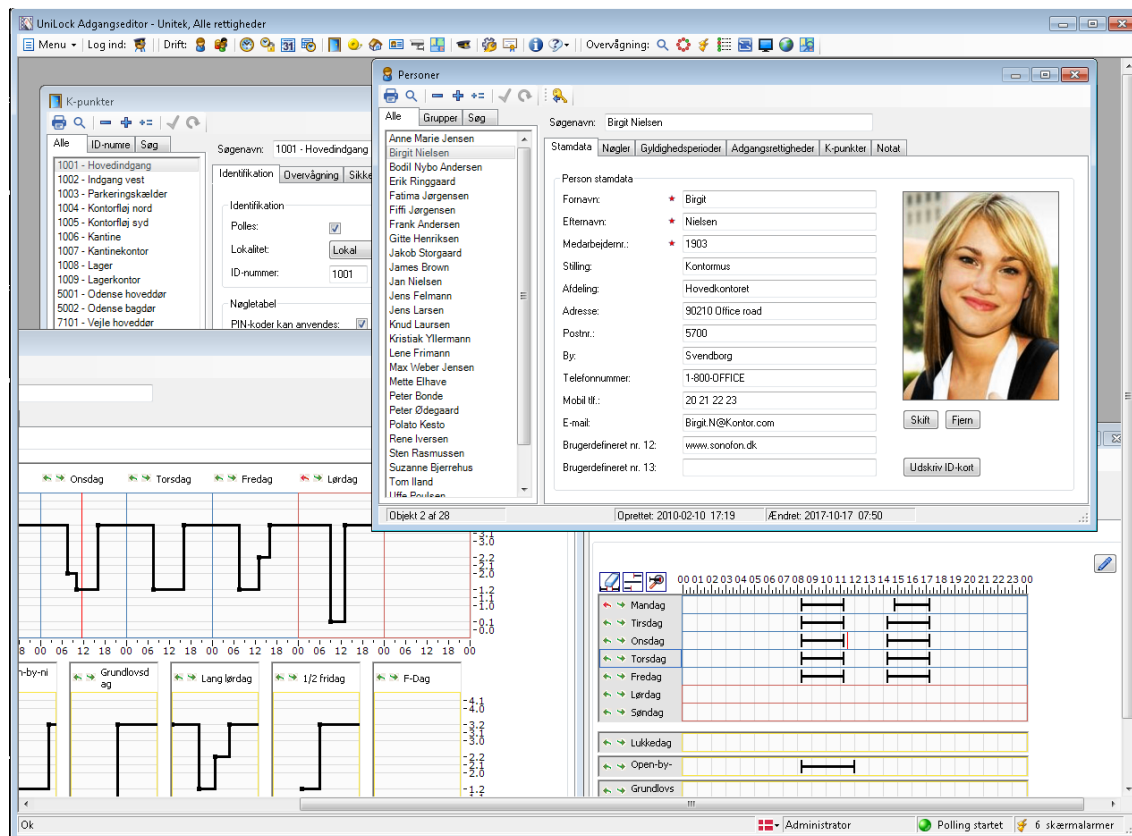
Hvis personer skal have adgang på specialdage, skal deres respektive tidstabeller indeholde adgangsperioder for specialdagen for at de kan oplåse døren. Desuden skal andre tidstabeller der anvendes på specialdage også indeholde perioder for specialdagen.

## **Pollingslog**

Pc-programmet henter hele tiden logninger i k-punkterne og gemmer dem på harddisken. Denne log indeholder, afhængig af opsætning, information om de hændelser der er sket ved k-punkterne og de hændelser som pc-programmet har lavet fx opdatering af k-punkter.

Denne log indeholder også skærmalarmer som er genereret af enten k-punkterne eller programmet.

## 3. Adgangseditor



### 3.1 Beskrivelse

Adgangseditoren er administrationsprogrammet, og er det program dagligdagsbrugeren primært stifter bekendtskab med. I programmet oprettes k-punkter (døre), personer, tidstabeller mv. Adgangseditoren kan afvikles på alle pc'er i et netværk, og flere Adgangseditorer kan afvikles på samme tid. De ændringer operatøren via Adgangseditoren foretager i databasen, vil Polleren automatisk sende til k-punkterne.

Programmet indeholder et stort arbejdsområde hvorpå der samtidigt kan åbnes mange objektvinduer, som hver især kan skaleres til den ønskede størrelse. Da der kan være mange objektvinduer åbne på samme tid, er det en fordel med en stor skærm med en høj opløsning.



I toppen af programvinduet er der en værktøjslinje med ikoner, og herfra kan alle objektvinduer og nogle dialogbokse startes. Efterfølgende beskrives objektvinduer og dialogbokse i den rækkefølge ikonerne er placeret på værktøjslinjen. Knappen [Menu] viser alle ikoner med tilhørende navn.

### 3.2 Generelt for alle objektvinduer

Hvert objektvindue opfører sig næsten som et selvstændigt Windows program, der hver især kan åbnes og lukkes, skaleres og minimeres. I venstre side af objektvinduet er en liste over alle de objekter (personer, k-punkter, tidstabeller mv.), der kan arbejdes på i det pågældende

objektvindue. Når objektvinduet lukkes, vil størrelse og placering blive husket til næste gang det åbnes af den samme operatør.

I alle objekter lige efter objekts navn, er angivet to tidspunkter for henholdsvis objektets oprettelse og for den sidste ændring. Disse tidspunkter kan være en nyttig oplysning i forbindelse med dokumentation af, hvornår et objekt er oprettet/ændret.

For alle objektvinduer gælder, at ændringer først gemmes i databasen, når ikonet for [Gem] aktiveres. Fortryder operatøren de ændringer der er lavet, aktiveres ikonet [Genindlæs] og data fra databasen genindlæses.

### Bruges af

Flere objektvinduer indeholder fanebladet [Bruges af] hvor der oplyses, hvilke andre objekter der bruger det pågældende objekt. Denne information kan være meget nyttig at kigge på, før der foretages ændringer i objektet, da en ændring vil påvirke funktionen af de objekter, der bruger det pågældende objekt. Før der fx ændres i en tidstabel, kan det være en god ide at kigge på fanebladet [Bruges af], for at se hvilke andre objekter, der bruger den pågældende tidstabel, da en ændring af tidstabellen vil påvirke alle de objekter, der bruger tidstabellen.

### Notat

Alle objektvinduer indeholder fanebladet [Notat], hvor det er muligt at skrive private notater og kommentarer til hvert enkelt objekt.

### Udskrivning

Ønskes der udskrift af et objekt, vælges det pågældende objekt i objektvinduet og printerikonet aktiveres. I udvalgte objektvinduer kan der skrives til CSV-fil.

## 3.3 Login/ud

Der kan oprettes et ubegrænset antal operatører i programmet, som hver kan tildeles individuelle operatørrettigheder. Hver operatør logger ind med eget operatørnavn og adgangskode. Der logges ud ved at aktivere ikonet [Log ind/ud], eller ved at afslutte Adgangsedatoren. Når der logges ud lukkes alle objektvinduer, og deres størrelse og placering huskes til næste gang den pågældende operatør logger ind igen.

Under Operatøren "Systemadministrator" kan operatørmodulene aktiveres eller deaktiveres.

The image shows a login dialog box titled "UniLock Adgangseditor login". It contains the following fields and controls:

- Godkendelse:** A dropdown menu with the selected option "Windows-godkendelse (aktuelle bruger)".
- Brugernavn:** A text input field containing "UNITEK\FLB".
- Adgangskode:** A text input field with masked characters (dots).
- Auto-logon:** An unchecked checkbox.
- Below the input fields are two buttons: "Skift adgangskode" and "Glemt adgangskode".
- At the bottom are two buttons: "OK" (highlighted with a blue border) and "Annuller".

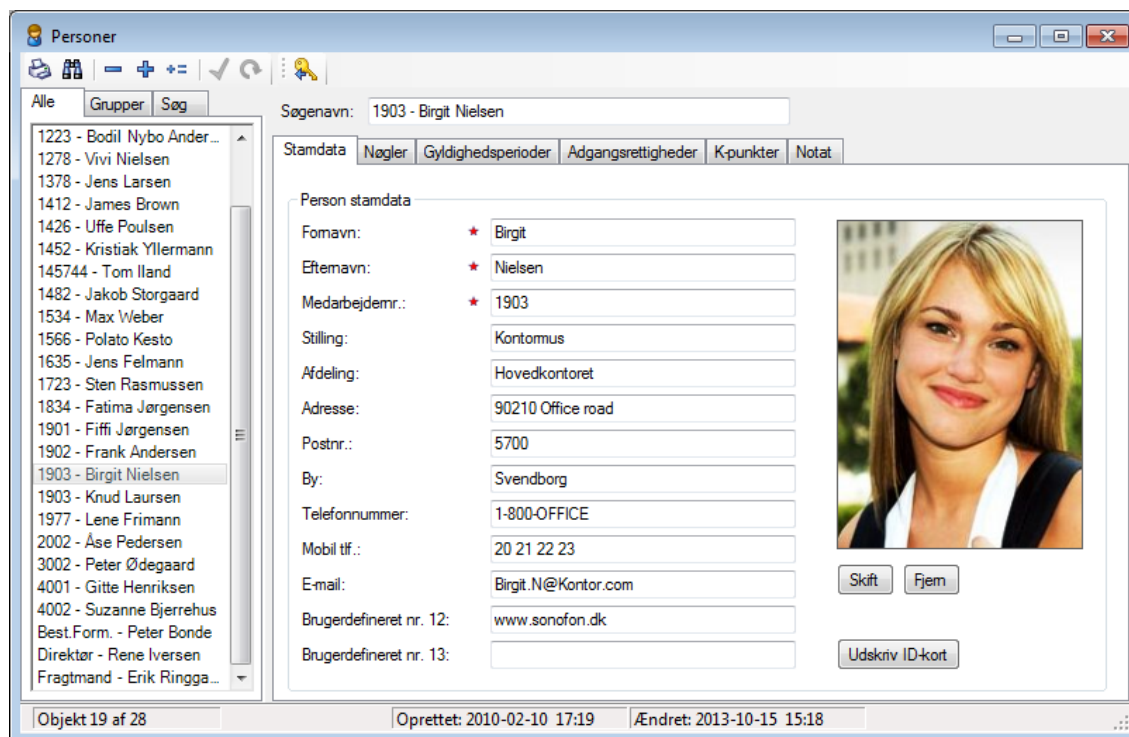
Der er mulighed for tre typer af godkendelse:

- |   |   |
|---|---|
| [UniLock-godkendelse]                   | Operatøren skal være oprettet med brugernavn og adgangskode i UniLock. Operatøren indtaster brugernavn og adgangskode for at logge ind.   |
| [Windows-godkendelse]                   | Pc skal være på et Windows domæne og operatøren er oprettet på domænet. Operatøren skal være oprettet i UniLock via import fra Active Directory. Operatøren indtaster brugernavn og adgangskode for at logge ind. |
| [Windows-godkendelse (aktuelle bruger)] | Pc skal være på et Windows domæne og operatøren er oprettet på domænet. Operatøren skal være oprettet i UniLock via import fra Active Directory. Tryk [OK] for at logge ind hvis ikke [Auto-logon] er aktiveret.  |

### **Auto-logon**

Login-proceduren kan lettes ved at aktivere [Auto-logon]. [Auto-logon] kan aktiveres når godkendelsestypen er [Windows-godkendelse (aktuelle bruger)]. Auto-logon gør at der automatisk logges ind i Adgangseditoren med den brugerkonti, der er logget ind i Windows (Single sign-on).

## 3.4 Personer



For at oprette en person med adgang, skal personen som minimum have et "Søgenavn" (objektnavn), en nøglekode og en adgangsrettighed. For at kunne skelne personer fra hinanden, skal feltet [Søgenavn] være entydigt. [Fornavn] og [Efternavn] i stamdata kan derimod udfyldes med personens korrekte navn.

### 3.4.1 Stamdata

Dette faneblad indeholder ingen oplysninger som adgangskontrollen skal bruge, men kun oplysninger der kan lette operatørens arbejde med administration og identifikation af personer og nøgler.

I menuen [Indstillinger], [Udfyldning af søgenavn] kan programmet sættes til at udfylde søgenavnet automatisk med "[Fornavn] [Efternavn]", "[Efternavn], [Fornavn]" eller andre valgbare felter fra stamdata.

Feltteksten for de 13 felter er brugerdefinerbar. Indtastningsfeltets default længde er 50 karakterer.

#### Billede

Som et ekstra supplement til identifikation af personer, er det muligt at indsætte et billede af personen. Billedet kan være i de mest anvendte grafikformater og kan gemmes i en vilkårlig billedmappe på netværket. Billedet kan eventuelt være fælles med og automatisk hentes i et medarbejderarkiv, ID-kort fabrikationsudstyr mv. Filstørrelsen på billedet bør ikke være for stor, da det kan sløve indlæsningen af personer, specielt hvis der køres over netværk. Et typisk billede fylder mellem 5 kB og 20kB.

Billede kan angives manuelt eller indlæses automatisk ud fra filnavn og mappe angivet i stamdatafelter. Til dette anvendes integrationstypen "Import af personbilleder".

## 3.4.2 Nøgler

For at kunne passere et k-punkt, skal personen have en nøgle. Formålet med en nøgle er at kunne identificere den person, der ønsker at passere et k-punkt. Derfor indeholder nøglen en entydig nøglekode. Som nøgle kan anvendes mange forskellige medier fx magnetkort, chipkort, stregkoder, radiosender, telefonnummer, proxkort (berøringsfri kort, RFID-kort, Mifare-kort), kontaktløse betalingskort, NFC baserede Apps (Google Pay, Apple Pay, My Wallet), nummerplader, fingeraftrykslæser mv. Systemet skal selvfølgelig anvende en læser, der kan læse koden i den nøgletype der anvendes.

Nøgler kan tildeles en valgfri nøgletekst som fx ”Sygesikringsbevis”, ”Dankort”, ”Firma-kort”.

### Oprettelse af nøgler

Ud fra de informationer der står på nøglen, beregner systemet en nøglekode, som sendes ud til de k-punkter, hvor nøglen må bruges. Når personen skal have udleveret en nøgle, skal nøglens nøglekode parres sammen med personen, dette kan gøres på flere måder:

1. Indlæs nøglen i en speciel læser som er tilsluttet pc'en (K17 USB bordlæser).
2. Aktiver ikonet [Hent nøglekode fra k-punkt] og vælg i dialogboksen det k-punkt der er nærmest, gå derefter ud til læseren og indlæs nøglen, aktiver derefter knappen [Hent nøglekode].
3. Indlæs nøglen i en tilfældig læser. I Poller log vil der komme en logning ”Nøgle afvist, ikke oprettet -- <ukendt nøgle: 'xxxxxxx'>”, indtast den oplyste nøglekode i feltet [Nøgledata].
4. Kendes data på nøglen kan de indtastes direkte i feltet [Nøgledata].

### PIN-kode

Indtastningsfeltet [PIN-kode] og tasten [Tilfældig PIN-kode] kan virke på flere måder, afhængig af den opsætning der er foretaget i menuen [Indstillinger], [Nøgledata og PIN-kode].

Personen behøver ikke nødvendigvis at have en PIN-kode, det afhænger af det sikkerhedsniveau der skal anvendes. Personlig PIN-kode bruges normalt kun på sikkerhedsniveau 3.x. På sikkerhedsniveau 0.1 og 1.x bør normalt kun anvendes ”fælles PIN-kode”. I opsætningsmenuen kan der dog gives tilladelse til anvendelse af personlig PIN-kode på sikkerhedsniveau 0.1 og 1.x.

Opmærksomheden henledes på, at anvendelse af personlige PIN-koder på sikkerhedsniveau 0.1 og 1.x er en kraftig reduktion af sikkerheden, specielt hvis der er mange PIN-koder i systemet. Er der fx 1000 firecifrede PIN-koder i systemet, er risikoen 1:10 for, at en tilfældig valgt PIN-kode vil give adgang.

Hver person kan frit vælge en 2, 3, 4 eller 5 cifret PIN-kode mindre end 65.536. Hvis der i opsætningen er fravalgt [Entydige PIN-koder], kan flere personer udmærket have samme PIN-kode.

Er PIN-koder i opsætningsmenuen sat til at være skjulte for operatøren, har operatøren ingen mulighed for at se personers PIN-koder. Dette giver mulighed for at personer kan anvende deres helt private kode (fx samme kode som de har på deres Dankort).

I specialsituationer kan det være påkrævet at der gives adgang på sikkerhedsniveau 3.x uden indtastning af PIN-kode for specifikke nøgler. Det kan fx være den nøgle som brandfolk

afhenter i en nøgleboks. Tildeles en nøgle PIN-koden ”9”, så kan denne nøgle oplåse på sikkerhedsniveau 3.2 uden indtastning af PIN-koden.

### 3.4.3 Gyldighedsperioder

Globale gyldighedsperioder kan fx bruges, når det ønskes at oprette en nøgle som først skal være gyldig fra et senere tidspunkt eller når systemet automatisk skal fjerne en persons adgangsrettigheder ved dennes afrejse om fx et år.

Da der kan oprettes op til 8 globale gyldighedsperioder per person, er det også muligt at bruge denne funktion til at gøre nøgler ugyldige i ferieperioder, personlige fridage, jul, påske mv.

Starttidspunkter og udløbstidspunkter ligger kun i databasen på pc'en, hvorfor nøgler kun tilføjes og fjernes fra k-punkter, når Polleren har forbindelse til k-punkterne.

### 3.4.4 Adgangsrettigheder

Før en person kan passere et k-punkt, skal personen have nogle adgangsrettigheder. Hver person kan helt individuelt tildeles adgangsrettigheder i en given tidsperiode for hvert enkelt k-punkt. Dette medfører, at hver enkelt person kan tildeles rettigheder, som er tilpasset lige præcis den aktuelle person.

Adgangsrettigheder til et k-punkt kan tildeles direkte eller indirekte gennem medlemskab af en eller flere grupper.

#### Grupper

Adgangsrettigheder til k-punkter kan tildeles indirekte gennem medlemskab af én eller flere grupper. En gruppe er en samling af k-punkter med tilhørende tidstabel. Adgangsrettigheder bør normalt altid tildeles gennem medlemskab af en gruppe, da det letter administrationen betydeligt, selv ved små systemer.

Medlemskab af grupper kan være gyldig altid eller tildeles periodevis med op til 50 gyldighedsperioder eller delt undtagelse for hvert gruppemedlemskab for hver person. Periodevist medlemskab gør det muligt at forprogrammere adgangsrettigheder for personer i rotation, turnus eller som på anden vis har skiftende fremmøde i forskellige områder, som fx elever, vikarer, løsarbejdere, freelancere, konsulenter mv.

Starttidspunkter og udløbstidspunkter ligger kun i databasen på pc'en, hvorfor nøgler kun tilføjes og fjernes fra k-punkter, når Polleren har forbindelse til k-punkterne.

#### K-punkter

En rettighed kan også tildeles direkte. Rettigheden består af et k-punkt med tilhørende tidstabel, som evt. kan være <Altid>. Den vedhæftede tidstabel indeholder tider for, hvornår k-punktet kan passeres.

Justering af rettigheder erhvervet gennem medlemskab af en gruppe

Direkte tildeling af k-punkter kan bruges til at give en person yderligere rettigheder, eller begrænse de rettigheder der er erhvervet gennem medlemskab af én eller flere grupper.

Er der erhvervet adgangsrettigheder til en række k-punkter gennem en gruppe, kan adgang til et specifikt k-punkt i gruppen forhindres, ved at tildele personen rettighed til det



pågældende k-punkt efter en tom tidstabel. På samme måde kan personens rettighed til et specifikt k-punkt ændres, ved at tildele adgang efter en anden tidstabel eller vælge <Altid>.

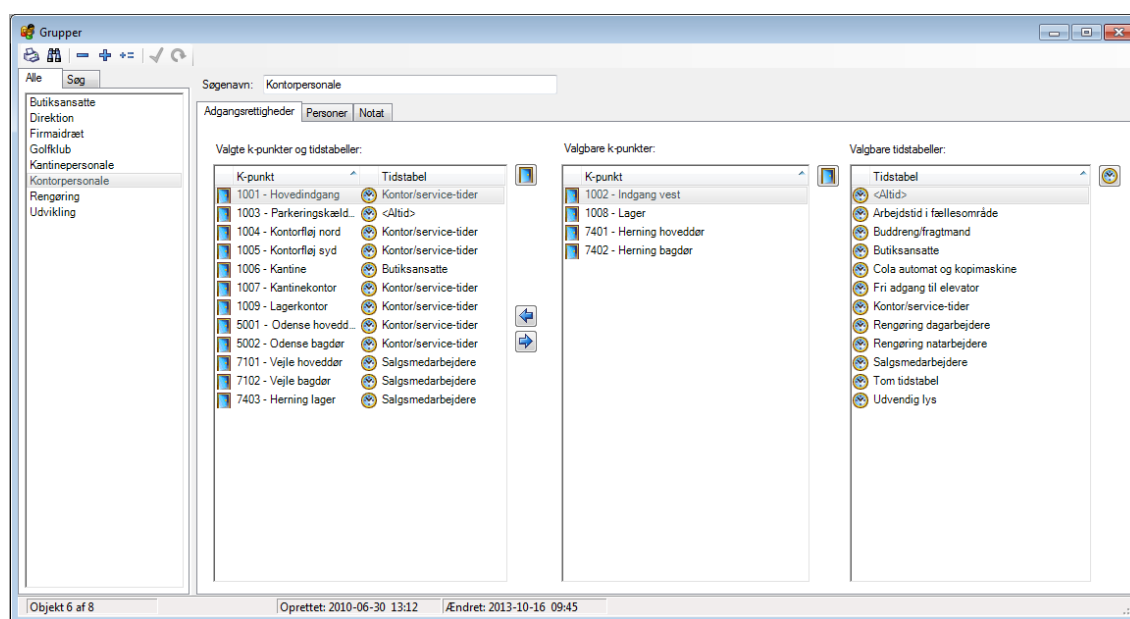
Vær opmærksom på, at hvis et k-punkt indgår i flere grupper, bruges rettigheden til det enkelte k-punkt fra den gruppe der står nederst i listen [Valgte grupper].

For at få oplyst personens effektive adgangsrettigheder vælges fanebladet [K-punkter].

### 3.4.5 K-punkter

Denne side er en ren informationsside, og der kan ikke foretages ændringer på siden. Siden viser personens effektive adgangsrettigheder som en liste af k-punkter med tilhørende tidstabel. Indholdet af grupperne er altså opløst i k-punkter med tilhørende tidstabeller. Informationerne er specielt nyttige, hvis personen er medlem af flere grupper, og der eventuelt også er tilføjet yderligere k-punkter, for at justere persons rettigheder, så kan det være svært at overskue de effektive adgangsrettigheder.

## 3.5 Grupper



Det er ikke nødvendigt at bruge grupper i systemet, men det letter oprettelse og administration af personer betydeligt. Fx er det besværligt, hver gang der skal oprettes en ny person, at tildele direkte adgang i fx 10 k-punkter efter lige så mange forskellige tidstabeller. Arbejdet lettes, hvis der oprettes grupper, som hver især svarer til fx en personalegruppe. Hver gang en ny person skal oprettes, tildeles blot medlemskab af den eller de grupper, som passer til adgangsbehovet.

En anden fordel ved grupper er, at hvis der ændres i gruppens adgangsrettigheder, påvirker det straks alle medlemmer af gruppen – der skal altså kun ændres et sted, og ikke under alle relevante personernes adgangsrettigheder.

### 3.5.1 Adgangsrettigheder

Her tildeles de rettigheder som gruppens medlemmer får. Individuelt for hvert k-punkt kan der kobles en tidstabel på k-punktet, som angiver de tidsperioder k-punktet kan passeres.

Må k-punktet altid kunne passeres, vælges <Altid> i stedet for en tidstabel.

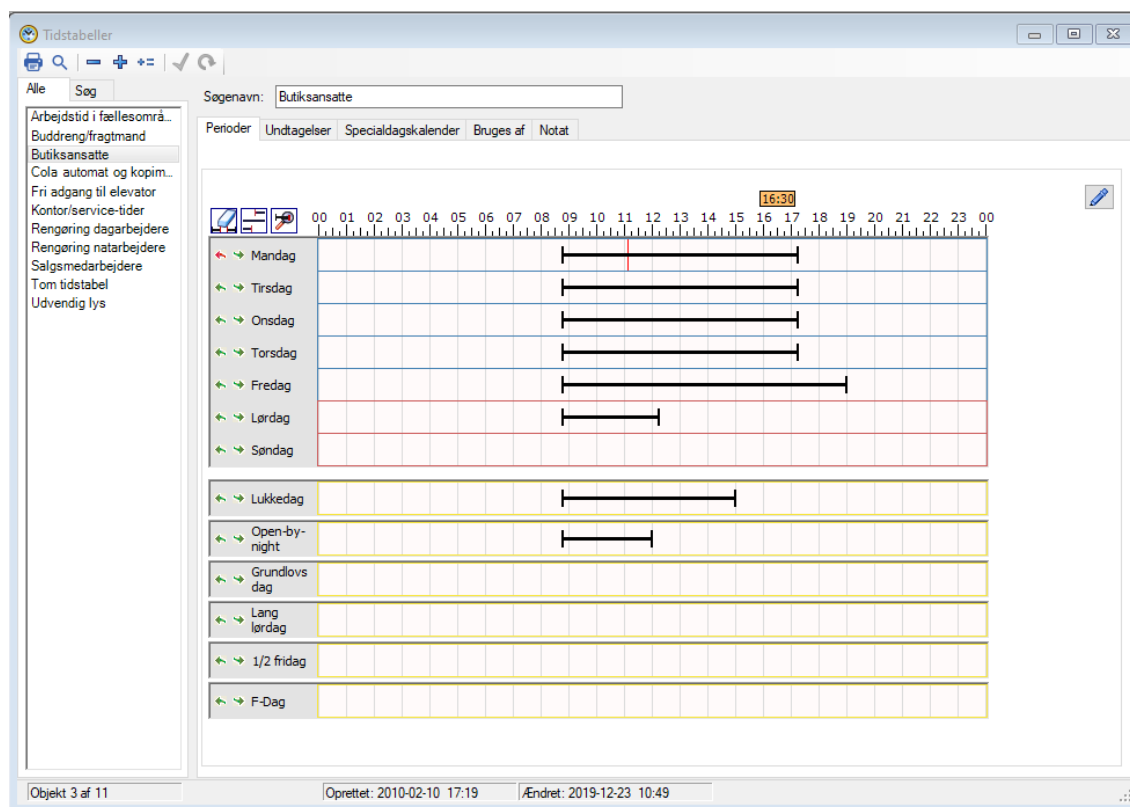
## 3.5.2 Personer

På denne side er det muligt at se, hvilke personer der er medlem af en gruppe. Før der laves ændringer i en gruppes adgangsrettigheder, kan det være en god ide at kigge på denne side og se, at ændringen kun berører de personer som man forventer.

Som noget helt specielt kan man også på denne side melde personer ind og ud af gruppen. Således er det fx muligt at oprette en helt ny gruppe, og derefter ved brug af kun denne side, at melde alle relevante personer ind i gruppen, uden at skulle igennem hver eneste persons adgangsrettigheder.

Er personen i forvejen medlem af én eller flere grupper, vil den sidst tilføjede gruppe have den højeste prioritet.

## 3.6 Tidstabeller



Tidstabellernes formål er at styre forskellige funktioner i systemet som er afhængig af tiden på døgnet, ugen og året. En tidstabel kan bruges til fx:

- Begrænse en persons adgangsrettighed til et k-punkt.
- Tidsstyring af udgange til fx lys, ventilation, cirkulationspumper mv.
- Begrænse tidspunktet for, hvornår en dør skal overvåges.
- Angive arbejdstiden for tyverialarmstyring og områdestyring.
- Begrænse tidspunktet for, hvornår forskellige hændelser skal logges.

En tidstabel udfører som sådan ikke noget, før der er nogle funktioner der bruger den, det kan fx være en adgangsrettighed til en bestemt dør for en nøgle, styring af en udgang på låsecomputeren til styring af lyset på parkeringspladsen.

Før der laves ændringer i en tidstabel, er det altid en god ide at kigge på fanebladet [Bruges af]. Her oplyses det, hvem der bruger den pågældende tidstabel, og som eventuelle ændringer vil påvirke.

### 3.6.1 Perioder

Der kan oprettes ubegrænset antal tidstabeller, hver af disse tidstabeller kan indeholde op til 16 tidsperioder, som frit kan fordeles mellem alle ugens 7 dage og de 6 fiktive special-dage. En tidsperiode kan udmærket gå hen over midnat, og det er fx muligt at lave en tidsperiode fra [Mandag 06:00] til [Fredag 16:00].

Redigering kan foregå på tabelform efter tryk på blyantknappen eller direkte i tidsområdet med træk-og-slip med musen.

Der findes tre knapper til at lette redigering:

- [Slet tidsperioder (Skift + markér område)]
- [Sammenhængende tidsperiode (Ctrl + markér område)]
- [Finjustér tidspunkt (Alt + træk endemarkør)], som zoomer redigering til minut-interval.

### 3.6.2 Undtagelser

Normalt gentager en tidstabel sig selv uge efter uge, men i visse situationer kan det være ønskeligt at bryde denne monotoni. En undtagelse består af en tidsperiode, hvor der anvendes en anden valgbar funktion end den, der er angivet i tidstabellen.

En undtagelse kan fx bruges til at tildele (eller hindre) ekstraordinær adgang for en person eller persongruppe i en nøje specificeret tidsperiode.

#### Undtagelsesperiode

Der kan oprettes 8 undtagelser for hver tidstabel, hver med op til fire undtagelsesperioder, hvor hver undtagelsesperiode kan gå fra et minut til flere år. Ved overlappende undtagelser har den øverste undtagelse højeste prioritet i overlappingsperioden.

Det er endvidere muligt at anvende delte undtagelser. En delt undtagelse giver mulighed for, at undtagelser for forskellige tidstabeller og sikkerhedsniveautidstabeller benytter samme tidsperiode, som så kun skal ændres et sted.

En delt undtagelse kunne være ”Ferie lukning”, ”Åbent hus” eller ”Fest”, altså en periode hvor mange tidstabeller og sikkerhedsniveautidstabeller ønskes påvirket af den samme handling.

#### Funktion

Ved hjælp af funktionsvalg er det muligt at bestemme, hvad der skal ske i undtagelsesperioden. Det kan vælges om tidstabellen skal:

- Være konstant on eller off.
- Følge en anden tidstabel.
- Følge en specialdag.

Det er således muligt at programmere en tidstabel til at følge en anden tidstabel eller en specialdag i fx sommerferien.

Undtagelser har højere prioritet end specialdage i specialdagskalenderen.

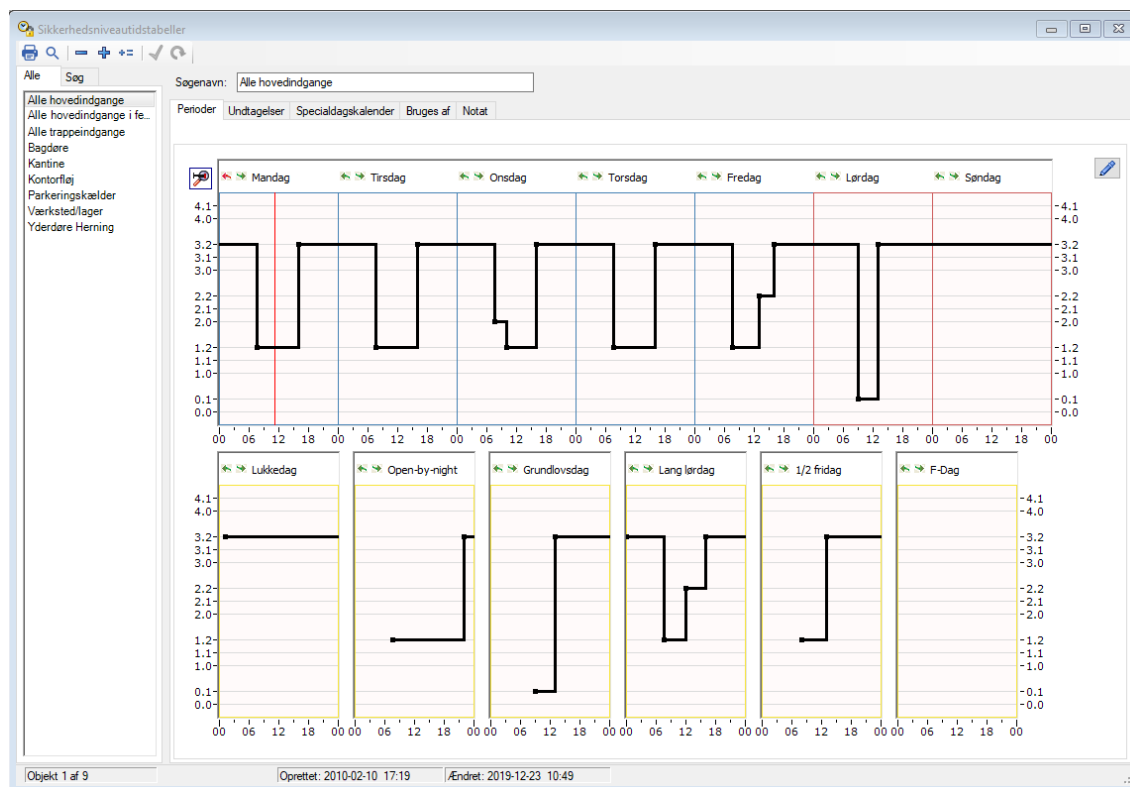
### 3.6.3 Specialdagskalender

Tidstabellen vil følge de specialdage, der er i den valgte specialdagskalender.

### 3.6.4 Prioritering

Tabellen følger den pågældende dag bestemt af specialdagskalenderen. Når en undtagelse er aktiv, så følges undtagelsens funktion.

## 3.7 Sikkerhedsniveautidstabeller



Sikkerhedsniveautidstabellernes formål er at styre k-punkternes sikkerhedsniveau som en funktion af tiden på døgnet, ugen og året. En sikkerhedsniveautidstabel udfører som sådan ikke noget, før et eller flere k-punkter bruger den.

Alle k-punkter der har samme sikkerhedsprofil, fx alle "Hovedindgange", kan styres af den samme sikkerhedsniveautidstabel, således at der kun skal ændres et sted, for at ændre sikkerhedsniveauet på alle hovedindgange.

Et k-punkts sikkerhedsniveau fortæller noget om, hvor svært det er at passere det pågældende k-punkt. Følgende sikkerhedsniveauer kan anvendes:

- 0.0 Konstant oplåst (kan ikke låses med normal nøgle).
- 0.1 Konstant oplåst efter anvendelse af første nøgle eller PIN-kode.
- 1.0 Nøgle eller PIN-kode (skiftefunktion, starter med oplåst).
- 1.1 Nøgle eller PIN-kode (skiftefunktion, starter med låst).

- 1.2 Nøgle eller PIN-kode (oplåst i tid).
- 2.0 Nøgle (skiftefunktion, starter med oplåst).
- 2.1 Nøgle (skiftefunktion, starter med låst).
- 2.2 Nøgle (oplåst i tid).
- 3.0 Nøgle + PIN-kode (skiftefunktion, starter med oplåst).
- 3.1 Nøgle + PIN-kode (skiftefunktion, starter med låst).
- 3.2 Nøgle + PIN-kode (oplåst i tid).
- 4.0 Konstant låst efter anvendelse af første nøgle + PIN-kode.
- 4.1 Konstant låst (kan ikke oplåses med almindelig nøgle).

Før der laves ændringer i en sikkerhedsniveautidstabel, er det altid en god ide at kigge på fanebladet [Bruges af]. Her oplyses det, hvem der bruger den pågældende tabel og som eventuelle ændringer vil påvirke.

### 3.7.1 Niveauskift

Der kan oprettes ubegrænset antal sikkerhedsniveautidstabeller, der hver kan indeholde op til 32 sikkerhedsniveauskift, som frit kan fordeles mellem alle ugens 7 dage og de 6 fiktive specialdage.

Ved skift til en specialdag, som altid foregår kl. 00:00, vil sikkerhedsniveauet være det, det var lige før midnat, hvis der ikke er defineret et nyt sikkerhedsniveau på den pågældende specialdag kl. 00:00.

Som noget specielt er det muligt flere gange lige efter hinanden, at skifte til det samme sikkerhedsniveau. Dette kan fx bruges hvis det ønskes, at døren skal sikkerhedslåse kl. 16:00, 17:00 og 18:00, på disse tidspunkter skiftes så til sikkerhedsniveau "2.1". Er der så nogen i huset som efter kl. 16:00 venter gæster, må de altså ud til læseren for at oplåse døren konstant igen, de "køber" altså en ekstra times åbningstid. Kl. 17:00 sikkerhedslåses døren igen, og man må igen "købe" tid osv. Hvis der så kl. 19:00 skiftes til niveau 2.2 er det slut med at købe tid, for herefter oplåser døren kun i tid (5 sek.).

Redigering kan foregå på tabelform efter tryk på blyantknappen eller direkte i tidsområdet med træk-og-slip med musen.

Der findes tre knapper til at lette redigering:

- [Kopiér dag]
- [Indsæt dag]
- [Finjustér tidspunkt (Alt + træk endemarkør)], som zoomer redigering til minutinterval.

### 3.7.2 Undtagelser

Normalt gentager en sikkerhedsniveautidstabel sig selv uge efter uge, men i visse situationer kan det være ønskeligt at bryde denne monotoni. En undtagelse består af en tidsperiode, hvor der anvendes en anden valgbar funktion end den, der er angivet i sikkerhedsniveautidstabellen.

En undtagelse kan bruges til at ændre sikkerhedsniveauet ekstraordinært i forbindelse med sommerferie, åbent hus, aften arrangement, udlån af gymnastiksal mv.

## Undtagelsesperiode

Der kan oprettes 8 undtagelser for hver sikkerhedsniveautidstabel, hver med op til fire undtagelsesperioder, hvor hver undtagelsesperiode kan gå fra et minut til flere år. Ved overlappende undtagelser har den øverste undtagelse højeste prioritet i overlappingsperioden.

Det er endvidere muligt at anvende delte undtagelser. En delt undtagelse giver mulighed for, at undtagelser for forskellige tidstabeller og sikkerhedsniveautidstabeller benytter samme tidsperiode, som så kun skal ændres et sted.

En delt undtagelse kunne være ”Ferie lukning”, ”Åbent hus” eller ”Fest”, altså en periode hvor mange tidstabeller og sikkerhedsniveautidstabeller ønskes påvirket af den samme handling.

## Funktion

Ved hjælp af funktionsvalg er det muligt at bestemme, hvad der skal ske i undtagelsesperioden. Det kan vælges om sikkerhedsniveautidstabellen skal:

- Være konstant på et valgt sikkerhedsniveau
- Følge en anden sikkerhedsniveautidstabel
- Følge en specialdag.

Det er således muligt at programmere en sikkerhedsniveautidstabel til at følge en anden sikkerhedsniveautidstabel eller en specialdag i fx sommerferien.

Undtagelser har højere prioritet end specialdage i specialdagskalenderen.

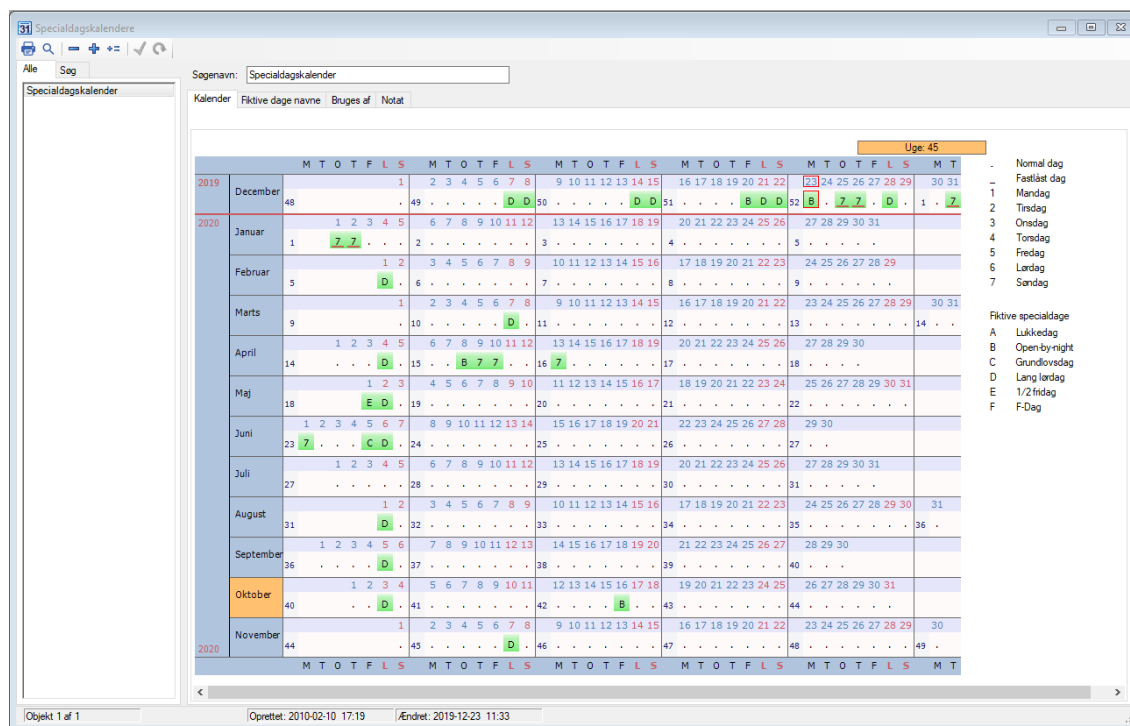
### 3.7.3 Specialdagskalender

Sikkerhedsniveautidstabellen vil følge de specialdage, der er i den valgte specialdagskalender.

### 3.7.4 Prioritering

Tabellen følger den pågældende dag bestemt af specialdagskalenderen. Når en undtagelse er aktiv, så følges undtagelsens funktion.

## 3.8 Specialdagskalendere



Specialdagskalendere indeholder informationer om, hvilke dage der ikke er normale ugedage, fx helligdage, 1. maj, lang lørdag, åbent hus mv. En specialdag går altid fra kl. 00:00 og et døgn frem.

Specialdagskalender kan tilvælges for den del af systemet, som skal gøre noget specielt på specialdage. Hvis en dag er en specialdag, kan det således gælde kun for udvalgte k-punkter og ikke nødvendigvis for hele systemet.

Udover de 7 almindelige ugedage, kan der opereres med 6 fiktive specialdage. Hver dag indenfor det næste år kan frit tilknyttes én af disse 6 fiktive specialdage.

### 3.8.1 Kalender

I kalenderdelen kan de næste 11-12 måneders specialdage planlægges og skrives ind i kalenderen. Der kan anvendes følgende angivelser i kalenderen:

- 0 Normal ugedag. Der er ingen afvigelse fra normalkalenderen.
- 1-7 Anvendes, hvis der skal benyttes en anden ugedag end den aktuelle. Hvis der fx anvendes "søndags drift" på helligdage, skrives 7 ud for disse dage (1=mandag, 7=søndag). Eller der kan måske anvendes "lørdags drift" (dag 6) 1. maj, 24. december osv.
- A-F Bruges, når der skal anvendes en af de fiktive specialdage A-F.

En fiktiv specialdag anvendes, hvis ingen af de andre dage (1-7) kan anvendes på den ønskede dato.

Hvis der fx skal anvendes helt specielle adgangskriterier den første lørdag i måneden (lang lørdag), skrives fx "A" ud for første lørdag i hver måned.

Hvis der er specialdage der går igen fra år til år, og de ønskes overført til året efter, kan disse dage "låses" ved at understrege specialdagen med tasten [ \_ ].

### **Tidstabeller og fiktive specialdage**

Hvis personer skal have adgang på fiktive specialdage, skal deres respektive tidstabeller indeholde adgangsperioder for den fiktive specialdag der anvendes. Personer der altid har adgang (Tidstabel <Altid>), har selvfølgelig også altid adgang på alle fiktive specialdage.

På samme måde, hvis en tidstabel styrer fx lyset på parkeringspladsen, og dette lys skal tændes på en fiktiv specialdag, så skal tidstabellen indeholde en tidsperiode for den pågældende fiktive specialdag.

Alle tidstabeller der skal være aktive på en fiktiv specialdag, skal altså indeholde tidsperioder for den pågældende fiktive specialdag.

### **Sikkerhedsniveautidstabeller og fiktive specialdage**

Sikkerhedsniveautidstabellen indeholder tider for skift til et andet sikkerhedsniveau på døren. Indeholder sikkerhedsniveautidstabellen ikke skift for den pågældende fiktive specialdag der anvendes, vil døren på hele specialdagen forblive på det sikkerhedsniveau den var på, før den fiktive specialdag startede kl. 00:00.

Skal sikkerhedsniveauet være anderledes end det var kl. 00:00, eller skal niveauet skifte i løbet af den fiktive specialdag, skal dette sikkerhedsniveau altså defineres i sikkerhedsniveautidstabellen for den aktuelle fiktive specialdag.

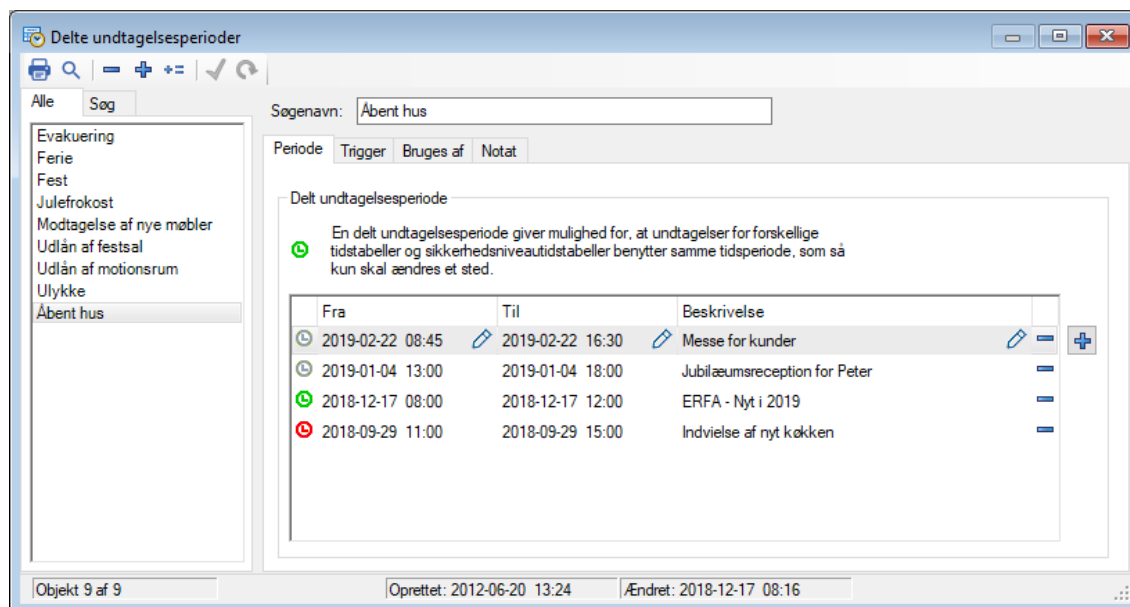
Ved afslutning af en specialdag skiftes altid til sikkerhedsniveauet for den efterfølgende dag.

## **3.8.2 Fiktive specialdage navne**

Her er det muligt, men ikke nødvendigt, at give de 6 fiktive specialdage (A-F) et mere sigende navn som fx "Lang lørdag". Det navn, der er givet til den fiktive specialdag, vil herefter blive brugt i tidstabeller og sikkerhedsniveautidstabeller, som anvender specialdagskalenderen.



## 3.9 Delte undtagelser



Undtagelser er et kraftigt supplement til specialdagskalenderen. Modsat specialdage, der varer hele døgnet, varer undtagelser i en valgbar tidsperiode.

Normalt gentager en tidstabel og sikkerhedsniveautidstabel sig selv uge efter uge, men i visse situationer kan det være ønskeligt at bryde denne monoton. En undtagelse består af en tidsperiode, hvor der anvendes en anden valgbar funktion end den, der er angivet i tidstabelen.

En delt undtagelse giver mulighed for:

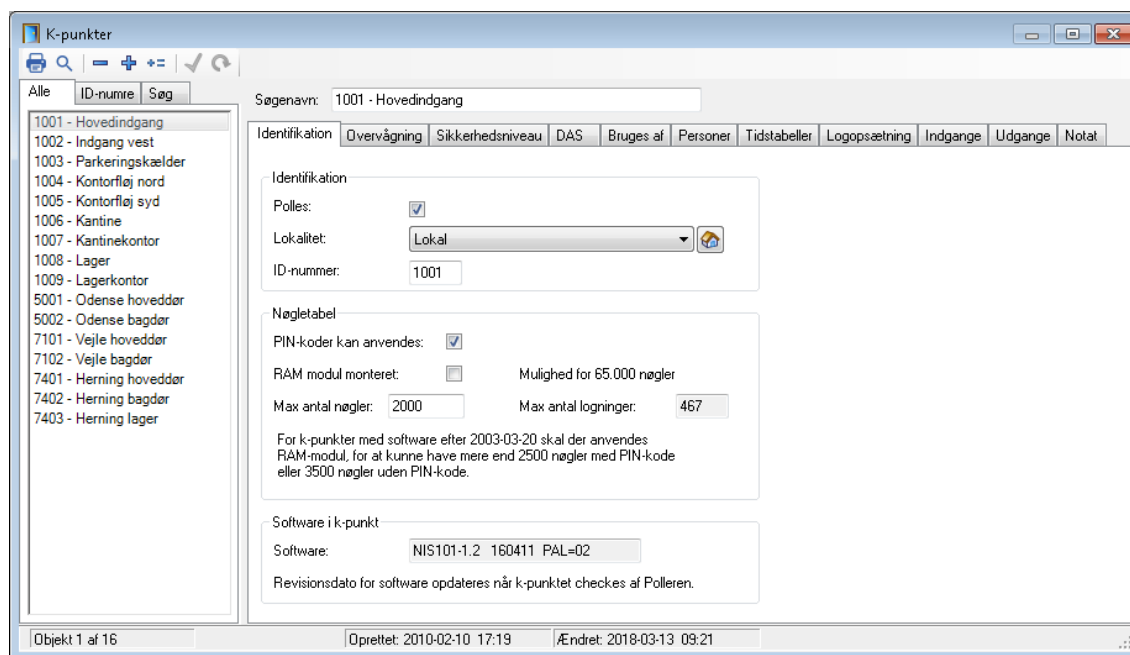
- At undtagelser for forskellige tidstabeller og sikkerhedsniveautidstabeller benytter samme tidsperioder/trigger, som så kun skal ændres et sted.
- At personers adgangsrettigheder gennem medlemskab af grupper styres af delte undtagelsers tidsperioder/trigger.

Der kan oprettes et ubegrænset antal delte undtagelser, hver med op til 100 tidsperioder, hvor hver tidsperiode kan gå fra et minut til flere år, eller trigger, som kan vælges som et signalniveau på en valgfri indgang i et valgfrit k-punkt.

Eksempelvis kunne der oprettes en delt undtagelse kaldet "Fest". Når der så skal være fest i firmaet, indtastet start- og slut-tidspunktet på festperioden. Alle de tidstabeller og sikkerhedsniveautidstabeller der skal påvirkes af festen tilføjes den delte undtagelsesperiode, og som funktion vælges den handling, den pågældende tabel skal udføre under festen. Dette kunne være at oplåse alle hoveddøre, tildele ekstraordinær adgang til kantinen, frakoble tyverialarmen, starte ventilationen og tænde for Cola-automaten.

Når festen er slut, vender systemet automatisk tilbage til normal drift. Den delte undtagelse kaldet "Fest" slettes ikke, men kan genbruges ved næste fest. Når tid og dato for næste fest er kendt indtastes de, og alle undtagelsesfunktioner gentager sig.

## 3.10 K-punkter



K-punkt er en forkortelse for kontrolpunkt, altså et punkt hvor der er kontrol af, hvem der kan passere og hvornår. Et k-punkt behøver ikke være en dør, men kan også være fx er bom, port, elevator mv. I dette objektvindue foretages primært systemopsætninger, så dagligdags-operatøren vil normalt ikke stifte meget bekendtskab med dette objektvindue.

### 3.10.1 ID-nummer

Kommunikationen til alle låsecomputere i k-punkterne foregår over et fælles kommunikationsnet. Derfor skal hver enhed på nettet have et entydigt ID-nummer, således at Polleren kan identificere hver enkelt låsecomputer.

Som ID-nummer vælges et tilfældigt 4 cifret tal (hexstal kan anvendes med undtagelse af FFF1-FFF2). For at lette identifikationen af k-punkter anbefales det, at anvende en eller anden form for systematisk nummerering. K-punkter på første sal kan fx gives numrene 1001, 1002, ..., på anden sal 2001, 2002, ... osv. Er der mange eksterne afdelinger (lokaliteter) i installationen kunne, de to første cifre i ID-nummeret være de to første cifre i postnummeret.

#### Lokalitet

En lokalitet er et antal k-punkter der har forbindelse med hinanden på det samme kommunikationsnet (RS485 eller Ethernet). Er der langt til nogle k-punkter, kan disse oprettes i en eller flere særskilte lokaliteter, hvor de enkelte k-punkter i hver lokalitet er koblet på samme kommunikationsnet. Forbindelsen til en eksternt lokalitet kan etableres med modem over telefonnettet (analog eller GSM) eller med en COM Server (CV72) over et IP-netværk (pc-netværk og/eller internettet).

#### Max antal nøgler

Hvert k-punkt kan i standardkonfigurationen indeholde op til 2500 nøgler med PIN-kode eller 3500 nøgler uden PIN-kode. Indenfor disse begrænsninger er det valgfrit, hvor mange

nøgler der skal reserveres plads til. Den resterende hukommelse i låsecomputeren bruges til at gemme logninger.

Ønskes det at oprette flere end de 2500 nøgler med PIN-koder der er plads til i låsecomputerens standard konfigurationen, kan der anskaffes et RAM-modul. RAM-modulet giver mulighed for at oprette op til 65.000 nøgler med PIN-kode.

### **3.10.2 Overvågning**

Er der monteret en karmkontakt på døren, giver det mulighed for at overvåge, om døren lukkes igen efter en bevilget adgang, eller om døren tvangsåbnes.

Hvis der er monteret karmkontakt, låses døren et sekund efter at døren åbnes, så døren ikke springer op igen, når døren lukkes. Dette forhindrer ligeledes andre i at smutte med ind, efter at en person med gyldig adgang har lukket døren efter sig

#### **Overvågningstidstabel**

Denne tidstabel indeholder perioder for, hvornår der er overvågning på døren. Udenfor de perioder der er i tidstabellen, er der ikke overvågning på døren. Vær opmærksom på, at hvis der skal være overvågning af døren på specialdage, skal tidstabellen også indeholde perioder for specialdagen.

#### **Tid før opmærksomhedssignal**

Efter en oplåsning af døren, skal døren lukkes igen inden denne tid er gået. Hvis døren ikke lukkes igen, begynder udgang 2 på låsecomputeren at "blinke" (skiftevis trukket/ikke trukket). Denne udgang kan bruges til at aktivere en summer/sirene der afgiver et opmærksomhedssignal, så brugeren kan nå at lukke døren igen, inden der afgives alarm. Tiden kan være 0 til 255 sekunder, indsættes 0 er funktionen ikke aktiv.

[Tid før opmærksomhedssignal] og regnes fra det tidspunkt, hvor døren ikke længere er oplåst.

#### **Tid før alarmsignal**

Hvis ikke døren lukkes igen, inden denne tid er gået, trækker udgang 2 og 4 på låsecomputeren konstant. Er der en sirene på udgang 2, vil den så skifte til konstant lyd, og dermed gøre brugerne opmærksom på alarmtilstanden. Udgang 4 kan bruges til at aktivere en alarm eller anden sikkerhedsforanstaltning. Tiden kan være 0 til 255 sekunder, indsættes 0 er funktionen ikke aktiv.

Når døren oplåses, aktiveres udgang 3 i denne tid. Så længe døren er konstant oplåst er udgang 3 aktiv. Udgang 3 er beregnet til alarmforbikobling.

[Tid før alarmsignal] regnes fra det tidspunkt, hvor døren ikke længere er oplåst.

#### **Udtryk oplåser ikke elektrisk men tillader mekanisk oplåsning**

Elektrisk ud-oplåsning på visse elektromekaniske låse kan give sikkerhedsmæssige udfordringer. Problemet er, at vibrationer fra ydersiden kan forplante sig til ud-håndtaget hvor der sidder en "åbningsswitch" - dette medfører at slag på ydersiden kan få døren til at oplåse.

Problemet er blandt andet aktuelt i de populære og uheldigt designede låse type EL480/482/580/582 fra Assa Abloy.

Af sikkerhedsmæssige grunde bør denne funktion aktiveres på el-låse med mekanisk udoplåsning.

### **Overvågning af læsere**

Læsere kan overvåges for at alarmere når forbindelse til læsere mistes og når læsere detekterer forsøg på nedtagning og uautoriseret adgang til læserens indre (tamper/sabotage).

Alarmering kan ske via en valgfri udgang på låsecomputeren, skærmalarm i pc-program og alarmering til kontrolcentral når SIA integration anvendes.

Yderligere er det muligt at aktivere signalering af ”Dør ikke lukket” med læserens indbyggede lyd giver.

### **Overfaldskode**

På sikkerhedsniveau 3.x kan der anvendes overfaldskode, således at hvis brugeren indtaster sin PIN-kode + 1 afgives der en alarm på pc'en, og en valgbare udgang aktiveres.

## **3.10.3 Sikkerhedsniveau**

På denne side findes funktioner der styrer, hvor svært det skal være for brugeren at passere k-punktet.

K-punktets aktuelle sikkerhedsniveau er gældende for nøgler anvendt i indlæser, mens alle nøgler i k-punktet altid vil kunne oplåse ved at anvende udlæser.

### **Døroplåsningstid**

Denne tid angiver, i hvor lang tid døren skal oplåse, når døren er på et sikkerhedsniveau der oplåser i tid (1.2, 2.2 eller 3.2). Tiden som døren oplåser, kan indstilles mellem 1 og 99 sekunder. Hvis der er monteret karmkontakt, låser døren (udgang deaktiveres) når den åbnes.

### **Fælles PIN-kode**

Hvis der er angivet en fælles PIN-kode, kan denne bruges til at oplåse/låse døren, når k-punktet er på sikkerhedsniveau 0.1 eller 1.X. Som navnet angiver, er denne kode ikke knyttet til en bestemt person men til k-punktet, og kan derfor være forskellig for alle k-punkter i systemet.

Oplåsning med fælles PIN-kode giver selvsagt en meget lav sikkerhed, men dog betydelig højere sikkerhed end oplåsning med personlig PIN-kode alene.

Som PIN-kode kan vælges et 2, 3, 4 eller 5 cifret tal mindre end 65.536. Indtastes mere end fem forkerte PIN-koder efter hinanden blokeres for yderligere forsøg i fem minutter. Skift af sikkerhedsniveau eller adgang med nøgle vil ophæve denne blokering af læseren.

### **Konstant / tidsstyret sikkerhedsniveau**

Et k-punkt kan enten have et konstant sikkerhedsniveau, eller det kan følge en sikkerhedsniveautidstabel.

Tip: Hvis flere k-punkter skal have samme konstante sikkerhedsniveau, kan der også med fordel oprettes en sikkerhedsniveautidstabel der angiver det sikkerhedsniveau, som de aktuelle k-punkter skal anvende. På den måde kan sikkerhedsniveauet rettes for de aktuelle

k-punkter blot ved at rette i én sikkerhedsniveautidstabel, i stedet for at skulle rette for hver enkelt k-punkt.

### **Default sikkerhedsniveau**

Et k-punkt er altid på et sikkerhedsniveau. Normalt følger sikkerhedsniveauet sikkerhedsniveautidstabellen. Der anvendes dog default sikkerhedsniveau i nedenstående tilfælde.

- Hvis der anvendes konstant sikkerhedsniveau.
- Uret i k-punktet er ikke stillet (efter strømsvigt).
- Hvis den angivne sikkerhedsniveautidstabel er tom
- Hvis et k-punkt anvender en sikkerhedsniveautidstabel som endnu ikke er blevet sendt til k-punktet.

### **Sikkerhedsniveautidstabel**

En sikkerhedsniveautidstabel indeholder tider for, hvornår k-punktet skal skifte sikkerhedsniveau. Vær opmærksom på, at hvis der anvendes specialdage, skal der også i sikkerhedsniveautidstabellen angives sikkerhedsniveauskift for specialdagene.

Alle k-punkter der har samme sikkerhedsprofil, fx alle ”Hovedindgange”, kan styres af den samme sikkerhedsniveautidstabel, således at der kun skal ændres et sted, for at ændre sikkerhedsniveauet på alle hovedindgange.

### **Tvangsstyret sikkerhedsniveau**

Med et signal på en valgfri indgang er det muligt at tvangsstyre sikkerhedsniveauet til et ønsket sikkerhedsniveau eller kræve, at kun masternøgler har adgang. (Masternøgler er nøgler i k-punktet med tidstabellen <Altid>).

Da der er to kanaler, er det fx muligt at tvangsstyre til to ønskede faste sikkerhedsniveauer fx. 4.1 (tvangslåst) og 0.0 (tvangsåben), eller at tvangsstyre til et fast sikkerhedsniveau på den ene kanal, mens der på den anden kanal kan vælges ”Kun adgang med masternøgler”. Der kan udmærket vælges samme indgang i begge kanaler, eventuelt hvor den ene er aktiv ved høj, og den anden er aktiv ved lav.

### **Begrænsning af udpassage**

Udpassage gennem k-punktet kan begrænses eller forhindres, når sikkerhedsniveauet er over et valgt niveau. Det er muligt, at vælge forskellige sikkerhedsniveauer for hvornår henholdsvis udtryk og udlæser ikke kan anvendes.

Fx når sikkerhedsniveauet hæves til 3.2 ønsker man af sikkerhedsgrunde, at udtrykket ikke kan anvendes, da gæster i bygningen skal lukkes ud af en medarbejder med et nøglekort.

Ligeledes kan man lave en total dørspærring ved at forhindre brug af udlæser og udtryk, når sikkerhedsniveauet er over fx 4.0.

## **3.10.4 DAS**

DAS'en (Decentral Alarm Styring) giver den enkelte låsecomputer mulighed for at styre til- og frakoblingen af tyverialarmen i det område hvortil låsecomputeren giver adgang.

Opsætning af alarmstyring er meget kompliceret. Derfor bør alarmstyring kun opsættes af personer med stort kendskab til tyverialarmer, adgangskontrol og anvendelse af pc'er.

Samtidig bør man gøre sig det klart, hvordan alarmen ønskes styret, før opsætning af parametre påbegyndes.

## **Bruger ved k-punktet**

### **Frakobling**

Når en gyldig nøgle anvendes i et k-punkt, frakobles alarmen straks. Desuden kan alarmen frakobles automatisk ved start af arbejdstid hvis det ønskes.

Ved manuel frakobling vil den gule lysdiode blinke i 8 sekunder. Er der tilbagemelding fra tyverialarm, vil lysdioden lyse konstant indtil der modtages frakoblingssignal fra tyverialarmen, herefter blinker den i 8 sekunder.

### **Tilkobling**

For at tilkoble tyverialarmen manuelt trykkes på <\* + et tal> hvorefter en gyldig nøgle anvendes. "Stjernetallet" kan frit vælges mellem "0" og "254". Anvendes PIN-kode som nøgle taster man: <\* + stjernetal + # + PIN-kode + #> som fx `"*0#7211#"`.

Er "stjernetallet" valgt til "0" (anbefales) og bruges berøringsfri læsere fra Unitek, vil alarmen blive tilkoblet når nøglen holdes foran læseren i 5 sekunder.

Endvidere tilkobles alarmen automatisk ved udløb af arbejdstid, købetid og bagstopper.

Ved manuel tilkobling vil den gule lysdiode lyse konstant i 8 sekunder (tilkoblingsstatus vises vedvarende hvis det er valgt). Er der tilbagemelding fra tyverialarm, vil lysdioden blinke indtil der modtages tilkoblingssignal fra tyverialarmen, herefter tændes lysdioden konstant i 8 sekunder (tilkoblingsstatus vises vedvarende hvis det er valgt).

### **Tidsforskudt tilkobling**

Alarmen kan af bruger tilkobles på et forskudt tidspunkt. Det gøres som ved normal tilkobling, blot efterfølges stjernetallet af et klokkeslæt (<\*xxxhhmm>), hvorefter en gyldig nøgle anvendes. Stjernetallet "xxx" kan være 1 til 3 cifre, mens tidspunktet "hhmm" altid skal angives med 4 cifre. Er "stjernetallet" valgt til "0" kan man helt specielt lave tidsforskudt tilkobling uden at angive "stjernetallet", som fx (<\*hhmm>) efterfulgt af en gyldig nøgle.

Hvis alarmen allerede er tilkoblet, kan tidsforskudt tilkobling ikke programmeres.

Tidsforskudt tilkobling har højeste prioritet, og tilsidesætter derfor alle andre automatiske tilkoblinger, dvs. at alarmen ikke tilkobles ved udløb af arbejdstid, købetid og bagstopper.

Det indtastede tilkoblings-tidspunkt kan ændres ved at indtaste en ny tid.

En tidsforskudt tilkobling kan kun ophæves ved at tilkoble alarmen manuelt eller ved at lade den tilkoble på det indtastede tidspunkt.

Ved en godkendt tidsforskudt tilkobling vil den gule lysdiode blinke i 8 sekunder.

### **Købetid**

Købetid anvendes, når alarmen frakobles udenfor arbejdstiden. Hver gang der anvendes en gyldig nøgle, udskydes den automatiske tilkobling i denne tid. Hvis købetiden fx er 2 timer, tilkobles alarmen automatisk 2 timer efter sidst anvendte gyldige nøgle.

Kommer den automatiske tilkoblingstid indenfor arbejdstiden, vil tilkoblingen først ske ved udløb af arbejdstiden.

Ved udløb af købetid tilkobles alarmer automatisk efter en prealarm.

### Automatisk låsning af døre

Når tyverialarmen tilkobles ved én af dørene, vil alle dørene i den samme DAS gruppe automatisk blive låst. Anvendes et hierarki af DAS-grupper vil alle døre i underliggende DAS-grupper også låse. På samme måde kan alle døre i en DAS-gruppe sættes til at oplåse, når alarmer frakobles ved én af dørene.

### Gul lysdiode i læser

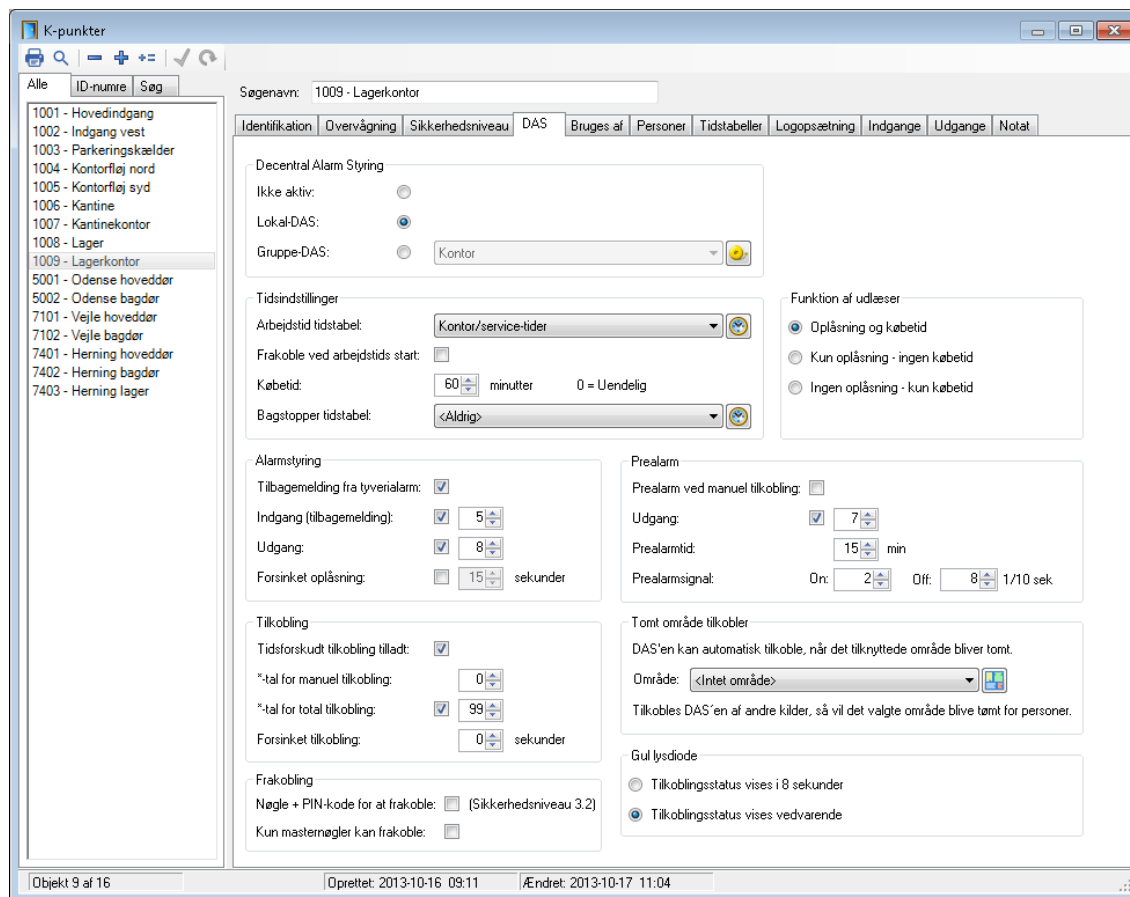
Den gule lysdiode i læseren angiver status for en frakobling, tilkobling og tidsforskudt tilkobling af tyverialarmen.

Afhængig af den valgte opsætning vil den gule lysdiode følge funktionen i én af de fire søjler i nedenstående tabel.

	Opsætning 1	Opsætning 2	Opsætning 3	Opsætning 4
	Uden tilbagemelding fra tyverialarm		Med tilbagemelding fra tyverialarm	
Hændelse	Status vises i 8 sek.	Status vises vedvarende	Status vises i 8 sek.	Status vises vedvarende
Tilkobling ved læser	<b>Konstant</b> i 8 sek.	<b>Konstant</b>	<b>Blink</b> (max. 8 sek.)	<b>Blink</b> (max. 8 sek.)
Tyverialarm tilkobler			<b>Konstant</b> i 8 sek.	<b>Konstant</b>
Frakobling ved læser	<b>Blink</b> i 8 sek.	<b>Blink</b> i 8 sek.	<b>Konstant</b> (max 8 sek.)	<b>Konstant</b>
Tyverialarm frakobler			<b>Blink</b> i 8 sek.	<b>Blink</b> i 8 sek.
Tidsforskudt tilkobling godkendt	<b>Blink</b> i 8 sek.	<b>Blink</b> i 8 sek.	<b>Blink</b> i 8 sek.	<b>Blink</b> i 8 sek.

Generelt kan siges, at

- Konstant tændt lysdiode betyder, at tyverialarmen er tilkoblet.
- Blink (5 Hz) betyder at tyverialarmen er frakoblet, men er i en fase, hvor den skal ændre, eller har ændret tilstand (tyverialarm er lige frakoblet eller der er sendt besked til tyverialarm, at den skal tilkoble, men der er endnu ikke modtaget bekræftelse fra tyverialarmen på tilkoblingen).



## Lokal-DAS

Lokal-DAS bruges, hvis der kun er én adgangsvej til det område som tyverialarmen styrer.

Lokal-DAS udveksler ikke informationer med andre k-punkter, men fungerer helt selvstændigt i det k-punkt, der giver adgang til området som tyverialarmen overvåger. Det er dog muligt fra udvalgte læsere, at lave en total tilkobling af alle lokal-DAS'er og gruppe-DAS'er.

Der er ingen begrænsning i antallet af lokal-DAS'er. Der kan oprettes én i hvert k-punkt.

## Gruppe-DAS

Gruppe-DAS bruges, hvis der er mere end én adgangsvej til det område som tyverialarmen styrer, eller hvis k-punktet indgår i et hierarki af over-DAS'er og under-DAS'er. Læs nærmere om muligheder med DAS-grupper i afsnit 3.11 DAS-grupper.

K-punkter, der giver adgang til det samme tyverialarmområde, tildeles samme DAS-gruppe.

K-punkter i samme DAS-gruppe udveksler DAS-informationer med hinanden om manuel frakobling, manuel tilkobling og programmering af tidsforskudt tilkobling.

Der er ingen begrænsninger på antallet af k-punkter i en DAS-gruppe.

Der kræves ingen specielle kabler mellem k-punkterne i en DAS-gruppe, kun at den normale kommunikationsforbindelse er intakt. DAS funktionaliteten er således uafhængig af installationspc'en, som således godt kan slukkes.



Alarmstyrings-udgang og tilbagemeldings-indgang vælges i det k-punkt der er nærmest tyverialarmen (k-punktet skal selvfølgelig være medlem af den DAS-gruppe, der giver adgang til det aktuelle område).

Som prealarm udgang kan der frit vælges en udgang i et eller flere k-punkter. Det er således muligt, at have en prealarm ved hvert k-punkt i DAS-gruppen, uden at skulle trække særskilte kabler rundt til flere lydgivere fra et k-punkt. Udgangen kan udmærket parallelkobles med den udgang (Out2), der er forbundet til lyd giveren som angiver, at døren ikke er lukket.

### **Opsætning i DAS-grupper**

Alle parametre der er fælles for k-punkter i en DAS-gruppe indsættes i det særskilte objektvindue [DAS grupper]. Dette letter administrationen betydeligt, da der kun skal ændres et sted, ændringer vil derefter automatisk blive sendt til alle k-punkter, der er medlem af den pågældende gruppe. De parametre der er fælles for alle k-punkter i gruppen, bliver vist men kan kun ændres i objektvinduet [DAS grupper].

### **Arbejdstids tidstabel**

Denne tidstabel angiver, hvornår det er normal arbejdstid. Når alarmen frakobles indenfor arbejdstiden, forbliver den frakoblet indtil arbejdstidens ophør. Udenfor arbejdstiden anvendes købetid.

Anvendes tidstabellen <altid>, er det altid arbejdstid, hvilket betyder, at alarmen ikke tilkobles automatisk, med mindre der anvendes en bagstopper tidstabel.

Anvendes en tom tidstabel, er det aldrig arbejdstid, og der anvendes derfor altid købetid.

Ved udløb af arbejdstid tilkobles alarmen automatisk efter en prealarm.

### **Frakoble ved arbejdstid start**

Hvis dette kryds er sat, frakobles alarmen automatisk når arbejdstiden starter. Denne funktion kan vælges, hvis døren automatisk skal være oplåst, når den første person møder om morgenen, og denne person ikke skal oplåse med nøgle.

### **Købetid**

Købetid anvendes, når alarmen frakobles udenfor arbejdstiden. Hver gang der anvendes en gyldig nøgle, udskydes den automatiske alarmtilkobling i denne tid. Hvis købetiden fx er 2 timer, tilkobler alarmen automatisk 2 timer efter sidst anvendte gyldige nøgle. Dog kan en anden funktion tilkoble alarmen tidligere, fx bagstopper tidstabel, manuel tilkobling eller tidsforskudt tilkobling.

Vær opmærksom på, at hvis der er indtastet en tidsforskudt tilkobling, vil alarmen ikke tilkoble ved udløb af købetid, men først på det valgte tidspunkt.

Kommer den automatiske tilkoblingstid indenfor arbejdstiden, vil tilkoblingen først ske ved udløb af arbejdstiden.

Ved udløb af købetid tilkobles alarmen automatisk efter en prealarm.

Sættes købetiden til 00:00 er købetiden uendelig, dvs. efter en frakobling uden for arbejdstiden tilkobles alarmen først igen, når det gøres af en anden funktion, fx manuel tilkobling.

## **Bagstopper tidstabel**

Denne tidstabel bruges til at tvangstilkoble tyverialarmen på bestemte tidspunkter. Tidstabellen indeholder en række tidsperioder, men det er kun "til"-tiden der bruges. Når en af perioderne i tabellen udløber, afgives en prealarm hvorefter alarmen tilkobles.

Bagstopper tidstabel vil også kunne tilkoble alarmen i arbejdstiden.

Vær dog opmærksom på, at en tidsforskudt tilkobling sætter bagstoppertidstabellen ud af drift til efter det tidsforskudte tilkoblingstidspunkt.

## **Udlæser**

Her vælges hvad "udlæseren" skal bruges til. Det kan vælges, om udlæseren skal oplåse døren, bruges til at købe tid i eller begge dele.

Skal udlæseren kun bruges til at registrere, hvem der forlader lokalet, vælges funktionen [Kun oplåsning - ingen købetid eller alarmstyring], så undgår man, at personer der forlader lokalet, automatisk køber tid i området.

Skal udlæseren udelukkende bruges til at købe tid med, kan den placeres midt i lokalet og funktionen [Ingen oplåsning - kun købetid og alarmstyring] vælges. Herved undgås, at personer der køber tid også oplåser døren.

## **Tilbage melding fra tyverialarm**

Denne funktion giver mulighed for fuld integration mellem adgangskontrol og tyverialarm.

Som følge af denne integration er der fuld "korrespondance" mellem tyverialarmen og låsecomputerens DAS funktion. Dette medfører blandt andet, at både tyverialarmen og DAS-funktionen kan tilkobles og frakobles fra såvel adgangskontrollen som fra tyverialarmens betjeningspanel.

Tilbage melding fra tyverialarmen giver endvidere den fordel, at brugeren der tilkobler tyverialarmen ved læseren, får en bekræftelse på, at tyverialarmen faktisk også har tilkoblet. Når tilkoblingskviktering modtages fra tyverialarmen, skifter den gule lysdiode fra blink til konstant lys.

Hvis fx tyverialarmen tilkobles via tyverialarmens betjeningspanel, vil alle døre, der giver adgang til de tilkoblede områder, automatisk låse.

Kan tyverialarmen altid tilkobles, og skal den kun betjenes fra adgangskontrollen er det ikke nødvendigt med tilbage melding fra tyverialarmen.

## **Indgang (tilbage melding)**

Ønskes det at anvende tilbage melding fra tyverialarm, forbindes en signalledning fra tyverialarmen, der angiver, om tyverialarmen er tilkoblet eller frakoblet, til en valgt indgang på låsecomputeren. Indgangen er flankestyret, og lavt niveau angiver, at tyverialarmen er tilkoblet.

Indgår k-punktet i en DAS-gruppe, forbindes signalet kun til et k-punkt i gruppen. Dette k-punkt vil så sende informationen til de andre k-punkter.

## **Alarmstyring Udgang**

Denne udgang bruges til at styre tyverialarmen. Når DAS'en ønsker at frakoble tyverialarmen, er udgangen aktiveret. På den måde bliver tyverialarmen tilkoblet, hvis kablet bliver

klippet over, hvis låsecomputeren slukkes eller lignende. Hvis ikke udgangen skal styre tyverialarmen slettes checkboksen. Det er især gældende for DAS-grupper, hvor det sjældent har nogen mening at lade mere end ét k-punkt styre tyverialarmen.

### **Forsinket oplåsning**

Ved nogle tyverialarmer kan der gå flere sekunder fra de modtager besked om at frakoble til de faktisk frakobler. For at forhindre, at personen der frakobler alarmen, går ind i et område med stadig tilkoblet alarm, kan oplåsning af døren forsinkes mellem 0 og 15 sekunder.

Er funktionen ”Tilbage melding fra tyverialarm” aktiveret, vil døren først oplåse, når låsecomputeren modtager besked fra tyverialarmen om, at den er frakoblet. Hvis tyverialarmen af en eller anden grund ikke frakobler, vil døren oplåse efter en forsinkelse på 15 sekunder.

### **Prealarm ved manual tilkobling**

Med denne checkboks vælges, om der skal afgives en prealarm, når alarmen tilkobles manuelt. Hvis der alligevel er andre personer i huset, som ikke ønsker alarmen tilkoblet, har disse personer mulighed for at frakoble alarmen igen, inden den rent faktisk bliver tilkoblet.

### **Prealarm Udgang**

Denne udgang er beregnet til en lyd giver, der afgiver et prealarm signal før alarmen tilkobles.

En prealarm afgives altid før en automatisk alarm-tilkobling, så personer i området kan nå at forlade det eller købe tid.

Hvis ikke udgangen skal styre en lyd giver, slettes checkboksen. Hvert k-punkt i en DAS-gruppe kan udmærket have sin egen lyd giver, hvis der fx skal bruges flere lyd givere for at dække hele alarmområdet.

### **Prealarmtid**

Det kan her vælges, i hvor lang tid prealarmen skal være aktiv, før alarmen tilkobles.

Ved automatiske tilkoblinger afgives der altid prealarm. Der er kun prealarm ved manuel tilkobling, hvis [Prealarm ved manuel tilkobling] er valgt.

Efter udløb af prealarmen tilkobler tyverialarmen automatisk.

### **Prealarmsignal**

Disse to tider bestemmer, hvordan prealarmen skal lyde. Når prealarmen starter, aktiveres udgangen i [On] tiden. Derefter holdes der pause i [Off] tiden, hvorefter der startes forfra, indtil [Prealarmtid] er gået.

Tiden indsættes i 1/10 sekunder, og skal være mindre end 999,9 sekunder.

### **Tidsforskudt tilkobling tilladt**

Tidsforskudt tilkobling kan anvendes, hvis brugeren ønsker at tilkoble tyverialarmen på et brugerbestemt tidspunkt, fordi det den pågældende dag måske er uhensigtsmæssigt at anvende købetid.

Alarmen tilkobles som ved normal tilkobling, blot efterfølges stjernetallet af et klokkeslæt (<\*xxxhhmm>), hvorefter en gyldig nøgle anvendes. Stjernetallet "xxx" kan være 1 til 3 cifre, mens tidspunktet "hhmm" altid skal angives med 4 cifre.

Ved tidsforskudt tilkobling afgives altid prealarm før alarmtilkobling.

Hvis alarmen allerede er tilkoblet, kan tidsforskudt tilkobling ikke programmeres.

Tidsforskudt tilkobling har højeste prioritet, og tilsidesætter derfor alle andre automatiske tilkoblinger, dvs. at alarmen ikke tilkobles ved udløb af arbejdstid, købetid og bagstopper.

En tidsforskudt tilkobling kan kun ophæves ved at tilkoble alarmen manuelt eller ved at lade den tilkoble på det indtastede tidspunkt.

Det indtastede tilkoblings-tidspunkt kan programmeres om ved at indtaste en ny tid.

### **\*-tal for manuel tilkobling**

Det tal (stjernetal), brugeren skal indtaste ved læseren for at tilkoble alarmen manuelt. Efter indtastning af tallet skal der indlæses en gyldig nøgle. Alarmen tilkobles først efter den tid der er angivet i [Forsinket tilkobling]. Hvis der er valgt [Prealarm ved manuel tilkobling] afgives der først en prealarm før tilkoblingen foretages.

Som \*-tal kan der vælges et tal mellem 0 og 254. Det anbefales generelt at benytte "0".

Bruges en berøringsfri læser fra Unitek vil den automatisk sende <\*0> når nøglen holdes foran læseren i 5 sekunder, og alarmen vil derefter tilkoble.

### **\*-tal for total tilkobling**

Denne funktion er som funktionen [\*-tal for manuel tilkobling], dog med den tilføjelse at samtlige lokal-DAS'er og gruppe-DAS'er i netværket tilkobles.

Som \*-tal kan der vælges et tal mellem 0 og 254. Det anbefales generelt at benytte "0" ved alle døre for såvel lokal som total tilkobling (lettere for brugeren).

Skal brugeren ved en given dør have mulighed for at vælge mellem en total og lokal tilkobling, er det selvfølgelig nødvendigt med to forskellige \*-tal, men normalt ønsker man kun lokal tilkobling når lageret, tegnestue, kantine mv. forlades, men en total tilkobling når huset forlades gennem hoveddøren.

### **Forsinket tilkobling**

Efter udløb af prealarm og ved manuel tilkobling uden prealarm, er alarmen pr. definition tilkoblet, og det logges som tilkoblet. Den faktiske alarm-tilkobling kan dog forsinkes fra 0 - 99 sekunder. Dette benyttes, hvis alarmen skal tilkobles inden området forlades. Ligeledes har alarm-sensorer tid til at falde til ro.

Mens forsinket alarm-tilkobling er aktiveret, afgives der et signal på prealarm udgangen, der er 1 sek. on og 2 sek. off.

### **Tomt område tilkobler**

Områdevisning kan samarbejde med DAS'en, således at når det tilknyttede område bliver tomt, sender Områdevisningen (pc-programmet) en "manuel tilkobling" besked til DAS'en om at tilkoble tyverialarmen i de relevante alarmområder. Omvendt vil en DAS tilkobling automatisk tømme det tilknyttede område for personer.

Flere DAS'er kan godt være tilknyttet det samme område, således at når dette område bliver tomt, tilkobles DAS'en i flere alarmområder.

Det anbefales at områdets arbejdstidstabel anvendes i stedet for DAS arbejdstidstabel og bagstoppertidstabel, når området styrer DAS.

Denne funktion kræver, at k-punkter er online i pc-programmet.

### **Frakobling**

Når DAS'en er tilkoblet, kan sikkerhedsniveauet hæves over det skemalagte sikkerhedsniveau, således at der kræves både nøgle og PIN-kode og/eller en masternøgle for at frakoble DAS'en (Masternøgler er nøgler i k-punktet med adgang jævnfør tidstabellen <Altid>).

### **Gul lysdiode**

Den gule lysdiode i læseren angiver status for en frakobling, tilkobling og tidsforskudt tilkobling af tyverialarmen.

Denne funktion giver mulighed for to typer status visning. Den mest sikre viser kun status i 8 sekunder hvorefter den slukker igen. Alternativt kan vælges, at lysdioden er tændt konstant når tyverialarmen er tilkoblet.

Af sikkerhedsmæssige grunde kan det være uheldigt, at den gule lysdiode er tændt konstant når tyverialarmen er tilkoblet (indbrudstyve er jo ikke altid dumme), men en gang i mellem kan det være rart for de ansatte, at de til enhver tid kan se om alarmen er tilkoblet, måske specielt på de indre alarmområder.

## **3.10.5 Personer**

Denne side er en ren informationsside, og der kan ikke foretages ændringer på siden. Siden viser en liste over alle de personer, der har adgang, og efter hvilken tidstabel. Tidstabellen indeholder tider for, hvornår k-punktet kan passeres. Endvidere oplyses status for nøglen som kan være:

[Nøgle ikke gyldig]      Nøglen udenfor en gyldighedsperiode.

[Nøgle ikke aktiv]      Personens nøglekode er ikke aktiveret.

Siden kan være en god hjælp, hvis fx lagerforvalteren ønsker en liste over alle de personer der har adgang til hans lager. Han behøver altså ikke at gennemgå hver enkelt persons adgangsrettigheder, for at se hvem der kan komme ind på lageret.

## **3.10.6 Tidstabeller**

Denne side er en ren informationsside, og der kan ikke foretages ændringer på siden. Siden viser en liste over de tidstabeller, der bruges i k-punktet. Hvert k-punkt kan anvende op til 50 tidstabeller.

## **3.10.7 Logopsætning**

Et k-punkt kan sættes op til at logge hændelser i k-punktet. De hændelser der er afmærket, logges i k-punktet, men kun indenfor de perioder der er angivet i tidstabellen for hver hændelse.

En hændelse kan give en skærm-alarm, som vises i Poller og Alarmvisning.

### 3.10.8 Indgange

Hvert k-punkt har 8 indgange som individuelt kan sættes op til at logge, når niveauet skifter fra høj til lav og/eller lav til høj. De kan ligeledes give en alarm som beskrevet under logopsætning.

Hvert "indgangs-niveau" (høj og lav) kan have sin egen beskrivelse. Angives der en beskrivelse, bruges den alle de steder hvor niveau-skift på en indgang vises, fx i loggen, skærm-alarm, k-punkt oversigt osv.

### 3.10.9 Udgange

Hvert k-punkt har 8 open-collector udgange + 3 CMOS-udgange til lysdioder. En open-collector udgang er aktiv lav når den er "aktiv" (on), mens en CMOS udgang giver +5 Volt når den er aktiv (on).

Hvert "udgangs-niveau" (høj og lav) kan have sin egen beskrivelse. Angives der en beskrivelse, bruges den alle de steder hvor niveau-skift på en udgang vises, fx i loggen, skærm-alarm, k-punkt oversigt osv.

Det anbefales at bruge udgangene med de største numre først, da k-punktet selv starter med de laveste numre.

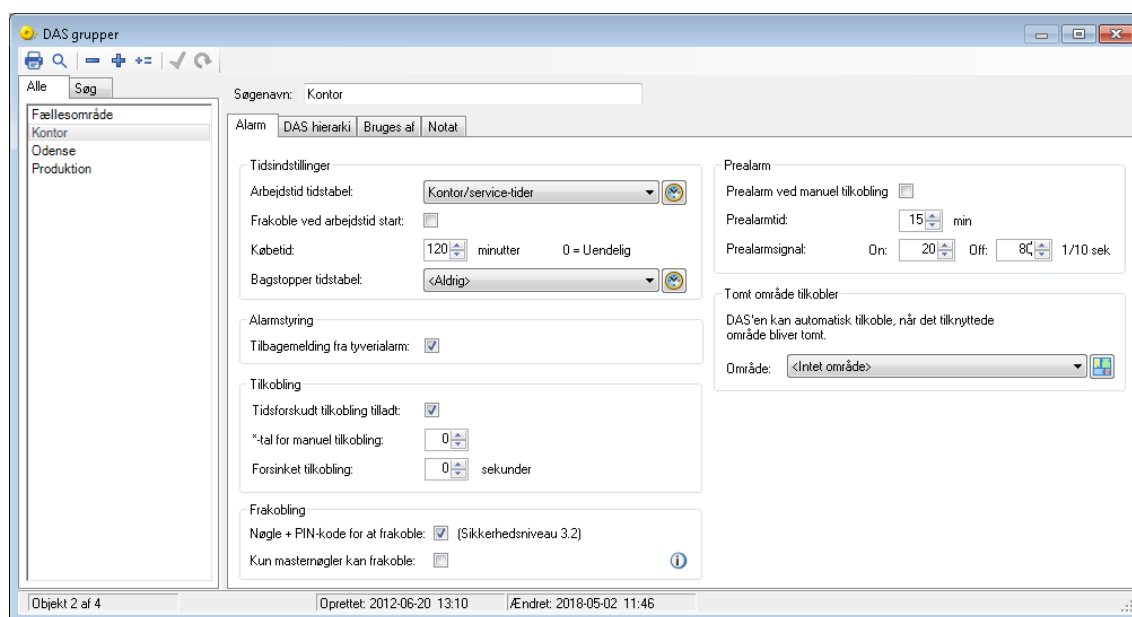
Vær sikker på at udgangene kun bruges til én ting, da flere funktioner ellers kan modarbejde hinanden. Fx er udgang 2, 3 og 4 reserverede, hvis der er overvågning på døren, og disse kan derfor ikke også bruges til tidsstyring. De kan godt bruges hvis der ikke er overvågning på døren.

Udgangene kan tvangsstyres til at være konstant on eller off eller følge en bestemt tidstabel.

[Ingen styring]	Der er ingen tvangsstyring af udgangen, dvs. den kan benyttes af andre funktioner i programmet, fx dørstyring, alarmstyring.
[Tvangsstyret ON]	Udgangen er konstant on. Hvis en anden funktion prøver at ændre tilstanden på udgangen, bliver den automatisk ændret tilbage til on.
[Tvangsstyret OFF]	Udgangen er konstant off. Hvis en anden funktion prøver at ændre tilstanden på udgangen, bliver den automatisk ændret tilbage til off
[Tidsstyret]	Udgangen er on indenfor de perioder der er angivet i tidstabellen, mens den er off udenfor perioderne.

Skiftes der fra en af de tre tvangsstyrings tilstandene til [Ingen styring], vil udgangen forblive på det niveau (on eller off), som den var på før skiftet.

## 3.11 DAS-grupper



Formålet med DAS-grupper (Decentral Alarm Styring) er at samle administrationen af alarmstyringen for de k-punkter, som giver adgang til det samme tyverialarmområde. Det medfører, at hvis der laves en ændring i en DAS-gruppe, vil denne ændring påvirke alarmstyringen i alle de k-punkter, der bruger den pågældende DAS-gruppe. Bemærk at k-punkter i samme DAS-gruppe skal være i samme lokalitet, da DAS informationer udveksles i lokalitetens 'netværk'.

Der kan oprettes ubegrænset antal DAS-grupper, dog max 63 DAS-grupper per lokalitet.

Før der laves ændringer i en DAS-gruppe, er det altid en god ide at kigge på fanebladet [Bruges af]. Her oplyses det, hvem der bruger den pågældende DAS-gruppe, og som eventuelle ændringer vil påvirke.

### 3.11.1 Alarm

Alle parametre der er fælles for k-punkter i en DAS-gruppe, indsættes på denne side. Der er ingen forskel på opsætning af gruppe-DAS og lokal-DAS. Derfor henvises til beskrivelsen for DAS i k-punktet i afsnit 3.10.4 DAS.

### 3.11.2 DAS hierarki

DAS-grupper kan opbygges i et eller flere hierarkier af over-DAS'er og under-DAS'er (overområder og underområder). Når der købes tid i en DAS-gruppe, købes der også tid i alle dens over-DAS'er. Ved tilkobling af en DAS-gruppe, tilkobles også alle dens under-DAS'er.

For hver DAS-gruppe der indgår i hierarkiet, vælges denne gruppes nærmeste over-DAS.

Sammenhæng mellem hændelser i over-DAS og efterfølgende handling i over-DAS og under-DAS'er er:

Hændelse i over-DAS	Over-DAS	Under-DAS
Arbejdstid udløb. Bagstoppertid udløb.	Prealarm startes.	Prealarm startes.
Manuel tilkobling. Tømning af det valgte område i [Tomt område tilkobler].	Prealarm startes, hvis [Prealarm ved manual tilkobling] er aktiveret, ellers tilkobles.	Prealarm startes, hvis [Prealarm ved manual tilkobling] er aktiveret i under-DAS, ellers tilkobles.
Tidsforskudt tilkoblingstid programmeres på læser.	Tidsforskudt tilkoblingstid programmeret.	Tidsforskudt tilkoblingstid synkroniseres fra over-DAS, hvis [Tidsforskudt tilkobling tilladt] er aktiveret i under-DAS, ellers ingen handling.
Tidsforskudt tilkobling tidspunkt.	Prealarm startes.	Prealarm startes, hvis [Tidsforskudt tilkobling tilladt] er aktiveret i under-DAS, ellers ingen handling.
Frakobling	Frakobling	Ingen handling.

Sammenhæng mellem hændelser i under-DAS og efterfølgende handling i under-DAS og over-DAS'er er:

Hændelse i under-DAS	Under-DAS	Over-DAS
Arbejdstid start.	Frakobling, hvis [Frakobl ved arbejdstid start] er aktiveret, eller ingen handling.	Ingen handling.
Manuel frakobling. Første person ankommer i det valgte område i [Tomt område tilkobler].	Frakobling, hvis [Arbejdstid tidstabel] er ON, ellers startes [Købetid].	Frakobling, hvis [Arbejdstid tidstabel] er ON i over-DAS, ellers startes [Købetid].
Tilkobling	Tilkobling	Ingen handling



## 3.12 Lokalteter

En lokalitet er en samling af k-punkter der har forbindelse med hinanden på det samme kommunikationsnet (RS485 eller Ethernet). Er der langt til nogle k-punkter, kan disse med fordel oprettes i en eller flere eksterne lokaliteter. Polleren kan etablere forbindelse med et ubegrænset antal lokaliteter.

Polleren kan køre 153 opgaver (tråde) samtidig, og kan derfor på samme tid polle 103 lokaliteter, fordelt på 2 lokale lokaliteter, 200 kontinuerlig pollede IP lokaliteter og 1 tidsstyret polling (4 COM port modem lokaliteter og 4 IP modem lokaliteter). Den tidsstyrede IP poller og de 8 modem pollere kan hver indeholde et ubegrænset antal lokaliteter.

### 3.12.1 Forbindelse

Forbindelsen til en lokalitet kan etableres direkte via Poller pc'ens netkort, USB kommunikationsport, RS232 kommunikationsport, med modem over telefonnettet (analog eller GSM) eller med en COM Server (CV72/LS10-IP) over et IP-netværk (pc-netværk og/eller internet).

Ved at slette checkboksen [Polles] er det muligt at stoppe polling af alle k-punkter i en lokalitet. Dette kan bruges ved test, og hvis en lokalitet midlertidigt ikke skal polles.

### **3.12.1.1 IP-netværk lokalt**

Polleren kan kommunikere direkte med k-punkter i en lokal IP installation via pc'ens netkort.

Pc'en kommunikerer direkte med alle k-punkter (LS10-IP) i lokaliteten. Der kommunikeres via multicast protokollen, hvorfor kommunikationen som sådan fungerer uden brug af IP-numre, DHCP-server, gateways, routere mv.

Hver LS10-IP kan fungere som gateway til et RS485-net uden yderligere konfiguration, således at et RS485 også kan polle via denne lokalitetstype.

Denne lokalitetstype kan ikke nå enheder, der ligger bag ved udstyr, der stopper for multicast eller tæller TTL-værdien (Time-To-Live på IP-pakker) ned.

#### **Netværksforbindelse**

IP baserede k-punkter kan låses til den oprettede lokalitets netværk med en adgangskode, som således beskytter k-punkterne mod hijacking. Selvom der ikke anvendes adgangskode, så er kommunikationen altid krypteret og beskyttet mod replay og manipulation.

### **3.12.1.2 IP-netværk via Gateway**

Polleren kan via TCP/IP (internet-protokollen) etablere krypteret forbindelse over pc-netværk og internet til en COM Server gateway (CV72 eller LS10-IP) på lokaliteten. De låsecomputere der er i lokaliteten kommunikerer via kommunikationsnettet i lokaliteten - Ethernet eller tilslutning direkte til COM Serverens RS485 kommunikationsport.

#### **Netværksforbindelse**

For at polleren kan etablere en IP-forbindelse med COM Serveren, skal den IP-adresse og det port-nummer som COM-serveren har fået tildelt, indtastes. Tildeling af COM Serverens IP-adresse skal foretages i nært samarbejde med firmaets netansvarlige.

Går kommunikationen mellem Polleren og COM Serveren over internettet og gennem en internet-router med Port mapping (Exported Services - NAT, Network Address Port Translation), er det ikke COM Serverens IP-adresse der skal indtastes men routerens offentlige IP-adresse (WAN adresse). Routeren bruger så port-nummeret til at videresende data til en IP-adresse på det lokale pc-net (LAN).

Port mapping giver også mulighed for at have flere (over 65.000) COM Servere på den samme offentlige IP-adresse ved brug af forskellige port-numre.

Vær opmærksom på, at hvis kommunikationen skal ske gennem en firewall, skal denne konfigureres til at åbne for trafik på den valgte IP-port.

COM Serveren kan beskyttes ekstra med en adgangskode, som gør det umuligt at ændre parametre uden kendskab til adgangskoden. For optimal sikkerhed bør enheden tildeles en adgangskode på et lukket netværk, før den eventuelt flyttes til et offentligt netværk.

For yderligere information vedrørende netværksopsætning, se manual til COM Server CV72.

### **Kontinuerlig polling**

Kontinuerlig polling bruges, når det ønskes at ændringer og tilføjelser i databasen så hurtigt som muligt kommer ud til lokalitetens k-punkter. Endvidere hentes log hændelser løbende i k-punkterne.

En kontinuerlig pollet lokalitet har reelt sin egen poller, og polles samtidig og uafhængig af andre lokaliteter. Der kan oprettes op til 27 kontinuerligt pollede lokaliteter. Skal der oprettes flere end 27 lokaliteter, oprettes disse blot som tidsbestemte lokaliteter, hvor den periodiske opkaldstid kan sættes så lavt som 1 minut mellem hver polling.

Ved kontinuerlig polling vil k-punkterne i lokaliteten blive pollet efter samme pollingsprincip, som de k-punkter der er tilsluttet den lokale USB-port på poller pc'en.

### **Tidsbestemt polling**

I sammenligning med den båndbredde der normalt er til rådighed på et pc-netværk, er det yderst begrænset hvor meget båndbredde pollingen over netværk kræver. Men i hårdt belastede netværk eller hvor forbindelsen etableres over en VPN forbindelse (Virtual Private Network), kan det være ønskeligt at nedbringe netværkstrafikken så meget som muligt. Derfor kan systemet programmeres til at kalde lokaliteten op på bestemte tidspunkter af døgnet.

Når der anvendes tidsbestemt polling af lokaliteten, checkes låsecomputerne i lokaliteten på samme måde som ved en modem opkobling.

#### **3.12.1.3 USB**

Når der skal kommunikeres med låsecomputere i en lokal installation, benyttes Poller pc'ens USB kommunikationsport. I en afstand af maksimalt 5 meter fra pc'en skal der anbringes en USB til RS485 konverter (CV12).

#### **Lokal forbindelse**

Vælg det CV12-ID (default = 1) som Polleren skal bruge for at kommunikere med låsecomputerne i den lokale lokalitet.

#### **3.12.1.4 Modem**

Polleren kan kommunikere med k-punkter i eksterne lokaliteter gennem telefonmodem forbundet via IP eller til én eller flere af poller-pc'ens RS232 porte. Der kan tilsluttes op til 4 modems til poller-pc'en, således at Polleren kan kommunikere med 4 lokaliteter på samme tid. I lokaliteterne anbringes et modem med RS485 tilslutning (CV61). Alle låsecomputere i lokaliteten forbindes til dette RS485 net.

#### **Modemopsætning**

Vælg den IP-adresse og port eller COM-port (1-4), der skal polle den aktuelle lokalitet. Som modem kan vælges mellem et [Standard Hayes] og [Brugerdefineret]. Vælges [Brugerdefineret] skal der indtastes en initialiseringsstreng, der passer til det valgte modem.

#### **Modemforbindelse**

For at Polleren kan ringe op til en modem-lokalitet, skal telefonnummeret for lokaliteten indtastes. Telefonnummeret kan fx indtastes som 0W86614422W207. Hvor det første "0" er cifferet for at få en bylinie, det efterfølgende "W" angiver der skal ventes på klartone,

herefter følger selve telefonnummeret på lokaliteten, hvorefter der igen ventes på en klartone inden det direkte indvalgsnummer sendes.

### Tidsbestemt polling

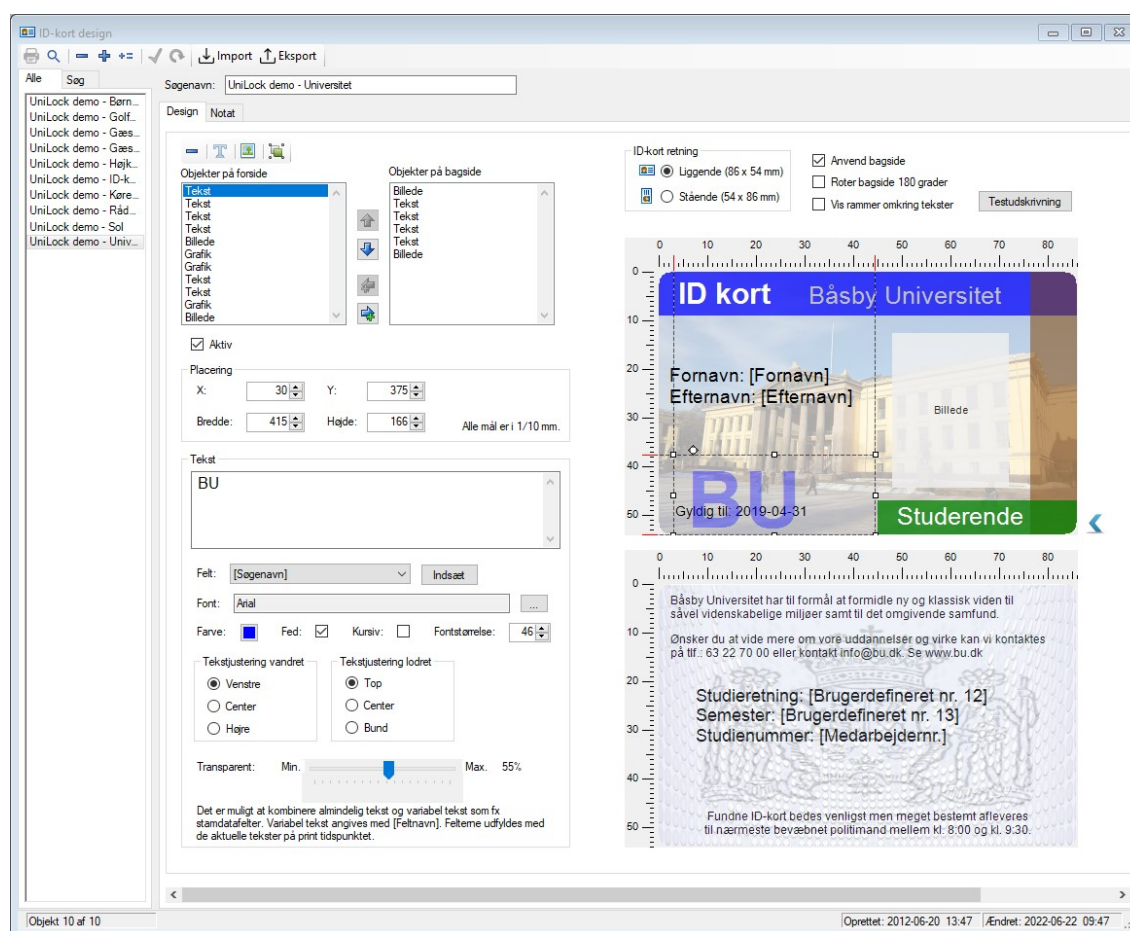
For at begrænse telefonregningens størrelse, kan systemet programmeres til at ringe til lokaliteten på bestemte tidspunkter af døgnet.

Hver gang Polleren etablerer modemforbindelse til en lokalitet, vil alle informationer om nye nøgler, slettede nøgler, ændringer i tidstabeller mv., som er foretaget siden sidste opkald, blive sendt ud til de respektive låsecomputere. Endvidere stilles uret i låsecomputerne, og alle logninger hentes. Før forbindelsen til lokaliteten afbrydes, checkes om der er overensstemmelse mellem alle checksummer i k-punkterne og pc'ens database.

## 3.12.2 K-punkter

Denne side er en ren informationsside, og der kan ikke foretages ændringer på siden. Siden viser en liste over alle de k-punkter, der tilhører den aktuelle lokalitet. Siden kan være en hjælp, hvis man vil have et hurtigt overblik over, hvilke k-punkter der i de forskellige lokaliteter.

## 3.13 ID-kort design og produktion



I ID-kort designeren er det muligt at designe ID-kort, der passer til firmaets image og behov. I [Person], [Stamdata], kan der printes ID-kort til den pågældende person, ved blot at aktivere knappen [Udskriv ID-kort].

## Profiler

Der kan i programmet oprettes et ubegrænset antal ID-kort profiler således, at ID-kortets tekst og design kan være forskellig for de enkelte medarbejdergrupper, afdelinger, adgangsniveauer, gæstekort mv. Programmet er intuitivt og nemt at bruge, og der medfølger en række ID-kort profiler, som kan inspirere eller danne grundlag for egne ID-kort design.

For hver profil kan man frit vælge om kortet skal være liggende eller stående, og om profilen også skal indeholde kort-bagside.

Personbillede, billeder, grafik og tekster kan frit placeres over alt på kortet. Man kan frit redigere hvilket element, der skal placeres forrest, bagerst mv. Transparens kan justeres på hvert element, således at kortet kan indeholde vandmærker med både firmalogo, billeder, grafik og tekster.

Ved redigering af billedstørrelse kan størrelsesforholdet bevares.

Hvert grafisk element kan redigeres mht. form, farve, gradient, gradientfarve, størrelse og placering.

Tekster kan frit kombineres ud fra fast tekst og variabel tekst, som hentes fra personens stamdata.

Hvert tekstfelt kan bestå af flere linjer, og der kan frit vælges skrifttype, skriftstørrelse, typografi, farve og tekstens justering i tekstfeltet.

I designeren kan man til enhver tid teste sit kort-design, ved at lave en testudskrivning på hvilken som helst printer på pc'en.

Hver profil kan eksporteres/importeres mellem forskellige UniLock installationer.

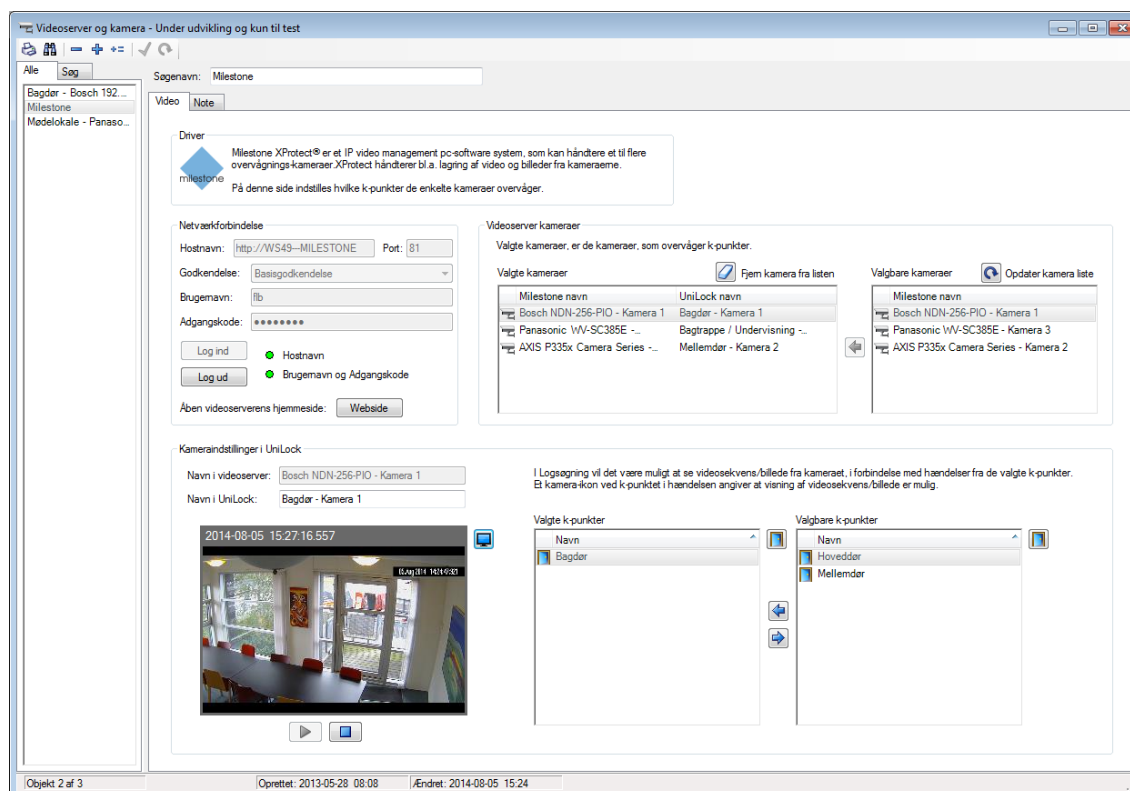
## Kortprinter

ID-kort kan printes på alle typer af kortprintere, såfremt der er installeret en standard Windows driver til den pågældende printer.

## Fonte

I ID-kort designeren kan man anvende alle standard fonte (TrueType) på pc'en.

## 3.14 Videoservert og kamera



I dette objektvindue er det muligt at oprette et vilkårligt antal videoservert og kameraer, hvorfra UniLock kan hente og afspille live video og optaget video.

Når et nyt objekt oprettes vælger operatøren om der oprettes et videoservert-system eller et kamera. UniLock kan automatisk afsøge det lokale netværk for tilsluttede IP kameraer, hvorefter operatøren kan vælge de kameraer, der skal oprettes i UniLock.

I vinduet indstilles hvilke k-punkter det enkelte kamera overvåger. Det er således muligt at ét kamera overvåger flere k-punkter, mens ét k-punkt kan blive overvåget af flere kameraer.

For at lette opsætning har vinduet et integreret afspilningsvindue til at lette valg af overvågede k-punkter.

Hvert kamera kan gives et navn, som kun anvendes i UniLock, for at lette genkendelsen af kameraet i forbindelse med video-verifikation af loghændelser. Kameraets navn i UniLock påvirker ikke kameraets navn i et eventuelt videoservert-system.

## Videoservert-systemer

Videoservert-systemer kan håndtere flere hundrede kameraer, styre lagring af optagelser, lave billedanalyse og anden avanceret funktionalitet.

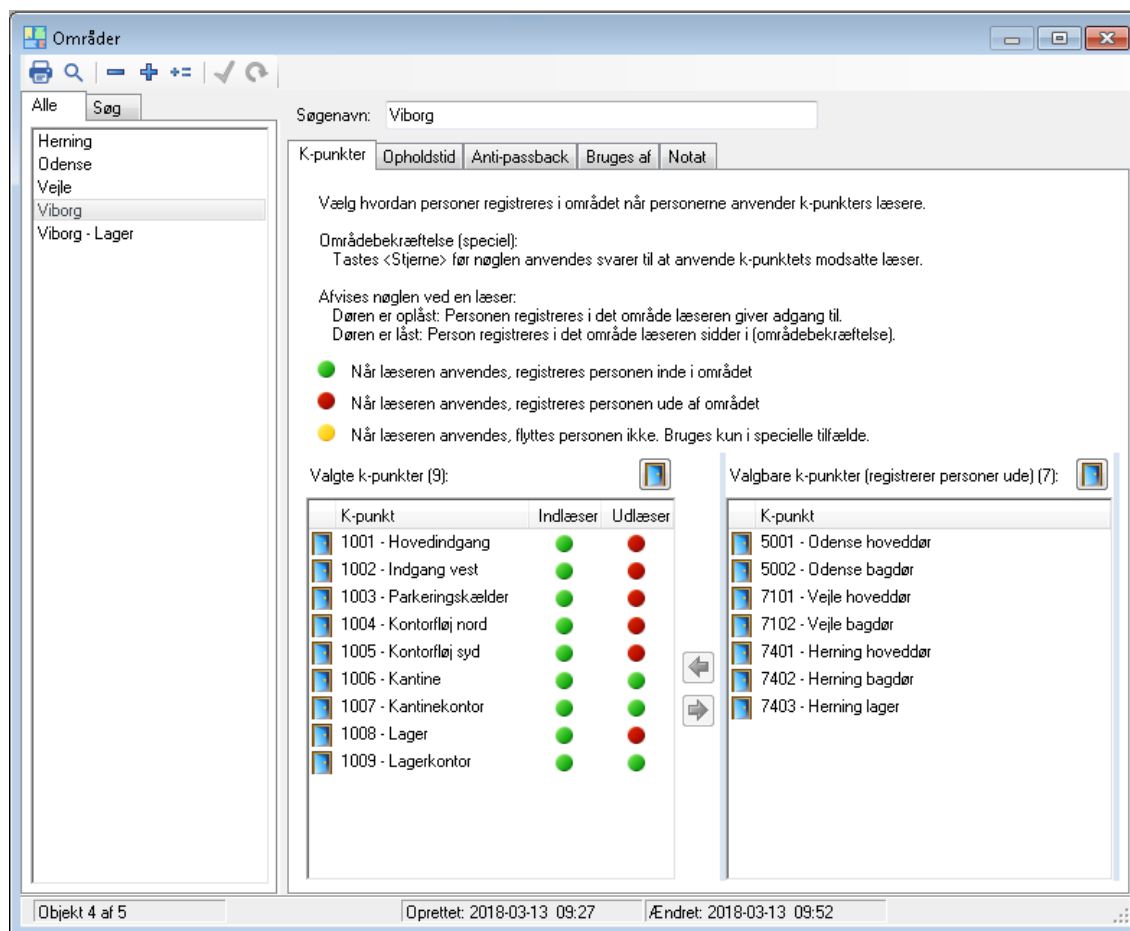
UniLock kan forbinde til IP-baserede videoservert-systemer og hente live video og optagelser, som så afspilles i vinduet [Videoafspilning].

## Kameraer

UniLock kan vise live video og afspille optagelser direkte fra IP kameraer, hvilket kan eliminere behovet for store videoservert-systemer.

Live video kan hentes fra alle kameraer, mens optagelser kan hentes fra kameraer med SD-kort eller netværkstilsluttet harddisk, da disse har en indbygget videoservert. Mht. de enkelte kameraers muligheder, service mv. henvises til kameraproducenten.

## 3.15 Områder



I dette objektvindue kan der oprettes et ubegrænset antal områder, som kan overvåges i områdevisning og anvendes til at styre tilkobling og frakobling af DAS.

For hvert område vælges de k-punkter, hvis læsere kan anvendes til at registrere personer inde i området eller ikke skal flytte personer i området.

### Opholdstid

Personers maksimale opholdstid i området anvendes til at sikre at områder automatisk tømmes for personer, der har glemt at registrere sig ude. Dette sikrer at tyverialarmen automatisk tilkobles, og at områdets personliste er tom til næste arbejdsdags begyndelse.

I hvert område angives den maksimale opholdstid i området før en person automatisk flyttes ud af området, hvis personen ikke i mellemtiden har genbekræftet sin tilstedeværelse med en ny nøgle-indlæsning.

Tiden for maksimal opholdstid kan mindskes, hvis det kombineres med en arbejdstidstabel, da maksimal opholdstid så først tæller fra udløb af arbejdstiden.

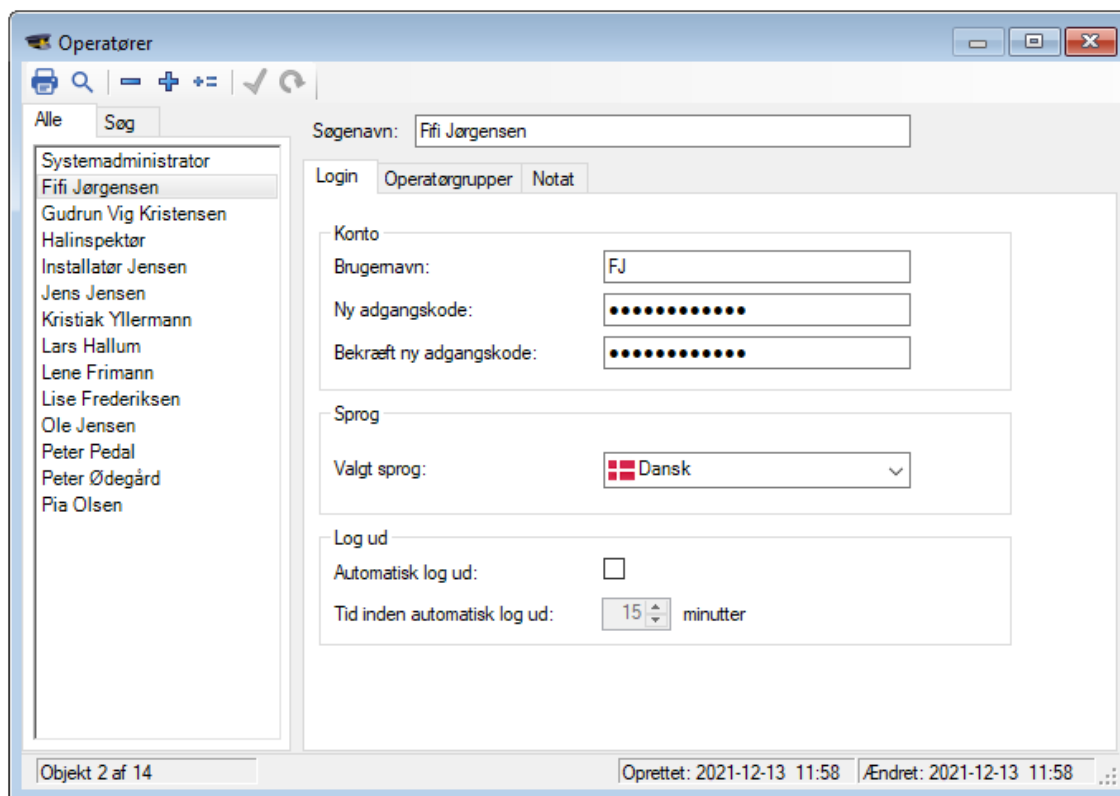
Personers aktuelle udløbstid ses i visning af området, mens udløb af opholdstid også kan vises som alarm i alarmoversigten.

### Anti-passback

Hvert område kan have egen anti-passback funktionalitet, som kan programmeres til fx at afgive skærmalarm, når en person har udvist manglende disciplin ved ikke, at stemple sig korrekt ind eller ud af området. Anti-passback aktiveres når personer forsøger at passere området i samme retning gentagne gange, altså både flere gange ud af området og flere gange ind i området.

## 3.16 Operatører

Det er muligt at oprette et vilkårligt antal operatører hver med helt individuelle rettigheder til systemet. Det er således muligt, at oprette operatører med kun lige de rettigheder der er nødvendig for, at vedkommende kan udføre sine administrative opgaver.



### Aktivering

Under Operatøren ”Systemadministrator” kan operatørmodulet aktiveres eller deaktiveres. Deaktiveres operatørmodulet skal der ikke logges ind i systemet, og operatøren vil automatisk være Systemadministrator.

### Systemadministrator

Systemet indeholder én predefineret operatør kaldet ”Systemadministrator”. Systemadministrator navn og ubegrænsede rettigheder kan ikke ændres. Systemadministrator kan efterfølgende oprette andre operatører med samme eller færre rettigheder.

Hvis Systemadministrators [Login navn] og/eller [Adgangskode] glemmes, er det ikke muligt at logge på systemet med administratorrettigheder.



## Sikkerhed

Aktiveres operatørmodul anbefales det, at oprette en ekstra systemoperatør med alle rettigheder. Denne "Ny systemadministrator" bruges så i dagligdagen som systemoperatør. Gem derefter [Login navn] og [Adgangskode] for operatøren "Systemadministrator" i en bankboks og brug kun denne operatør i nødstilfælde.

Systemadministrator kan altid tildele sig selv og alle de andre operatører nye adgangskoder.

Hvis systemadministrator ikke føler sig i stand til, at kunne huske [Login navn] og [Adgangskode], anbefales det at slette alle operatører og deaktivere operatørmodul. Herefter skal der ikke logges ind i programmet. Pc'en bør så sikres på anden måde.

Har Systemadministrator glemt sit [Login navn] og/eller [Adgangskode], kan Unitek A/S gennem leverandøren yde hjælp. Systemet kan generere en engangskode som skal sendes til Unitek A/S. Herefter modtages en åbningskode hvorefter Systemadministrator kan tildeles en ny adgangskode uden at være logget ind først.

Ud over udgiften til leverandøren beregner Unitek A/S sig honorar herfor.

### 3.16.1 Login

Hver enkelt operatør oprettes med eget [Brugernavn] og [Adgangskode]. Den ønskede adgangskode skal indtastes to gange og vises som [\*\*\*\*\*]. Af sikkerhedsmæssige grunde kan en adgangskode ikke være tom eller udlæses - heller ikke af Systemadministrator. Systemadministrator kan dog altid tildele operatøren en anden adgangskode.

Anvendes Windows domæne kan operatørens [Brugernavn] være operatørens kontonavn i domænet (fx "Unitek/JH"), mens [Adgangskode] er blankt. Dette kræver at programmodul "Integrationer" anvendes til at synkronisere operatørlogin og operatørrettigheder med Microsoft Active Directory.

## Sprog

Hver operatør kan individuelt anvende sit foretrukne sprog, således at programmet tilpasser sig det valgte sprog ved login.

### Lås program efter inaktivitet

Systemet kan automatisk låse programmet efter en given tid med inaktivitet. Har operatøren ikke været aktiv i en valgt tid mellem 1 og 600 minutter, så låses programmet og operatøren må logge ind igen for at fuldføre sit arbejde. Selv om programmet er låst, er det muligt - efter en advarsel - at logge ind som en anden operatør, eller lukke programmet, i begge situationer vil ikke gemt arbejde gå tabt.

### 3.16.2 Operatørgrupper

En Operatør har som sådan ingen rettigheder, de arves gennem medlemskabet af én eller flere Operatørgrupper. For at opnå operatørrettigheder skal operatøren altså være medlem af mindst én Operatørgruppe, som så skal indeholde de relevante operatørrettigheder.

### Medlem af flere operatørgrupper

I visse situationer kan det give mening, at operatøren er medlem af flere Operatørgrupper. Fx kan Systemadministrator være medlem af alle Operatørgrupper, Systemadministrator har

nu mulighed for, at logge ind i en ønsket Operatørgruppe, og ved selvsyn se om operatørgruppens rettigheder er som ønsket.

Hvis der i systemet oprettes Afdelinger kan operatøren have forskellige rettigheder i de forskellige Afdelinger, og det kan hurtigt skiftes mellem de forskellige Afdelinger uden at logge ud.

Er en operatør medlem af flere Operatørgrupper, så kan operatøren skifte mellem de forskellige Operatørgrupper uden at logge ud og ind igen, blot ved at vælge den nye operatørgruppe på statuslinjen.



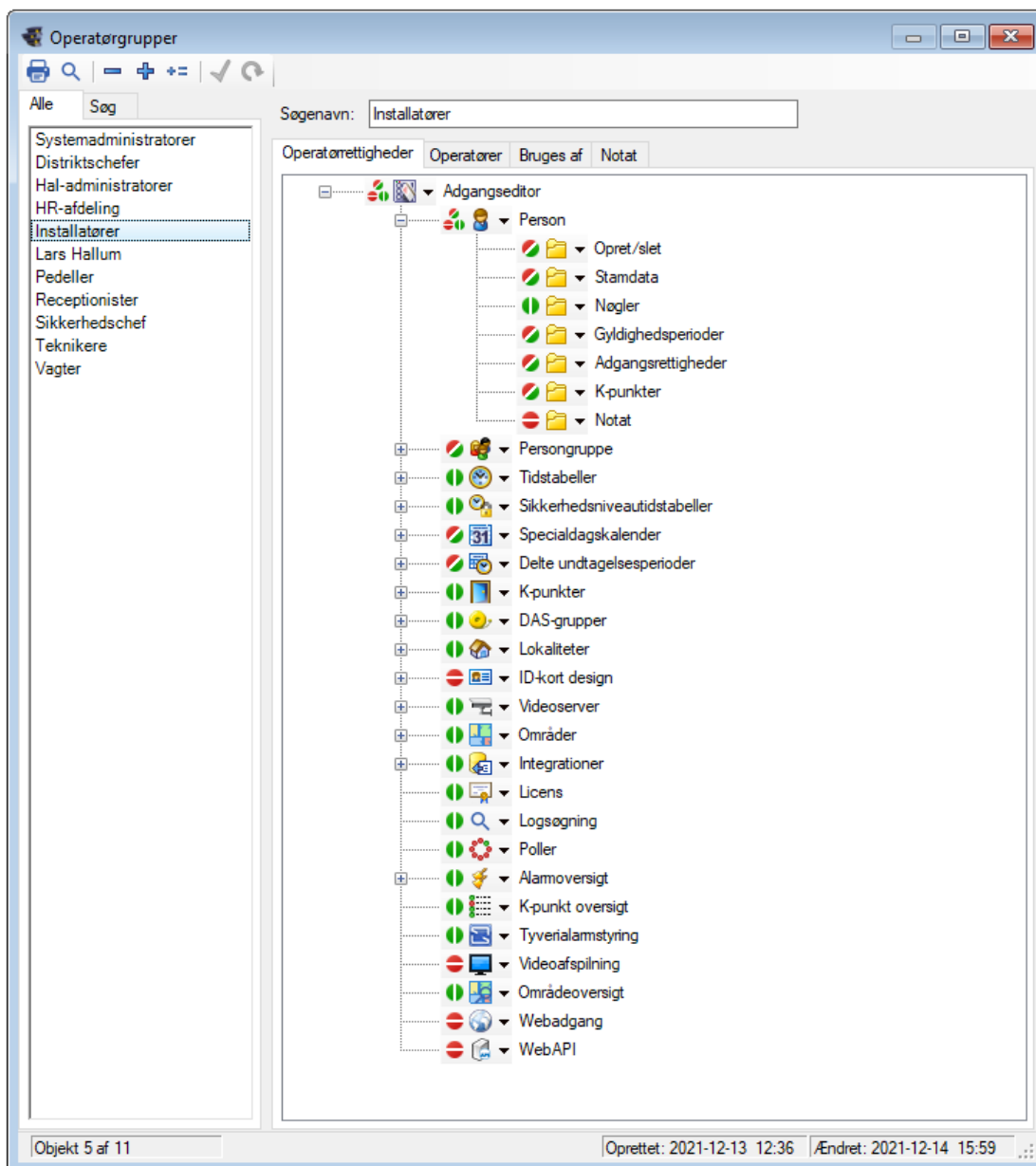
Hint: To operatører har forskellige operatørrettigheder, men i tilfælde af sygdom, kan det være praktisk, at den anden operatør kan varetage den sygemeldte operatørs administrative opgaver. Dette ønske klares let ved, at begge operatører også er medlem af den anden operatørs Operatørgruppe.

Når en operatør logger ind, og når operatøren skifter operatørgruppe logges det det i systemloggen.

### 3.17 Operatørgrupper

En Operatør får sine operatørrettigheder gennem medlemskabet af mindst én Operatørgruppe.

Det er muligt at oprette et vilkårligt antal operatørgrupper, hver med helt individuel tildeling af operatørrettigheder til systemet.



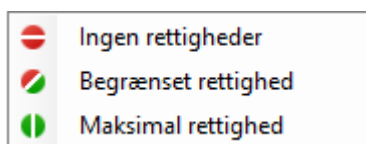
## Systemadministratorer

Systemet indeholder én predefineret operatørgruppe kaldet ”Systemadministratorer”, gruppens navn kan ikke ændres og operatøren ”Systemadministrator” kan ikke meldes ud af gruppe. Medlemskabet af denne gruppe giver ubegrænset adgang til hele systemet.

### 3.17.1 Operatørrettigheder

Operatørrettigheder kan begrænses til programmer, vinduer, faneblade og i visse tilfælde til enkelte indtastnings-felter.

Som rettighed til de enkelte objekter kan der normalt vælges mellem:



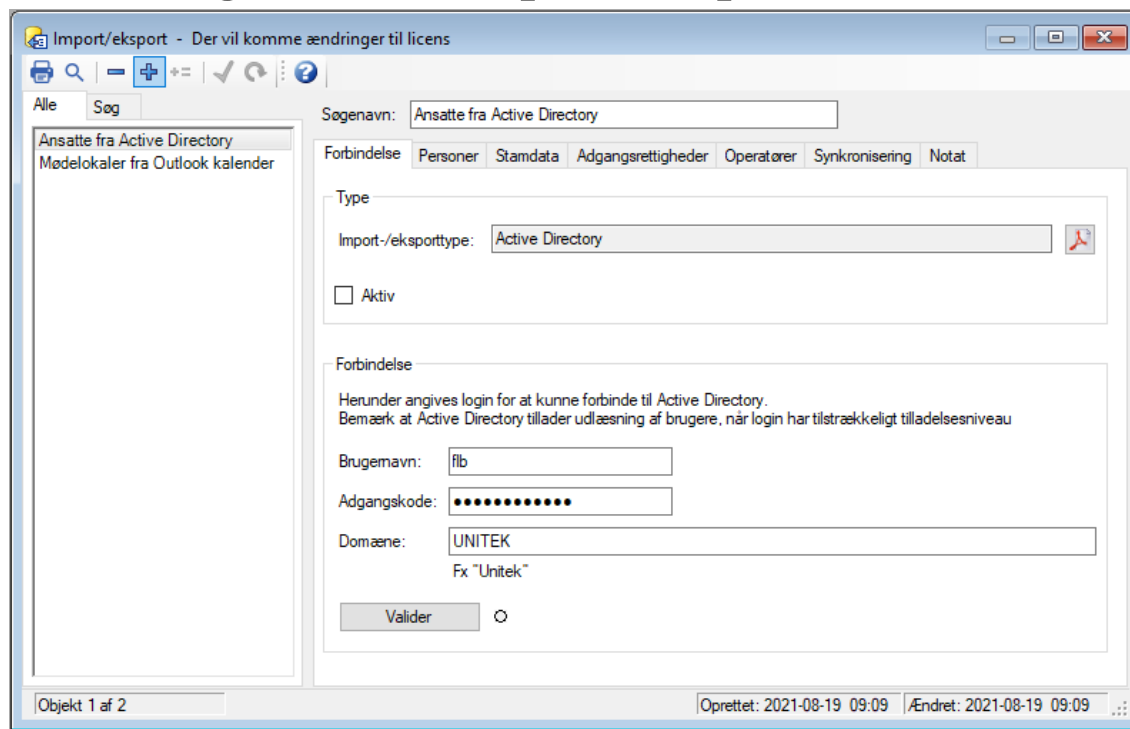
- [Ingen rettighed] Operatøren har ingen rettigheder til det pågældende objekt. Det er normalt heller ikke muligt at se informationer om objektet.
- [Begrænset rettighed] Operatøren vil normalt kunne aflæse alle informationer om objektet, men kan ikke ændre i data.
- [Maksimal rettighed] Operatøren har alle rettigheder til det pågældende objekt. Alle informationer kan ses og ændres.

### 3.17.2 Operatør

Her er det muligt at tildele Operatører medlemskab af den aktuelle Operatørgruppe. Alle de operatører der meldes ind i operatørgruppen, vil automatisk arve rettighederne i operatørgruppen.

Se ligeledes Operatørgrupper under Operatører.

## 3.18 Integrationer (Import/Eksport)



I dette objektvindue kan der oprettes et ubegrænset antal integrations-kanaler, som kan udveksle data med eksterne systemer.

UniLock har allerede indbygget integrationsdriver til mange tredjepartssystemer (Active Directory, Outlook Kalender mv.), hvor flere løbende tilføjes. En række tredjepartssystemer har allerede indbygget integration med UniLock.

## 3.19 Licens

I dette vindue er det muligt, at se ting der er relateret til programlicenser

Licens

Unitek Adgangskontrol - der virker

Installationssted | Leverandør | Rettigheder | Opdateringsaftale

Oplysninger om installationssted

Licensnavn: Unitek, Alle rettigheder

Navn: Unitek

Adresse: Vævervej 5

Postnummer og by: 8800 Viborg

Telefonnummer: 86 61 44 22

Licensnummer: [Redacted]

Licensnøgle: [Redacted]

Indtast licensnummer

Deaktiver licens (demo-mode)

Der er 29 dage tilbage af testperioden på 30 dage. Derefter kan UniLock Poller ikke længere anvendes uden aktiv licens.

Ved at deaktivere licensen sættes programmet i demo-mode, hvorved der er ubegrænset adgang til alle programmoduler. Er der i demo-mode brugt/aktiveret programmoduler, oprettet flere k-punkter mv. end der er licens til, vil programmet ikke fungere korrekt når licensen aktiveres igen, medmindre der i mellemtiden er erhvervet licens til de brugte programmoduler.

Opdater licensfil

Placering: C:\ProgramData\UniLock 2.0\Unitek.cfg

Eksisterende licensfil genereret: 2014-07-28 kl. 10:34

Hent licensfil lokalt fra medie. Er kun muligt på installations pc'en

Hent nyeste licensfil fra internet

Udskriv licensbevis OK Annuller

### Demo-mode

Indtil licensnummeret og licensnøglen er indtastet vil programmet køre uden aktiv licens (demo-mode), og der er ingen begrænsninger i programmets anvendelsesmuligheder, alle programmer og programmoduler er åbne for gennemsyn og test.

Programmet kan maksimalt køre i demo-mode i 30 dage – herefter stopper pollingen af K-punkter.

### Aktivering af licens

Efter licensbestillingen er afgivet, modtages fra leverandøren/licensudstederen et ”licensbevis”. Licensbeviset indeholder et [Licensnummer] og en [Licensnøgle], som indtastes efter at knappen [Indtast licensnummer] er aktiveret

Vær opmærksom på, at licensfilen (Cfg-fil) skal have nyere dato end datoen for selve licensbestillingen, se afsnittet ”Opdater licens”.

Når licensen er aktiveret, går programmet ud af demo-mode, og installationsstedets navn fremkommer nu på titellinjen i programmet.

Er der i demo-mode brugt/aktiveret programmoduler, oprettet flere k-punkter mv. end der er licens til, vil programmet ikke køre korrekt når licensen aktiveres.

### **Deaktiver licens**

Hvis der "her og nu" skal bruges en licensudvidelse, er det muligt at deaktivere licensen (demo-mode), hvorved der åbnes for alle programmoduler, og det er muligt at tilføje yderligere k-punkter mv. Det er tilladt at køre uden aktiv licens i den periode, hvor der ventes på ny licensfil. Når der modtages en ny licensfil, skiftes igen væk fra demo-mode og licens forholdende er igen bragt i orden.

Er der i demo-mode brugt/aktiveret programmoduler, oprettet flere k-punkter mv. end der er licens til, vil programmet ikke køre korrekt når licensen aktiveres igen, medmindre der i mellemtiden er erhvervet licens til de brugte programmoduler.

### **Opdater licens**

Alle licensrettigheder ligger i en krypteret licensfil (typisk: Unitek.cfg), der er fælles for alle installationssteder. Ved en ændring i licensforholdene er det normalt kun denne fil der skal opdateres.

Opdatering af en licensfil kan gøres på følgende måder:

1. **Aktiver knappen** [Fra internet].

Sidste nye licensfil hentes direkte fra internettet. Dette kræver selvfølgelig, at den anvendte pc har adgang til internettet.

2. **Aktiver knappen** [Fra medie].

Sidste nye licensfil hentes fra et medie (eller valgt drev/mappe). På en anden pc, som er forbundet til internettet hentes licensfilen fra Unitek's hjemmeside over på et medie. Licensfilen kan hentes på: <http://www.unitek.dk/cfg/unitek.cfg>

For at de bestilte rettigheder kan være inkluderet i licensfilen, skal licensfilen følgelig have en nyere dato end datoen for bestillingen. Feltet [Eksisterende licensfil genereret:] oplyser hvornår den installerede licensfil er genereret.

## 3.20 Systemoversigt

Systemoversigt

UniLock Version: 2.0 Build: 146 Revision: 2018-12-17

**Klient pc**

Pc navn: WS59-FL (Denne pc) IP: 192.168.1.50

Programmappe: C:\Program Files (x86)\UniLock 2.0

Pingtid [ms]: 1 Min: 1 Max: 11 Nustil

**Installations og Poller pc**

Pc navn: WS59-FL (Denne pc) IP: 192.168.1.50

Delt mappe: \\WS59-FL\UniLock 2.0

K-punkter: Vis oversigt

Installationsmappe: C:\Program Files (x86)\UniLock 2.0

Datamappe: C:\ProgramData\UniLock 2.0

**Database**

Sti (instans): WS59-FL\SQLEXPRESS2014

Database fil: C:\ProgramData\UniLock 2.0\Data\UniLockData.mdf

Log fil: C:\ProgramData\UniLock 2.0\Data\UniLockLog.mdf

Billedmappe: C:\ProgramData\UniLock 2.0\Data\Photo

Sidst opdateret: 13:06:32

Dette vindue er et rent informationsvindue, hvor der vises en række basis informationer og driftinformationer om UniLock systemet og det underliggende SQL databasesystem.

### Klient pc

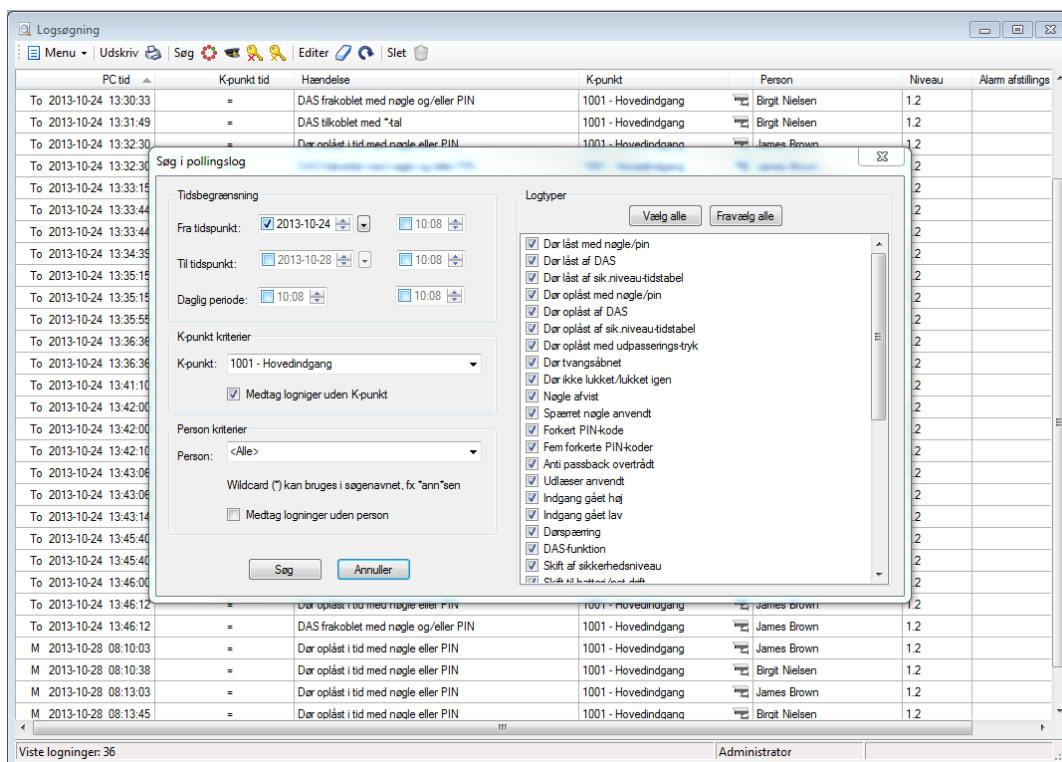
Klient pc er den pc, som operatøren har åbnet Adgangseditor på. Klient pc kan være en ekstra arbejdsstation eller selve installations- og Poller pc.

### Installations- og Poller pc

Dette er den pc eller server hvor UniLock er installeret. Det er her SQL serveren er installeret og hvor databaser er placeret.

Her angives hvor vigtige UniLock filer er placeret og status for forbindelsen til disse.

## 3.21 Logsøgning



Logsøgning viser i kronologisk rækkefølge hvad der er sket i adgangskontrolsystemet. Alle hændelser i Polleren og k-punkterne registreres med tid, hændelse, k-punkt, person, sikkerhedsniveau mv.

Logninger fra et k-punkt vil altid indeholde to tider – en for selve hændelsen i k-punktet og en tid for hvornår hændelsen er hentet hjem til pc'en. Disse to tider vil være forskellige, hvis Polleren ikke kørte på tidspunktet for hændelsen i k-punktet.

### Logsøgningsparametre

I et større system med mange personer og k-punkter kan der let blive produceret flere tusinde logninger om dagen. I sådanne systemer kan det let blive uoverkommeligt og uoverskueligt at kigge den kronologiske logliste igennem.

Operatøren kan opsætte en række søgekriterier, og programmet viser så kun de logninger, der opfylder de valgte søgekriterier. Søgningen kan begrænses vha. tidsperioder, k-punkter, personer og logtyper. Søgningen kan forfines indtil de ønskede logninger er fundet.

Alle disse oplysninger vil give operatøren et uvurderligt værktøj, til bagefter at rekonstruere hvad der skete og hvornår. Det er fx muligt at undersøge, hvor tit en bestemt person har besøgt et bestemt lokale i en udvalgt periode.

Bemærk at der kan søges med både foranstillet og bagved stillet wildcard(\*).

### Editering i logliste

Ved at markere én eller flere uinteressante logninger med musen, kan disse fjernes fra den viste logliste, således at kun relevante logninger er synlige. Dette vil igen lette operatørens opgave med at overskue hvad der er sket. Logninger fjernes ikke fra logfilen.



Markerede logninger fjernes ved at højreklikke med musen eller ved at bruge viskelæderikonet.

### **Udskrivning**

Når en logsøgning er gennemført, og eventuelt uinteressante logninger manuelt er editeret bort, kan resultatet udskrives til en printer eller CSV-fil. CSV-filer kan fx importeres i et regnearksprogram som fx Microsoft Excel for videre bearbejdning af data.

En logudskrift vil normalt kun indeholde en delmængde af ”virkelighedens” logninger, derfor indeholder starten af udskriften nøje informationer om, hvilke søgeparametre der er anvendt for logudskriften, og om der ved manuel editering er fjernet logninger.

### **Videoafspilning**

Er der integration med videoovervågning kan operatøren starte afspilning af video fra loghændelsen ved at trykke på kamera-ikonet. Dækker flere kameraer k-punktet, hvor hændelsen skete, vil et klik på kamera-ikonet vise listen af kameraer, hvorfra operatøren kan vælge det ønskede kamera.

Afspilning af video vises i vinduet [Videoafspilning], som startes med det valgte kamera og afspilningstidspunktet fra loghændelsen.

### **Se objekt**

Ønsker man at nærstudere data for personen, k-punktet eller operatøren, kan der blot dobbeltklikkes på objektet med musen og efterfølgende åbnes vinduet med data for objektet.

### **Søgning på sjældne brugte nøgler**

Som noget helt specielt er det muligt at søge på nøgler, som ikke er i brug mere, eller sjældent bruges. Dette kan bruges til at finde nøgler man har glemt at slette, eller personer der ikke benytter deres nøgler dagligt (som det måske kræves).

Derudover kan der også søges på ikke aktive og spærrede nøgler.

### **Sletning af personer**

I søgeresultatet for en søgning på [ikke gyldige nøgler] eller [sjældne brugte nøgler], er det muligt at markere en eller flere personer og efterfølgende slette de markerede personer permanent fra databasen ved at bruge skraldespandsikonet.

Slettefunktionen berører ikke logdatabasen, så alle loggede hændelser om de slettede personer bevares.

### **Sletning af gamle logninger**

I større systemer kan der let blive produceret flere tusinde logninger pr. dag, og efter måske et år er der mere end én million logninger i logfilen, svarende til en logfil på mere end 200 MB.

For at undgå unødvendigt store logfiler, kan systemet sættes op til automatisk at slette logninger, der er mere end et vist antal måneder gamle. Antal måneder det ønskes at gemme logninger i log-databasen, opsættes i programmet Adgangseditor i menuen [Indstillinger], [Database], [Logdatabase oprydning].

## 3.22 Poller

**Logninger 117**

PC tid	K-punkt tid	Hændelse	Info	Sted	Foretaget af
L 2018-09-01 13:00:00	=	Skift af sikkerhedsniveau	Sikkerhedsniveauudtabel, der var låst. Sikkerhedsniveau 0.1 -> 3.2	1002 - Indgang vest	
L 2018-09-01 13:00:00	=	Skift af sikkerhedsniveau	Sikkerhedsniveauudtabel, der var låst. Sikkerhedsniveau 0.1 -> 3.2	1004 - Kontorfløj nord	
M 2018-09-03 07:00:01	=	DAS frakoblet	Arbejdstid start. Sikkerhedsniveau 3.2	1001 - Hovedindgang	
M 2018-09-03 07:00:01	=	DAS frakoblet	Arbejdstid start. Sikkerhedsniveau 3.2	1002 - Indgang vest	
M 2018-09-03 07:00:01	=	DAS frakoblet	Arbejdstid start. Sikkerhedsniveau 2.2	1003 - Parkeringskælder	
M 2018-09-03 07:30:01	=	Skift af sikkerhedsniveau	Sikkerhedsniveauudtabel, der var låst. Sikkerhedsniveau 3.2 -> 1.2	1001 - Hovedindgang	
M 2018-09-03 07:30:01	=	Skift af sikkerhedsniveau	Sikkerhedsniveauudtabel, der var låst. Sikkerhedsniveau 3.2 -> 1.2	1002 - Indgang vest	
M 2018-09-03 07:45:01	=	Skift af sikkerhedsniveau	Sikkerhedsniveauudtabel, der var låst. Sikkerhedsniveau 3.2 -> 1.1	1004 - Kontorfløj nord	
M 2018-09-03 08:00:01	=	Skift af sikkerhedsniveau	Sikkerhedsniveauudtabel, der var låst. Sikkerhedsniveau 3.2 -> 2.1	1005 - Kontorfløj syd	
M 2018-09-03 08:19:09	=	Klient startet på pc	UNITEKFLB	1006 - Kantine	
M 2018-09-03 08:19:16	=	Log ind af operatør		IP 192.168.1.50'	
M 2018-09-03 08:19:47	=	Der oplåst	Nagle. Sikkerhedsniveau 2.1	WS59---FL	Administrator
M 2018-09-03 08:19:47	=	DAS frakoblet	Nagle og/eller PIN-kode. Sikkerhedsniveau 2.1	1006 - Kantine	Tom Iland
M 2018-09-03 08:19:47	=	Person ankom i område	Område 'Viborg'	1006 - Kantine	Tom Iland
M 2018-09-03 08:20:14	=	Der oplåst	Nagle eller PIN-kode. Sikkerhedsniveau 1.2	1001 - Hovedindgang	Kristiak Ylermann
M 2018-09-03 08:20:14	=	Person ankom i område	Område 'Viborg'	1001 - Hovedindgang	Kristiak Ylermann
M 2018-09-03 08:20:49	=	Der tvangsåbnet	Sikkerhedsniveau 1.2	1001 - Hovedindgang	
M 2018-09-03 08:20:49	=	Der oplåst	Udpasseringstryk. Sikkerhedsniveau 1.2	1001 - Hovedindgang	
M 2018-09-03 08:21:06	=	Der lukket	Ether alarm. Sikkerhedsniveau 1.2	1001 - Hovedindgang	
M 2018-09-03 08:21:33	=	DAS tilkoblet	Med stjernetal. Sikkerhedsniveau 2.1	1006 - Kantine	
M 2018-09-03 08:21:33	=	Der låst	DAS-silkobling. Sikkerhedsniveau 2.1	1006 - Kantine	
M 2018-09-03 08:21:33	=	*funktion	Stjernetal: 0	1006 - Kantine	Tom Iland
M 2018-09-03 08:22:05	=	Nagle åbnet	Ikke oprettet i k-punkt. Dør var låst. Sikkerhedsniveau 1.2	1001 - Hovedindgang	<Ukendt nøgle: "1a22da92">
M 2018-09-03 08:22:37	=	DAS timer programmeret	Sikkerhedsniveau 1.2	1001 - Hovedindgang	
M 2018-09-03 08:22:37	=	DAS tidsforskuet tilkobling aktiveret	Tilkoblingstidspunkt kl. 22:00. Sikkerhedsniveau 1.2	1001 - Hovedindgang	
M 2018-09-03 08:22:37	=	*funktion	Stjernetal: 0	1001 - Hovedindgang	Tom Iland
M 2018-09-03 08:22:37	=	Anti-passback overtrådt	Område 'Viborg'	1001 - Hovedindgang	Tom Iland
M 2018-09-03 08:22:37	=	Person forlod område	Område 'Viborg'	1001 - Hovedindgang	Tom Iland
M 2018-09-03 08:22:37	=	DAS timer programmeret	DAS timer programmeret (ekstern fra). Sikkerhedsniveau 1.2	1002 - Indgang vest	
M 2018-09-03 08:22:37	=	DAS tidsforskuet tilkobling aktiveret	Tilkoblingstidspunkt kl. 22:00. Sikkerhedsniveau 1.2	1002 - Indgang vest	
M 2018-09-03 08:22:37	=	DAS timer programmeret	DAS timer programmeret (ekstern fra). Sikkerhedsniveau 2.2	1003 - Parkeringskælder	
M 2018-09-03 08:22:37	=	DAS tidsforskuet tilkobling aktiveret	Tilkoblingstidspunkt kl. 22:00. Sikkerhedsniveau 2.2	1003 - Parkeringskælder	
M 2018-09-03 08:23:06	=	Forkert PIN-kode	PIN-kode. Sikkerhedsniveau 1.2	1001 - Hovedindgang	
M 2018-09-03 08:23:58	=	Objekt ændret	Operatør Lars Hallum'	WS59---FL	Administrator
M 2018-09-03 08:24:06	=	Log ind af operatør		192.168.1.50 (Webadgang)	Lars Hallum
M 2018-09-03 08:24:19	=	Der oplåst af operatør	Der '1005 - Kontorfløj syd'	192.168.1.50 (Webadgang)	Lars Hallum
M 2018-09-03 08:24:20	=	DAS frakoblet	Nagle og/eller PIN-kode ekstern fra. Sikkerhedsniveau 2.1	1005 - Kontorfløj syd	

Info logninger
  K-punkt logninger
  System logninger
  Operatør logninger
  Alarmer
 198 skærmalmer

Servertid: 08:28:13 Auto scroll

Pollereren er den teknisk del af programmet, der varetager kommunikationen med låsecomputerne i k-punkterne. Polleren henter løbende data i k-punkterne og checker ved hjælp af en række checksummer deres status. Er der uoverensstemmelse mellem pc'ens checksum og låsecomputerens checksum, opdateres låsecomputerens database helt automatisk. Logningerne fra k-punkterne gemmes i log-databasen. Logningerne kan så senere findes frem igen med programmet Logsøgning.

I programmet ses en status over, hvilke k-punkter der er online, offline og hvilke der ikke bliver pollet. Desuden kan de enkelte k-punkter checkes, så deres status kan undersøges detaljeret fx med I/O-status, checksummer osv.

Programmet skal afvikles på den pc hvortil RS485 kommunikationsnettet og/eller modemmet er forbundet.

Hvis Polleren ikke kører, når der via Adgangsedatoren laves ændringer i databasen, gemmes disse ændringer i en speciel liste. Indholdet af denne liste sendes så ud til de relevante k-punkter, når Polleren startes næste gang, så ingen data går tabt.

### Netværk

Når adgangskontrolsystemet anvendes i pc-netværk, er det muligt at anvende Adgangseditor på alle pc'er i netværket. Fra en vilkårlig pc i netværket kan der således udføres ændringer i databasen, alarmer kan modtages og der kan foretages gennemsyn af loggen. For at udførte ændringer i databasen skal blive sendt ud til k-punkterne og nye logninger fra k-punkterne skal være til rådighed i "real-time", er det nødvendigt, at Polleren kører hele tiden.

### 3.22.1 Kommunikation

K-punkterne kan være placeret lokalt eller i en række lokaliteter. Lokale k-punkter er direkte forbundet til pc'en, hvorimod forbindelsen til eksterne lokaliteter etableres over telefonnettet med modem forbindelse eller over internettet med TCP/IP forbindelse.

#### ID-nummer

Kommunikationen til alle låsecomputere i k-punkterne foregår over et fælles 2-ledet RS485 kommunikationsnet, derfor skal hver enhed på nettet have et entydigt ID-nummer, således at Polleren kan identificere hver enkelt låsecomputer.

ID-nummeret tildeles låsecomputeren med en Loader, eller det indtastes på kortlæseren i de første 25 sekunder efter at låsecomputeren er tændt (tast `*nnnn#`, hvor `nnnn` = ID-nummer).

Hvis en låsecomputer udskiftes, skal den `nye` låsecomputer blot tildeles det ID-nummer som k-punktet har, derefter vil Polleren ved næste check af k-punktet automatisk opdatere låsecomputeren med alle relevante data for det pågældende k-punkt.

#### Polling

Polling er en kommunikationsform hvor en master (Poller) styrer kommunikationen på kommunikationsnettet. Efter tur kalder Polleren ved hjælp af ID-nummeret hvert k-punkt op og `spørger`, om det har nogle logninger, som k-punktet derefter sender til Polleren.

Polling status vises altid i bunden af Adgangseditor vinduet, hvor dobbeltklik med musen vil åbne menuen hvor Polling kan startes og stoppes [Indstillinger], [PollerService], [Polling].

#### Check af k-punkter

Hver gang alle k-punkter i en lokalitet er blevet pollet, undersøges checksummerne for ét k-punkt. Derefter polles alle k-punkter igen, og det næste k-punkt i rækken checkes osv.

Et check af et k-punkt består i at k-punktet sender sin checksum for `Nøgletabel`, `Tidstabeller + Specialdagskalender`, `Sikkerhedsniveautidstabel` og `Driftsstatus` til Polleren. Er én af disse checksummer ikke i overensstemmelse med pc'ens, vil Polleren foretage en ekstra kontrolberegning af sine egne checksumme. Er der stadig uoverensstemmelse, vil Polleren opdatere låsecomputerens database. Det er denne funktion der automatisk sørger for, at opdatere en udskiftet låsecomputer med relevante data.

#### Tid og dato

I hver låsecomputer er der et software ur, som ved net drift er baseret på net frekvensen og dermed meget præcist. Ved net svigt skiftes der automatisk over til batteridrift, hvis der er monteret et backupbatteri i k-punktet. Hvis der ikke er monteret et backup-batteri, eller når dette er afladet, vil låsecomputeren miste sin tidsinformation. Når strømmen kommer igen, går uret i låsecomputeren ikke, og alle efterfølgende logninger vil have en dato og tid på `00-00-00 00:00`, indtil uret stilles igen.

En gang i minuttet sender Polleren dato og tid til alle tilsluttede låsecomputere.

Når Polleren ikke kører, vil en tilfældig låsecomputer blive tidserver og forsyne andre låsecomputere i systemet med dato og tid.

Tidsstyrede hændelser og tidsstemplingen af logninger er baseret på den dato og tid Polleren får af operativsystemet, derfor er det selvfølgelig vigtigt at uret i pc'en er indstillet til korrekt dato og klokkeslæt og går præcist.

### **Lokal lokalitet**

Polleren kommunikerer kontinuerligt med de lokale k-punkter gennem én af pc'ens netkort, USB eller RS232 porte. Ved USB/RS232 skal der anbringes en konverter indenfor maksimalafstanden for hver port type, hvor USB 2.0 maksimal længde er 5 meter, mens RS232 maksimal længde er 15 meter.

Polleren kan polle ca. 10 k-punkter i sekundet, det gør at logninger normalt ikke er mange sekunder gamle før de er registreret i pc'en. Har en Adgangseditor lavet ændringer i databasen, vil der normalt heller ikke gå mange sekunder før Polleren opdager det, og sender ændringerne ud til de relevante k-punkter.

### **Modem lokaliteter**

Polleren kan kommunikere med k-punkter i eksterne lokaliteter gennem telefonmodemmer forbundet via IP eller til én eller flere af poller-pc'ens RS232 porte. Der kan tilsluttes op til 8 modems til poller-pc'en, fordelt på 4 via IP og 4 via COM-port, således at Polleren kan kommunikere med 8 lokaliteter på samme tid. I lokaliteterne anbringes et modem med RS485 tilslutning (CV61). Alle låsecomputere i lokaliteten forbindes til dette RS485 net.

Polleren kan programmeres til at ringe lokaliteterne op på en række fastlagte tidspunkter.

Hver gang Polleren etablerer forbindelse til en lokalitet, vil alle informationer om nye nøgler, slettede nøgler, ændringer i tidstabeller mv., som er foretaget siden sidste opkald, blive sendt ud til de respektive låsecomputere. Endvidere stilles uret i låsecomputerne, og alle nye logninger hentes hjem. Før forbindelsen til lokaliteten afbrydes, checkes om der er overensstemmelse mellem alle checksummer i k-punkterne og pc'ens database.

Hvis en låsecomputer i en lokalitet udskiftes, vil den ved næste opkald automatisk blive opdateret med de relevante data.

Hvis én eller flere lokaliteter skal opdateres eller logninger hentes "her og nu", kan dette gøres i [K-punkt oversigt] ved at aktivere tasten [Opdater], hvorefter Polleren vil ringe lokaliteten op og skabe forbindelse til k-punkterne.

### **IP-lokaliteter**

Polleren kan via TCP/IP (internet-protokollen) etablere krypteret forbindelse over pc-netværk og internet til en COM Server gateway (CV72 eller LS10-IP) på lokaliteten. De låsecomputere der er i lokaliteten kommunikerer via kommunikationsnettet i lokaliteten - Ethernet eller tilslutning direkte til COM Serverens RS485 kommunikationsport.

Der kan oprettes op til 200 kontinuerligt pollede lokaliteter. En kontinuerlig pollet lokalitet har reelt sin egen poller, og polles samtidig og uafhængig af andre lokaliteter. Ved kontinuerlig polling vil k-punkterne i lokaliteten blive pollet efter samme pollingsprincip, som de k-punkter der er tilsluttet den lokale port på poller pc'en.

Skal der oprettes flere end 200 IP-lokaliteter, oprettes disse blot som tidsbestemte lokaliteter, hvor den periodiske opkaldstid kan sættes så lavt som 1 minut mellem hver polling. Når der anvendes tidsbestemt polling af lokaliteten, checkes låsecomputerne i lokaliteten på samme måde som ved en modempkobling.

### 3.22.2 Hovedvinduet

I hovedvinduet vises en række forskellige statusinformationer, som er med til at fortælle, hvordan systemet kører. Endvidere vises logninger og antallet af alarmer efterhånden som de indløber.

#### Pollingsstatus

I den øverste del af hovedvinduet vises en række statusinformationer om, hvordan kommunikationen med k-punkterne og lokaliteterne forløber. Med comboboksen [Vis pollingsstatus for:] er det muligt at vælge den lokalitet, som informationerne om k-punkter ønskes udlæst fra.

#### Logninger

Viser alle logninger i kronologisk rækkefølge efterhånden som de indløber fra de forskellige k-punkter. Visningen er beregnet til at danne sig et hurtigt overblik over hvad der foregår i systemet lige nu. Alle modtagne logninger overføres automatisk med det samme til log-databasen, hvor en nærmere undersøgelse af de modtagne logninger kan foretages med [Logsøgning].

Vinduet kan maksimalt indeholde de sidst 1.000 logninger og nulstilles ved genstart af pc'en. Visningen i vinduet kan filtreres således at kun ønskede logningstyper er tilgængelige.

## 3.23 Alarmoversigt

The screenshot shows the 'Alarmoversigt' window with 70 skærmalarmer. It is divided into two main sections: 'Alarmtyper' and 'Alarmkilder med stackede alarmer'.

**Alarmtyper**

PC tid	Hændelse	Kilder	Alarmer	Afstil
Ti 2017-03-28 16:10:17	Fem forkerte PIN-koder	1	1	<input type="checkbox"/>
Ti 2017-03-28 16:16:54	Nøgle afvist pga. tidstabel. Dør var låst	1	2	<input type="checkbox"/>
O 2017-03-29 09:23:00	Overfaldskode er anvendt	1	2	<input type="checkbox"/>
To 2017-03-30 10:37:18	Lokalitet gået off-line (5 minutter)	1	4	<input type="checkbox"/>
M 2017-04-10 13:51:21	Skift til DC-drift (batteri)	1	2	<input type="checkbox"/>
Ti 2017-04-11 08:07:54	Dør er tvangsåbnet	5	14	<input type="checkbox"/>
<b>Ti 2017-04-11 08:15:50</b>	<b>Dør ikke lukket</b>	<b>7</b>	<b>16</b>	<input checked="" type="checkbox"/>
Ti 2017-04-11 08:16:18	Forkert PIN-kode	1	11	<input type="checkbox"/>
Ti 2017-04-11 08:39:21	K-punkt gået off-line	4	7	<input type="checkbox"/>
Ti 2017-04-11 08:39:41	Nøgle afvist, ikke oprettet. Dør var låst	1	11	<input type="checkbox"/>

**Alarmkilder med stackede alarmer**

Hændelse	Sted	Alarmer	Afstil
<input checked="" type="checkbox"/> Dør ikke lukket	1007 - Kantinekontor	3	<input type="checkbox"/>
<input checked="" type="checkbox"/> Dør ikke lukket	1002 - Indgang vest	4	<input type="checkbox"/>
<input checked="" type="checkbox"/> Dør ikke lukket	1004 - Kontorfløj nord	1	<input type="checkbox"/>
<input checked="" type="checkbox"/> Dør ikke lukket	1003 - Parkeringskælder	2	<input type="checkbox"/>
<input type="checkbox"/> Dør ikke lukket	1001 - Hovedindgang	2	<input checked="" type="checkbox"/>

Below this table is a detailed view for the selected 'Dør ikke lukket' alarm:

PC tid	K-punkt tid	Hændelse	Niveau
Ti 2017-04-11 07:44:20	=	Dør ikke lukket	3.2
Ti 2017-04-11 07:44:28	=	Dør lukket igen efter alarm	3.2
Ti 2017-04-11 08:09:19	=	Dør ikke lukket	3.2
Ti 2017-04-11 08:09:29	=	Dør lukket igen efter alarm	3.2

At the bottom, there are filters for: Alarmer (red), Auto-clearedde alarmer (orange), K-punkt logninger (green), and System logninger (blue).

Det todelte alarmvindue giver et overskueligt og detaljeret overblik over skærmalarmer, som endnu ikke er afstillet.

### Skærmalarm

En række forskellige hændelser kan individuelt for hvert k-punkt opsættes til at give en skærmalarm. Derudover vil en række andre hændelser altid give en skærmalarm.

Skærmalarmer vises så snart hændelser hentes fra k-punkter og er automatisk i log-databasen med det samme. Der skal kvitteres for en alarm, det vil sige at en alarm skal afstilles.

### Alarmtyper

I det øverste alarmvindue vises alle alarmer grupperet i alarmtyper. Dette vindue giver et overordnet overblik over alarmtyper med aktive og auto-clearedde alarmer.

Hver alarmtypevisning indeholder tidspunkt for seneste ændring, antal alarmkilder og det samlede antal alarmer.

### Alarmkilder

I det nederste alarmvindue vises alle alarmer af samme type fordelt på alarmkilder. Hver alarmkildes alarm-stack kan åbnes, gennemses og afstilles. Alarmstacken viser hændelser for alarmer og hændelser for auto-clearing af alarmer.

## Afstille alarmer

Skærmalarmer afstilles ved at sætte flueben ved de ønskede alarmtyper eller alarmkilder og vælge ikonet [Afstil valgte skærmalarmer]. Operatører kan således hurtigt fokusere på relevante alarmer og fjerne behandlede eller uinteressante alarmer.

Når en operatør afstiller alarmer overføres informationen til log-databasen.

## 3.24 K-punkt oversigt

Dette vindue viser en række detaljerede informationer om de enkelte lokaliteter og k-punkter i systemet. I et oversigtsvindue vises k-punkternes placering i lokaliteterne.

Informationerne er hentet direkte fra k-punkter og lokaliteter og ikke fra pc'ens database. Dette medfører, at informationerne selvfølgelig ikke er til rådighed, hvis det valgte k-punkt eller valgte lokalitet ikke polles eller var offline da Polleren blev startet.

### K-punkter

I denne gruppe er det muligt at vælge hvilke k-punkter der skal vises i vinduet. Der kan vælges at vise de k-punkter der er [Online], [Offline], [Ikke pollede] og [Ukendte].

Ud for hvert k-punkt i oversigtsvinduet er der en farvet statusindikering der fortæller om k-punktet er online, offline eller ikke polles.

### 3.24.1 Lokalteter

Vælg den lokalitet der skal vises informationer om i vinduet. De tekniske informationer er underordnet i en normal driftssituation, og yderst relevante i en eventuel fejlfindingsituation.

Pollingsstatus	
Sidst checket:	øViborg - Hovedindgang fælles
Checktid:	1.3 sek.
Sidst pollet:	øViborg - Hovedindgang fælles
Pollingstid:	1.3 sek.
Handling:	<input checked="" type="checkbox"/> Pause

On-line status	Gateway CV72
Polles: <input checked="" type="checkbox"/>	Sidst opdateret: 2022-12-09 14:11:21 <a href="#">Webside</a>
Gæet on/off -line: 2022-12-09 12:53:22 (1)	Pingtid (RTT) [ms]: < 1 Min: < 1 Max: 7 <a href="#">Nulstil</a>
I alt: 1	Type: LS10 med CV72 LS10 ID: 1010
On-line: <input checked="" type="checkbox"/> 1 Ikke pollede: <input type="checkbox"/> 0	Software: PIC135-3.0 Rev:221206 <a href="#">OK</a> <a href="#">Opdater</a>
Off-line: <input type="checkbox"/> 0 Ukendte: <input type="checkbox"/> 0	Beskrivelse: FL Skrivebord LS10IP -- ID1010
Lokalitetstype: IP-netværk via gateway	Hostnavn: LS10IP-ID1010
Hostnavn: CV72LS10-ID1010	Angivet domæne: Unitek.local
IP-adresse: 192.168.1.192 Port: 7211	Registreringsadresse: 192.168.1.1
Adgangskode: Ja <input type="checkbox"/> Korrekt i enhed <input checked="" type="checkbox"/> <a href="#">Godkend</a>	Registreret DNS-navn: LS10IP-ID1010.Unitek.local (via DNS)
Kryptering: Korrekt i enhed	<input checked="" type="radio"/> Fast <input type="radio"/> DHCP
Opkalds info	IP-adresse: 192.168.1.192 Port: 7211
Polling: Kontinuerlig	Netmaske: 255.255.255.0
Opkaldsstatus: Forbindelse åben	Gateway: 192.168.1.99
Opkald ok: 4	<input checked="" type="radio"/> Fast <input type="radio"/> DHCP
Opkald mistykket: 0 <a href="#">Nulstil</a>	DNS-serveradresse: 192.168.1.1; 0.0.0.0
Gæet off-line: 1	Tid i CV72: 2022-12-09 14:11:21
	Oppetid: 0:07:48
	Pakker: Bytes:
	Ethernet sendt: 2.201 290.194
	Ethernet modtaget: 22.746 1.256.821
	RS485 sendt: 678 6.206
	RS485 modtaget: 0 0

#### Pollingsstatus

Gruppen viser status for pc-programmets polling i lokaliteten. [Checktid] viser den tid det sidst har taget at polle alle lokalitetens k-punkter for at hente nye logninger og sende nye indstillinger. [Pollingstid] viser den tid det sidst har taget at polle alle lokalitetens k-punkter for at hente status.

#### Lokalitets info

Her kan operatøren verificere om samme adgangskoden er korrekt indtastet i pc-programmet og i enheden. Er der indstillet sikkerhedskrav om at nye netværksenheder skal godkendes, før krypteringsnøgler sendes til enheden, udføres dette med knappen [Godkend]. Sikkerhedskrav til enhedsgodkendelse indstilles i vinduet [Indstillinger] menupunkt [Poller-Service], [Polling].



### 3.24.2 K-punkter

Vælg det k-punkt der skal vises informationer om i vinduet. Ethernet baserede k-punkter har et ekstra faneblad [IP-net], men netværksrelaterede informationer.

#### Kontaktinformation

Gruppen viser status for det valgte k-punkt. Hvis et k-punkt midlertidig skal sættes ud af drift, er det muligt at stoppe polling af k-punktet.

En lille farvet indikator viser aktuel status for k-punktet.

I feltet [Gået on/off -line] vises tidspunktet for hvornår k-punktet er gået "online" eller "offline". Vises tidspunktet med sort, er der ikke sket nogen tilstandsændring siden opstart af Polleren. Vises tidspunktet derimod med rød eller grøn, er der sket mindst én tilstandsændring fra "online" til "offline" eller omvendt.

Feltet [Sidst pollet] viser hvornår Polleren sidst har checket k-punktet. I gruppen "Checksummer" vises status for denne test.

#### Drift-parametre

Denne gruppe viser en række detaljerede informationer om det enkelte k-punkt. I forbindelse med fejlfinding af fx "hvorfor en dør ikke oplåste", kan informationen fra [Tid i k-punkt] og [Aktuel sikkerhedsniveau] være meget nyttige.

Versionen af den software der anvendes i låsecomputeren kan aflæses. Herved er man fri for at skulle ud til låsecomputeren for at se hvilken version af software låsecomputeren anvender.

#### DAS-status

Denne gruppe viser status for DAS i det enkelte k-punkt. Pt. kan status for DAS være:

- "DAS er frakoblet"
- "Tidsforskudt tilkobling kl. xx:xx"
- "Købetid udløber om xx:xx"
- "Prealarm udløber om xx:xx"
- "Forsinket tilkobling om xx:xx"
- "DAS er tilkoblet"
- "DAS er ikke aktiv"
- "Ny funktion i LS10 efter 2005-09-28" (Opdatér LS10 software)
- "Ingen data"

#### Checksummer

Denne gruppe viser, om der er overensstemmelse mellem låsecomputerens og pc'ens database.

Er én af låsecomputerens checksummer ikke i overensstemmelse med pc'ens, vil Polleren foretage en ekstra kontrolberegning af pc-databasens checksum. Er der stadig uoverensstemmelse, vil Polleren opdatere låsecomputerens database.

Ved at aktivere knappen [Opdater], vil det valgte k-punkt blive rykket frem i rækken og checkes som det næste k-punkt. Denne knap har kun betydning i meget store systemer, hvor [Checktid] kan blive større end ens tålmodighed.

## **Udgange**

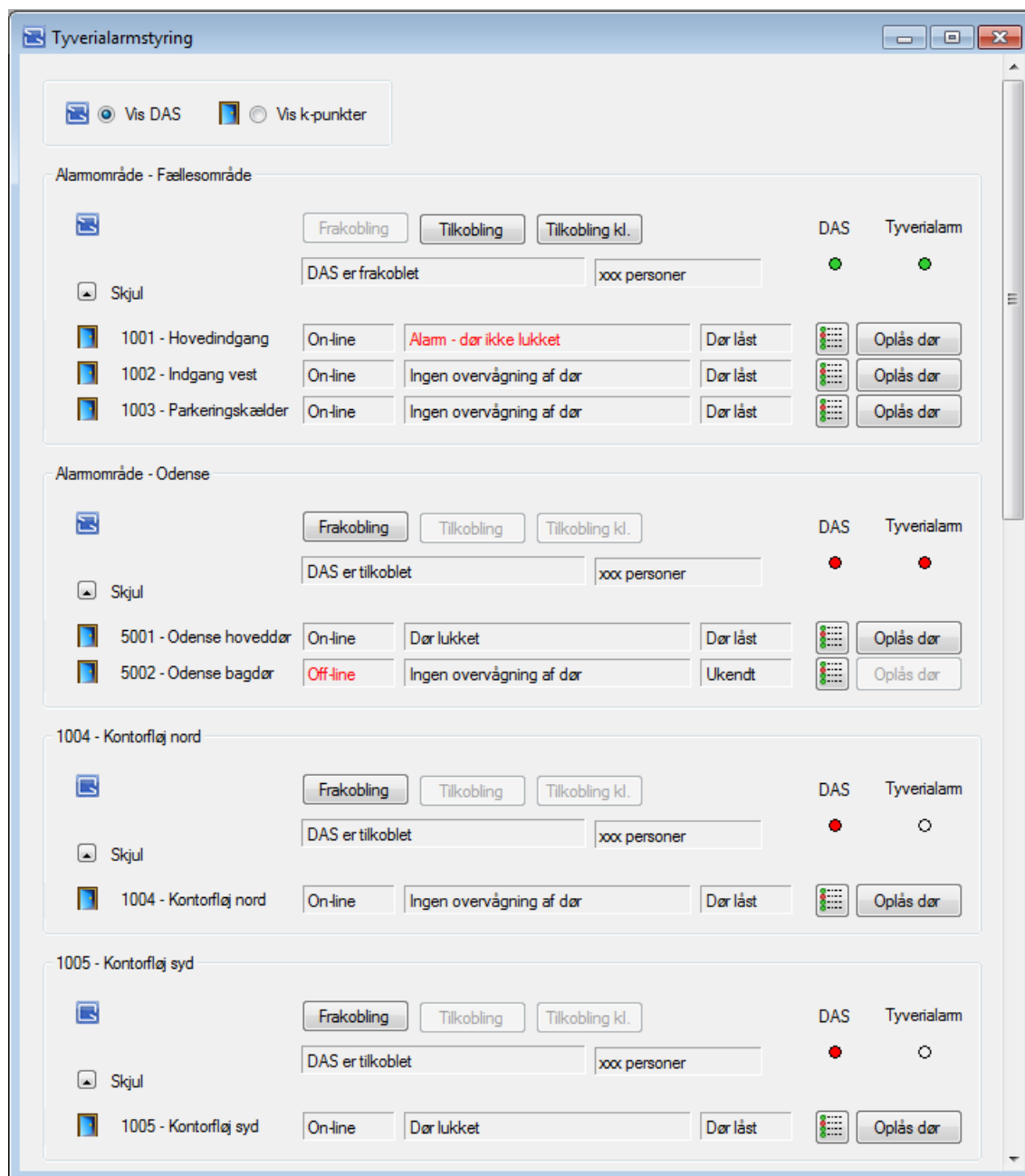
Her kan aflæses aktuel status på de 8 udgange, der er i låsecomputeren. I Adgangseditoren kan udgangene navngives, afhængig af hvad de bruges til. En lille indikator fortæller, om udgangen er aktiveret eller ikke. Ved at klikke på indikatoren med musen, kan status på udgangen skiftes. Opmærksomheden henledes på, at andre funktioner i systemet kan tvangsstyre udgangen til en anden stilling end den, man umiddelbart ønsker.

## **Indgange**

Her kan aflæses aktuel status på de 8 indgange, der er i låsecomputeren. I Adgangseditoren kan indgangene navngives, afhængig af hvad de bruges til. Indgangen kan have to forskellige tekster, afhængig af om indgangen er aktiveret eller ikke.

Hver indgang har en tæller tilsluttet, som tæller antal aktiveringer af indgangen. Denne tæller kan tælle til 999.999 før den starter ved 0 igen. Tællerne kan kun nulstilles ved en master-reset af låsecomputeren.

## 3.25 Tyverialarmstyring



Dette vindue giver mulighed for at overvåge og fjernkontrollere systemets tyverialarmer og døre fra pc'en. Aktuel status for døre, DAS (Decentrale Alarm Styring) og tyverialarmer vises og opdateres løbende. Der kan vælges mellem at få vist status for tyverialarmen (DAS), dørene eller begge dele. Vælges det at få vist status for tyverialarmen og dørene samtidig, vil de døre, der giver adgang til et givet alarm-område, blive vist lige efter statusvisningen for det pågældende alarmområde.

### Tyverialarm (DAS)

Dette vindue viser status for adgangskontrollens DAS og tilbagemelding fra tyverialarmen. Under normale forhold vil tyverialarmens status svare til DAS'ens status. Er der ikke tilbagemelding fra tyverialarmen, vises tyverialarmens status ikke.

Det er muligt for operatøren at til- og frakoble tyverialarmen i de enkelte alarmområder. Det er endvidere muligt at lave tidsforskudt tilkobling af tyverialarmen, altså tilkobling på et af operatøren indtastet klokkeslæt.

Er DAS'en programmeret til tidsforskudt tilkobling, kan det angivne tidspunkt ændres ved at indtaste en ny tid. En programmeret tidsforskudt tilkobling kan af sikkerhedsgrunde kun afmeldes ved at lave en tilkobling efterfulgt af en frakobling.

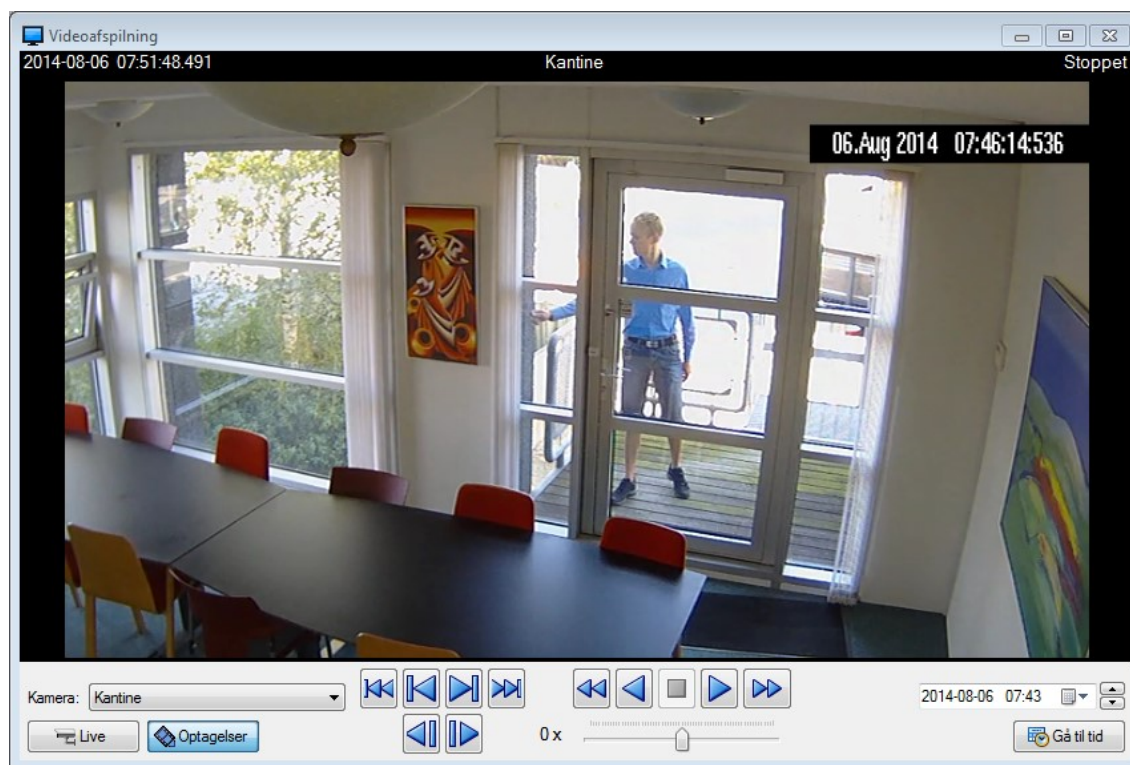
Er DAS'en tilknyttet et område i Områdevisningen, vises antal personer, der er i området. Det er muligt at få tyverialarmen til at tilkoble, når sidste person forlader området.

### K-punkter

Denne ramme viser status for døren. Er der ikke monteret karmkontakt på døren, kan døren følgelig ikke overvåges. Polles k-punktet ikke, vises status for den pågældende dør ikke.

Operatøren har mulighed for at oplåse døre. Er tyverialarmen tilkoblet i det område, døren giver adgang til, vil tyverialarmen automatisk blive frakoblet i det pågældende område.

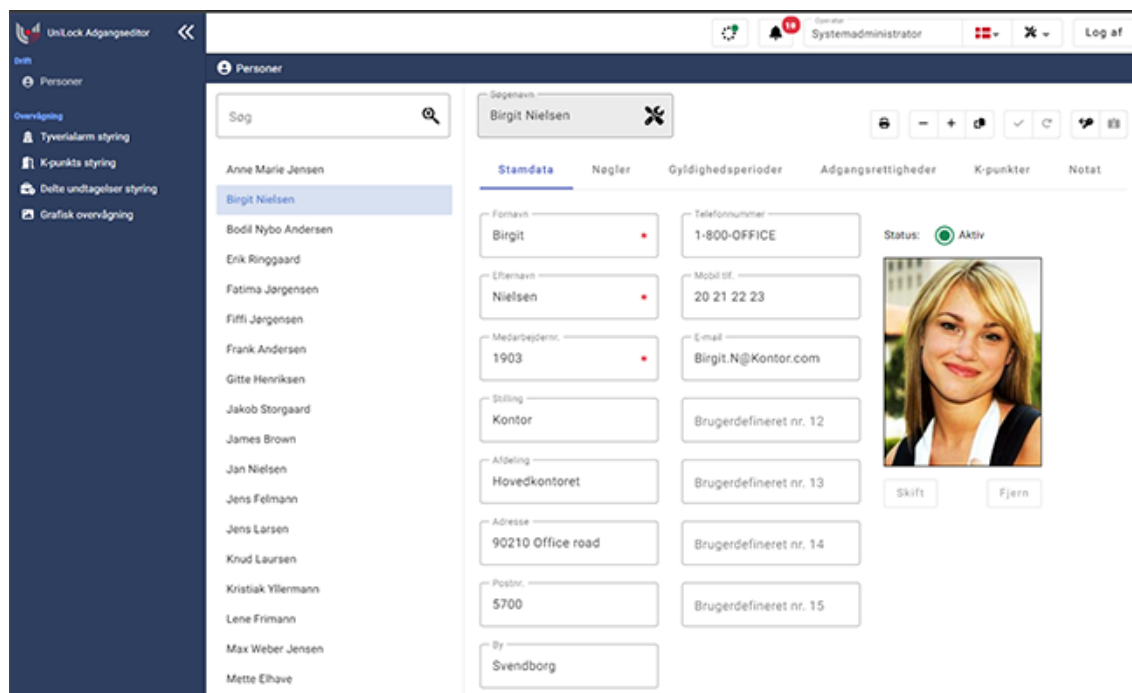
## 3.26 Videoafspilning



Dette vindue giver mulighed for at afspille live video og optaget video hentet fra eksterne IP videoservere (video management systemer og kameraer).

Operatøren kan vælge mellem de videoservere, som er oprettet i vinduet [Videoserver og kamera], og derefter se live video eller video-verificere tidligere hændelser med knappen [Gå til tid]. Efter tryk på [Gå til tid] sender UniLock en besked til videoserveren om at returnere video stream fra det pågældende tidspunkt. Den modtagne stream fra videoserveren afspilles derefter i vinduet.

## 3.27 Web-Adgangseditor



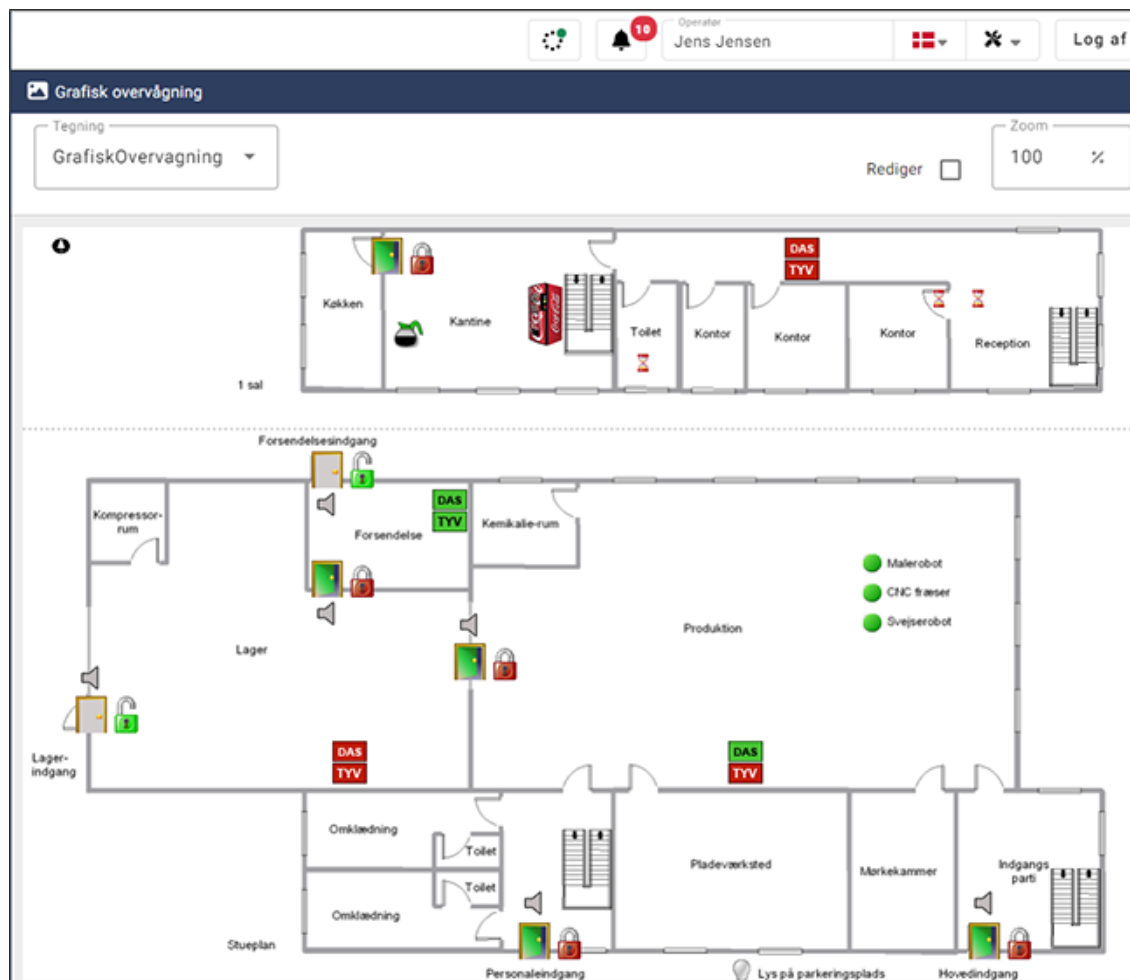
Web-Adgangseditor er en browserbaseret brugerflade til at varetage den administrative del af adgangskontrollen. Web-Adgangseditor tilgås via webbrowser og kan installeres som webApp på pc, tablet og smartphone.

Al kommunikation foregår ved hjælp af blandt andet XML og JSON, som er åbne standard protokoller. Hjemmesiden er bygget på HTML 5, som alle dagens webbrowsere understøtter.

Login er beskyttet med Digest Access Authentication for at modvirke afluring og replay angreb. Digest Access Authentication er en udbredt sikringsmetode, som blandt andet anvender MD5 kryptografisk hash.

Web-Adgangseditor og tilhørende Webserver er indbygget i UniLock PollerService. Der kræves således ikke andre programmer end UniLock for at anvende Web-Adgangseditor.

## Grafisk overvågning



På basis af en bygningstegning giver Grafisk overvågning et hurtigt samlet overblik over hele installationens aktuelle driftstilstand, så overvågning bliver en overskuelig og lettilgængelig opgave.

Grafisk overvågning består af et baggrundsbillede, hvorpå aktuel status for døre, DAS, tyverialarmer, indgange og udgange vises ved hjælp af dynamiske ikoner, der frit kan placeres på baggrundsbilledet. Døre, DAS og tyverialarmer kan ligeledes styres ved klik på ikonerne. Skift mellem forskellige baggrundsbilleder kan, udover den indbyggede drop-down, foretages ved at indsætte knapper.

### Delte undtagelser

For at give en simpel måde at ændre systemets daglige drift, kan delte undtagelser aktiveres/deaktiveres med et enkelt knaptryk.

For nærmere beskrivelse se afsnit 3.9 delte undtagelser.

### Integration via WebAPI

Eksterne systemer kan kommunikere med det indbyggede WebAPI, hvorved en række data og funktioner stilles til rådighed via en tovejs sikret webforbindelse.

Eksterne systemer, som SCADA, PSIM, overvågningssystemer, cloudsystemer, smartphone Apps mv., kan udføre driftsovervågning, kontrol og administration af UniLock adgangskontrol.

For nærmere oplysninger se særskilt manual (WebAPI).

## 3.28 Områdevisning

The screenshot displays three overlapping windows from a software application:

- Områdeoversigt (Area Overview):** A table listing areas with columns for name, number of persons, time point, event, person, and K-point.
- Personoversigt (Person Overview):** A window showing a list of persons on the left and a table of their current areas and latest events on the right.
- Viborg (Area Detail):** A window showing a list of persons on the left and a table of their passback status, expiration time, last seen, and K-point on the right.

Områdenavn	Antal Personer	Tidspunkt	Hændelse	Person	K-punkt
<Personoversigt>	28	2018-05-03 10:11	Ankom	Jan Nielsen	Administrator
<Ude>	1	2018-05-03 09:48	Forlod	Birgit Nielsen	1001 - Hovedindgang
Herning	1	2018-05-03 09:06	Ankom	Suzanne Bjerrehus	Administrator
Odense	5	2018-05-03 09:06	Ankom	Tom Iland	Administrator
Vejle	0	2018-05-03 09:18	Opholdstid udløbet	Lene Frimann	Områdevisning
Viborg	7	2018-05-03 10:11	Ankom	Jan Nielsen	Administrator
Viborg - Lager	1	2018-03-13 12:57	Ankom	Jan Nielsen	Administrator

Person	Aktuelle områder	Seneste hændelse
Jan Nielsen	Viborg, Viborg - Lager	2018-05-03 10:11 - Administrator
Birgit Nielsen	Viborg	2018-05-03 09:48 - 1001 - Hovedindgang
Max Weber Jensen	Viborg	2018-05-03 09:27 - 1002 - Indgang vest
Frank Andersen	Viborg	2018-05-03 09:27 - 1002 - Indgang vest

Person	Passback	Udløbstid	Sidst set	K-punkt
Jan Nielsen		2018-05-03 18:00	2018-05-03 10:11	Administrator
Birgit Nielsen		2018-05-03 18:00	2018-05-03 09:48	1001 - Hovedindgang
Max Weber Jensen		2018-05-03 18:00	2018-05-03 09:27	1002 - Indgang vest
Frank Andersen		2018-05-03 18:00	2018-05-03 09:27	1002 - Indgang vest
Jens Larsen		2018-05-03 18:00	2018-05-03 09:26	Administrator
Vivi Nielsen	Anti-passback overtrådt	2018-05-03 18:00	2018-05-03 09:09	1001 - Hovedindgang
Bodil Nybo Andersen		2018-05-03 18:00	2018-05-03 09:05	Administrator

Områdeoversigten giver overblik over den seneste hændelse i hvert område. Fra områdeoversigten kan alle områder og personoversigten åbnes i separate vinduer.

Personer kan være i flere områder på samme tid, således at fx lagerforvalteren kan se alle personer på lageret ved kun at se området Lager, selvom der er flere områder i området Lager, som fx kontorer, omklædningsrum, forsendelse mv.

Operatøren har mulighed for at flytte personer ind og ud af områderne fra personoversigten og fra de enkelte områder kan personer flyttes ud.

### Personoversigt

Personoversigten viser alle personers opholdssteder og opdateres automatisk med personers færden.

### Område

Hvert område indeholder en liste over personer i området inklusiv hver persons seneste hændelse i området med mulighed for videoverificering, visning af udløbstid og overtrædelse af anti-passback. Hvert område kan åbnes i sit eget vindue, således at de forskellige operatører kan vælge at se netop de områder, der er relevante for den pågældende operatør.



I områdevinduet kan vises personbilleder af de sidste 5 personer, der er gået ind i/ud af området. Dette kan fx være en stor hjælp for portvagten, som hurtigt kan sammenligne den ankomne person med personbilledet.

## **3.29 Øvrige indstillinger**

### **Opstartssprog**

For hver arbejdsstation kan det indstilles hvilket sprog programmet skal anvende ved opstart, hvilket indstilles i arbejdsstationen [Indstillinger], [Programindstillinger], [Sprog].

## 4. Programmoduler

### 4.1 Indledning

Grundlicensen indeholder alle de faciliteter, der kan forventes af et normalt adgangs-kontrolsystem, og der skal kun erhverves licens til det antal k-punkter, der er i installationen. Ved tilkøb er det muligt at aktivere en række ekstra programmoduler, som udvider programmets funktionalitet, ud over det der er i selve "grundpakken".

Dette afsnit indeholder en kort funktionsbeskrivelse af de programmoduler, der kan erhverves som en overbygning på grundlicensen.

#### Test af moduler

Ønskes det at teste et programmodul der ikke er erhvervet licens til, kan licensen deaktiveres ved at skifte til demo-mode. Herved åbnes der for alle programmoduler, og det er muligt at tilføje yderligere k-punkter mv. Det er tilladt at køre uden aktiv licens i den periode hvor der ventes på ny licensfil. Når der modtages en ny licensfil skiftes igen væk fra demo-mode, og licensforholdene er igen bragt i orden.

#### Modulbestilling

Grundlicensen og ekstra programmoduler bestilles gennem leverandøren. Bestillingen kan eventuelt foretages på formularen "Licensbestilling" og efterfølgende sendes til leverandøren/licensudstederen. Herefter hentes fra internettet en ny licensfil (CFG-fil) med de opdaterede rettigheder. For yderligere oplysninger se afsnittet "Licens".

#### Licensenheder

Prisen for programmet til en given installation udregnes som det samlede antal licensenheder, der er i installationen ganget med prisen for én licensenhed.

Som minimum skal erhverves en grundlicens, hvor der afregnes for det antal k-punkter der er i installationen. Prisen for hvert k-punkt udgør én licensenhed.

Prisen for ekstra programmoduler opgives også i et antal licensenheder. Kan et modul erhverves i flere eksemplarer, er licensenheder for modulet opgivet som  $n \times L$  (hvor  $n$  = antal moduler og  $L$  = licensenheder).

Prisen for en årlig opdateringsaftale opgives også i et antal licensenheder. Beregningen foretages ved at tage summen af licensenheder i installationen og gange med 0,10.

### 4.2 Modul oversigt

Følgende programmoduler er på nuværende tidspunkt tilgængelige:

Varenummer	Beskrivelse	Licensenheder
PCS125-K	Grundlicens, antal k-punkter	$n \times 1$
PCS125-M0100	Ekstra arbejdsstationer	$n \times 5$
PCS125-M0101	Personbillede	2
PCS125-M0106	Fiktive specialdage og undtagelser	2

PCS125-M0110	Flere specialdagskalendere	4
PCS125-M0107	Gyldighedsperioder for personer	2
PCS125-M0103	DAS (Decentral Alarm Styring)	2
PCS125-M0102	Operatører	4
PCS125-M0108	ID-kort design og produktion	5
PCS125-M0111	Videoovervågning	8
PCS125-M0201	Ekstra lokaliteter	5
PCS137	Områdevisning	8
PCS125-M0252	Eksport af data	8
PCS136	Import af data	6
PCS125-M0109	WebAPI	14
PCS125-opdat	Opdateringsaftale pr år	licenssum x 0,10

## 4.3 Modul beskrivelser

### 4.3.1 Grundlicens, antal k-punkter

**Grundprogram som indeholder de grundlæggende adgangskontrolfunktioner. Licens afregnes pr. k-punkt. (k-punkter udover 30 u/b).**

Med grundlicensen følger alle de faciliteter, der kan forventes af et normalt adgangskontrolsystem. Stilles der yderligere krav, må der tilkøbes yderligere programmoduler.

Afregning for grundlicensen sker efter det antal k-punkter, der er i installationen. Ved en eventuel senere udvidelse af installationen afregnes kun for det antal k-punkter, installationen udvides med. Er installationen over 30 k-punkter, afregnes kun for de første 30 k-punkter.

I grundlicensen er der licens til at anvende systemet på en enkelt arbejdsstation, som skal være den pc hvor et eventuelt lokalt RS485 kommunikationsnet er tilsluttet.

### 4.3.2 Ekstra arbejdsstationer

**Programmodul der giver mulighed for at anvende systemet på flere arbejdsstationer. Licens afregnes pr. ekstra samtidig arbejdsstation.**

I grundlicensen er der licens til at anvende systemet på en enkelt arbejdsstation, og alle programmer skal afvikles på samme arbejdsstation.

Med dette modul er det muligt i et pc-netværk at anvende UniLock programmerne samtidigt på en række forskellige arbejdsstationer. Der skal erhverves licens til det antal arbejdsstationer der ønskes anvendt på samme tid, ud over den pc hvorpå Polleren afvikles.

Er der flere arbejdsstationer og operatører anbefales det af sikkerhedsgrunde at anskaffe operatørmodulet.

### 4.3.3 Ekstra afdelinger

**Programmodul der giver systemadministratoren mulighed for at opdele og uddelegere administrationen af sin organisation til afdelingsadministratorer med hver deres afdeling.**

Afdelingsadministratorer kan oprette et vilkårligt antal operatører i deres respektive afdelinger, hver med helt individuelle rettigheder til afdelingens objekttyper.

Operatører kan være medlem af flere operatørgrupper, og den enkelte operatør kan frit vælge, hvilken operatørgruppe han ønsker at logge ind i.

Et objekt tilknyttes den afdeling, hvori det er oprettet, og denne afdeling bliver nu "ejer" af objektet. Andre afdelinger kan ikke se eller anvende objektet. Afdelingsadministratoren kan dele udvalgte objekter med andre afdelinger.

Modulet kræver at der er erhvervet licens til følgende programmoduler:

- Operatører
- Flere specialdagskalendere
- Flere lokaliteter
- Ekstra arbejdsstationer med et passende antal

### **4.3.4 Personbillede**

**Programmodul der giver mulighed for at vise et billede under hver persons stamdata.**

I personers stamdata er det, ud over de almindelige stamdata for personen, muligt at vise et billede af personen, således at identifikation af personer lettes.

Billedet kan være i de mest anvendte grafikformater, og kan valgfrit gemmes i en vilkårlig billedmappe. Billedet kan eventuelt være fælles med og automatisk hentes i et medarbejderarkiv, ID-kort fabrikationsudstyr mv.

### **4.3.5 Fiktive specialdage og undtagelser**

**Programmodul der tilføjer 6 fiktive specialdage til specialdagskalendere og 8 undtagelsesperioder til hver tidstabel og sikkerhedsniveautidstabel.**

#### **Fiktive specialdage**

Specialdagskalendere bruges til at få en dag til at opføre sig som en anden dag. Udover de 7 almindelige ugedage som systemet opererer med i grundlicensen, kan der med dette udvidelsesmodul opereres med 6 fiktive specialdage. Hver dag indenfor det næste år kan frit tilknyttes én af disse 6 fiktive specialdage.

Hvis der kun skal benyttes helligdage i specialdagskalendere, er dette modul ikke nødvendigt, men skal der opereres med fiktive dage som fx "Lang lørdag", "1/2 fridage", "Festdag", "Åbent hus", "1. maj" mv. skal dette modul anvendes.

Specialdagskalender kan tilvælges for den del af systemet, som skal gøre noget specielt på specialdage. Hvis en dag er en specialdag, kan det således gælde for hele systemet eller kun for udvalgte k-punkter.

#### **Undtagelser**

Normalt gentager en tidstabel og sikkerhedsniveautidstabel sig selv uge efter uge, men i visse situationer kan det være ønskeligt at bryde denne monotoni. En undtagelse består af en

tidsperiode, hvor der anvendes en anden valgbar funktion end den, der er angivet i tidstabelen.

Undtagelser er et kraftigt supplement til specialdagskalenderen. Modsat specialdage, der varer hele døgnet, varer undtagelser i en valgbar tidsperiode.

### 4.3.6 Flere specialdagskalendere

**Programmodul der giver mulighed for at oprette et ubegrænset antal Specialdagskalendere, således at hver Tidstabel og Sikkerhedsniveautidstabel kan følge en valgfri specialdagskalender.**

I grundlicensen er der kun én Specialdagskalender, og den er global for hele systemet. Hvis en dag er en specialdag, gælder det altså enten for hele systemet eller kun for udvalgte k-punkter. Dette softwaremodul giver mulighed for, at forskellige områder og afdelinger følger sin egen specialdagskalender med individuelle helligdage og specialdage.

For at anvende flere specialdagskalendere skal softwaren i låsecomputeren have revisionsdato 2003-08-13 eller senere.

### 4.3.7 Gyldighedsperioder for personer

**Programmodul der giver mulighed for, at hver person kan anvende gyldighedsperioder hver med en gyldighedsdato og en udløbsdato.**

Modulet kan bruges, når det fx ønskes at oprette en nøgle nu, men nøglen først skal være gyldig på en senere dato, eller når det ønskes, at systemet automatisk skal fjerne en persons adgangsrettigheder ved dennes afrejse om fx et år. Da der kan oprettes flere gyldighedsperioder, så det også er muligt at bruge denne funktion til at gøre nøgler ugyldige i ferieperioder, personlige fridage, jul, påske mv. Da der kan oprettes gyldighedsperioder på medlemskab af persongrupper, så er der muligt at gøre nøgler gyldige/ugyldige i dele af installationens døre.

Gyldighedsdatoer og udløbsdatoer ligger ikke i k-punktet men kun i pc'ens database, derfor oprettes og fjernes nøgler kun, når Polleren har forbindelse til k-punktet.

### 4.3.8 DAS (Decentral Alarm Styring)

**Programmodul der giver den enkelte låsecomputer mulighed for at styre tyverialarmen i det område hvortil låsecomputeren giver adgang.**

DAS'ens formål er, helt decentralt i k-punkterne, at styre til- og frakobling af tyverialarmen.

#### Manuel til- og frakobling

Alle nøgler der har adgang i k-punktet kan til- og frakoble tyverialarmen. Når en gyldig nøgle anvendes i et k-punkt, frakobles tyverialarmen straks. For at tilkoble tyverialarmen trykkes på <\* og et tal> hvorefter en gyldig nøgle anvendes. Bruges en af Unitek's berøringsfri læsere, vil alarmen blive tilkoblet når nøglen holdes foran læseren i 5 sekunder.

Endvidere kan DAS'en på læserens tastatur programmeres til tidsforskudt tilkobling, således at alarmen tilkobler på et senere tidspunkt.

#### Automatisk til- og frakobling

DAS'en kan programmeres til automatisk at frakoble alarmer ved arbejdstids start. Når arbejdstiden slutter, vil DAS'en automatisk tilkoble alarmer efter en prealarm. Findes der stadig personer i bygningen når prealarmer lyder, indlæser de blot deres kort i læseren, og alarmtilkoblingstidspunktet udsættes i en "købetid" som frit kan indstilles.

### **Købetid**

Købetid anvendes altid når tyverialarmer frakobles uden for arbejdstiden. Hver gang der anvendes en gyldig nøgle, udskydes den automatiske tilkobling i denne tid. Hvis købetiden fx er 2 timer, tilkobler alarmer altså 2 timer efter sidst anvendte gyldige nøgle.

### **Gruppe-DAS**

Gruppe-DAS bruges, hvis der er mere end én adgangsvej til det område, som tyverialarmer styrer, eller hvis k-punktet indgår i et hierarki af over-DAS'er og under-DAS'er. K-punkterne i samme gruppe udveksler informationer med hinanden om til- og frakobling af tyverialarmer i det fælles område, som de giver adgang til.

DAS grupper kan opbygges i et eller flere hierarkier af over-DAS'er og under-DAS'er (overområder og underområder). Når der købes tid i en DAS-gruppe, købes der også tid i alle dens over-DAS'er. Ved tilkobling af en DAS-gruppe, tilkobles også alle dens under-DAS'er.

Der er ingen begrænsninger på antallet af k-punkter i en DAS gruppe. Der kan oprettes 63 forskellige DAS grupper, som dækker hver sit område med én eller flere adgangsveje.

### **Automatisk låsning af døre**

Når alarmer tilkobles ved én af dørene, vil alle dørene i den samme DAS gruppe og alle under-DAS'er automatisk blive låst. På samme måde kan alle døre i en DAS-gruppe sættes til at oplåse, når alarmer frakobles ved én af dørene.

### **Tilbage melding fra tyverialarmer**

Denne funktion giver mulighed for fuld integration mellem adgangskontrol og tyverialarmer. Som følge af denne integration er der "korrespondance" mellem tyverialarmer og låsecomputerens DAS funktion. Dette medfører blandt andet, at både tyverialarmer og DAS-funktionen kan til- og frakobles fra såvel adgangskontrollen som fra tyverialarmens betjeningspanel.

## **4.3.9 Operatører**

### **Programmodul der giver mulighed for at oprette operatører med individuelle rettigheder til anvendelse af programmet.**

I grundlicensen kan der foruden "Systemadministrator" oprettes én ekstra operatør, som begge skal logge ind med adgangskode. Systemadministrator har altid alle programrettigheder.

Med operatørmodul er det muligt at oprette et vilkårligt antal operatører hver med helt individuelle rettigheder. Det er således muligt at oprette operatører med kun lige de rettigheder, der er nødvendig for, at vedkommende kan udføre sine administrative opgaver.

Operatørrettigheder kan begrænses til programmer, vinduer, faneblade og i visse tilfælde til enkelte indtastnings-felter.

Som rettighed til de enkelte objekter kan der normalt vælges mellem: adgang til at ændre data, adgang til kun at se data og ingen adgang til at se data.

Hver operatør kan individuelt anvende sit foretrukne sprog, således at programmet tilpasser sig det valgte sprog ved login.

### 4.3.10 ID-kort design og produktion

**Programmodul der giver mulighed for at designe og printe personlige ID-kort, således at ID-kortproduktion bliver fuld integreret i adgangskontrollen.**

Med den integrerede ID-kort designer er det muligt at designe ID-kort, der passer til firmaets image og behov. Under hver persons stamdata kan der printes et ID-kort til den pågældende person, ved blot at aktivere en knap.

Der kan i programmet oprettes et ubegrænset antal ID-kort profiler således, at ID-kortets tekst og design kan være forskellig for de enkelte medarbejdergrupper, afdelinger, adgangsniveauer, gæstekort mv. Programmet er intuitivt og nemt at bruge, og der medfølger en række ID-kort profiler, som kan inspirere eller danne grundlag for egne ID-kort design.

Personbillede og tekster kan frit placeres over alt på kortet. Tekster kan være faste tekster eller variable tekster, som hentes fra personens stamdata. Der kan frit vælges skrifttype, skriftstørrelse, typografi og farve. Som baggrund kan der indlægges et billede, som kan indeholde firmalogo, billede af firma mv.

ID-kort kan printes på alle typer af kortprintere, såfremt der er installeret en standard Windows driver til den pågældende printer. Ønskes der personbillede på ID-kortet, skal der også erhverves licens til Personbillede modulet.

### 4.3.11 Videoovervågning

**Programmodul der giver videoovervågning via integration med videoservere og kameraer.**

Med videoovervågning i UniLock kan operatører se live video og afspille optagelser hentet direkte fra IP videoservere og overvågningskameraer. Modulet giver videoovervågning og video-verifikation af hændelser i UniLock på en lettilgængelig og tidsbesparende måde.

Video-verifikation i UniLock minimerer tidsforbruget til at finde den korrekte video-sekvens blandt ugers optagelser, da ét museklik starter afspilningen af videosekvensen fra hændelsestidspunktet.

Afspilning af video i UniLock giver et bredt overblik over aktuelle situationer, da man kan se loghændelser, persondata, personbillede og video-sekvens på samme tid.

UniLock kan forbinde direkte til et ubegrænset antal IP-baserede videoserver systemer og kameraer, hvorfra optagelser og live-video hentes og afspilles i UniLock. Der er således frit valg mellem at anvende dedikerede videoserver systemer, eller blot forbinde direkte til overvågningskameraer.

### 4.3.12 Ekstra lokaliteter

**Programmodul der giver Polleren mulighed for at kommunikere med ubegrænset antal lokaliteter.**

I grundlicensen skal alle k-punkter tilsluttes den samme lokalitet/gateway. Med dette modul er det muligt at etablere forbindelse til et ubegrænset antal gateways i et ubegrænset miks af

forbindelsestyper. Forbindelsen til en gateway kan være af typerne: Ethernet (pc-netværk og/eller internettet), USB, telefonnet, GSM-net og COM port.

### **Pc-netværk og internet**

Direkte netværksforbindelse over pc-nettet/internettet til en eller flere lokaliteter, giver mulighed for omkostningsfri forbindelse til lokaliteterne 24 timer i døgnet.

Polleren kan via TCP/IP (internet-protokollen) etablere krypteret forbindelse over pc-netværk og internet til en gateway på lokaliteten, hvortil lokalitetens k-punkter er tilsluttet.

For at begrænse netværkstrafikken, kan Polleren eventuelt programmeres til at etablere forbindelse til lokaliteterne på en række fastlagte tidspunkter, og k-punkterne tjekkes så på samme måde som ved modem opkobling.

### **Telefonmodem**

Polleren kan programmeres til at ringe lokaliteterne op på en række fastlagte tidspunkter.

Hver gang Polleren etablerer modemforbindelse til en lokalitet, vil alle informationer om nye nøgler, slettede nøgler, ændringer i tidstabeller mv., som er foretaget siden sidste opkald, blive sendt ud til de respektive k-punkter. Endvidere stilles uret i k-punkterne, og alle logninger hentes. Før forbindelsen til lokaliteten afbrydes, tjekkes om der er overensstemmelse mellem alle checksummer i k-punkterne og pc'ens database.

## **4.3.13 Antal k-punkter med udvidet antal nøgler**

**Programmodul der åbner for udvidet antal nøglepladser i låsecomputeren.**

**Licens afregnes pr. k-punkt med behovet (k-punkter udover 250 u/b).**

Hvert k-punkt kan i standardkonfigurationen indeholde op til 2500 nøgler med PIN-kode eller 3500 nøgler uden PIN-kode. Op til 65.000 nøgler med PIN-kode kan oprettes i k-punktet ved at anskaffe dette programmodul og for LS10 også et udvidelsesmodul (PCB152).

Ved anskaffelse af udvidelsesmodulet til låsecomputeren (LS10) medfølger dette programmodul uden beregning.

Afregning for programmodulet sker efter det antal k-punkter, der har skal have plads til flere nøgler end i standardkonfigurationen. Er antallet over 250 k-punkter, afregnes kun for de første 250 k-punkter.

## **4.3.14 Områdevisning**

**Programmodul der giver overblik over personers placering, og som kan automatisere styring af tyverialarmen.**

Hver gang en person anvender en læser, bliver det automatisk registreret hvor personen er. Med disse registreringer kan receptionisten, værkførere, sikkerhedsansvarlige mv. hele tiden se, hvem der er mødt, og i hvilke områder de forskellige personer befinder sig.

Når sidste person registreres ude af et område, kan tyverialarmen automatisk blive tilkoblet.

For at hjælpe med korrekt registrering i områder, har operatører mulighed for at markere og flytte personer ind og ud af områderne. Operatører kan også printe personlister som rapport for fremmøde, mønstring, evakuering mv.

**Visning af personer i områder**



Områdevisning indeholder tre forskellige visninger, som henholdsvis giver overblik over alle områder, alle personer eller personer i de enkelte områder. Alle visninger og områder kan overvåges i separate vinduer på samme tid.

Områdeoversigten giver et hurtigt overblik over antallet af personer i de enkelte områder inklusiv detaljer om den seneste hændelse i hvert område.

Personoversigten er en liste med alle personer, hvor der for hver person vises, hvilke områder personen er registreret inde i samt detaljer for deres seneste hændelse.

Hvert område indeholder en liste over personer i området inklusiv hver persons seneste hændelse i området med mulighed for videoverificering, visning af udløbstid og overtrædelse af anti-passback. Hvert område kan åbnes i sit eget vindue, således at de forskellige operatører kan vælge at se netop de områder, der er relevante for den pågældende operatør.

I områdevinduet kan vises personbilleder af de seneste 5 personer, der er gået ind i/ud af området. Dette kan fx være en stor hjælp for portvagten, som hurtigt kan sammenligne den ankomne person med personbilledet.

#### **Anti-passback**

Hvert område indeholder en separat anti-passback funktion, der kan programmeres til at afgive en skærmalarm, når en person har udvist manglende disciplin, ved ikke at stemple sig korrekt ind eller ud af området.

#### **Maksimal opholdstid i område**

For hvert enkelt område kan der angives en maksimal opholdstid, således at hvis en person ikke har registreret sig i denne tid, vil personen automatisk blive flyttet ud af området. Dette sikrer at tyverialarmen automatisk tilkobles, og at områdets personliste er tom til næste arbejdsdags begyndelse.

Tiden for maksimal opholdstid kan mindskes, hvis det kombineres med en arbejdstidstabel, da maksimal opholdstid så først tæller fra udløb af arbejdstiden.

#### **Tyverialarmstyring**

Områder kan styre tyverialarmer, således at tyverialarmen automatisk tilkobles når sidste person forlader et område. Når et område bliver tomt, sender områdevisningen en besked til DAS'en (Decentral Alarm Styring) om at tilkoble tyverialarmen i de relevante alarmområder.

Når et alarmområde tilkobles, tømmes det pågældende område for personer. Denne funktionalitet kan fx anvendes til at tømme områder ved at tilkoble DAS manuelt fra døres læsere, Webadgang, tyverialarm/kontrolcentral eller på foruddefinerede tider på døgnet.

### **4.3.15 Antal Integrationskanaler (import/eksport)**

**Programmodul der åbner for integration med andre systemer i form af både import, eksport eller en kombination af begge.**

Integrationer gør at flere systemer automatisk udveksler informationer og samler derved systemernes funktionalitet til en helhed.

Integrationer sikrer at data er ens i alle systemerne og kun skal indtastes et sted en gang.

UniLock har allerede indbygget integrationsdriver til mange tredjepartssystemer, hvor flere løbende tilføjes.

En række tredjepartssystemer har allerede indbygget integration med UniLock, hvor disse systemer og nye systemer også anbefales at kigge på integration via UniLock programmodulet WebAPI.

### **Eksport af logninger**

Integrationstype der giver mulighed for at eksportere alle UniLock system- og k-punkts logninger.

Eksport af logninger anvendes til at eksportere alle UniLock system- og k-punkts-logninger til tredjepartssystemer, som fx infoskærme, statusovervågning, videoovervågning og registreringssystemer til fremmøde, opholdstid, booking, betaling, løn, time/sag, statistik mv.

Med eksport af logninger kan tredjeparts systemers specifikke funktionalitet automatisk blive baseret på faktuelle data fra UniLock.

Har man i forvejen et foretrukket system til at samle og bearbejde logninger, kan man få udvidet sit samlede overblik ved også at bearbejde logninger fra sit UniLock adgangskontrolsystem.

### **Eksport af transaktionsregistrering**

Integrationstype der eksporterer bestemte logninger (stjerne-indtastninger). Bruges til fx komme- og gå registrering.

Transaktionsregistrering registrerer alle stjerne-indtastninger der er foretaget på læsere i de forskellige k-punkter, og eksporterer dem til en komma-separeret fil. Kun stjerne-indtastninger logges, så personen skal gøre noget aktivt for at blive logget. Transaktionsregistrering kan bruges til komme- og gå-registrering, time/sags styring, jobstyring mv.

Modulet opretter en særskilt fil hvori log-data gemmes i "real time". Det program der skal bruge de loggede informationer "tager" filen ved at omdøbe den. Når dette modul ved næste logning opdager, at filen ikke længere eksisterer, oprettes den automatisk igen.

### **Eksport af adgangsregistrering**

Eksporttype der i en komma-separeret fil i "real time" gemmer persondata for, hvem der har fået adgang hvor og hvornår.

Programmodul der får Polleren til at gemme oplysninger om alle hændelser, der har givet adgang i et k-punkt. Når der kommer en logning, der har givet adgang, gemmes det "real time" i en komma-separeret fil hvem der har fået adgang, hvornår det er sket, i hvilket k-punkt samt andre brugerdefinerede felter for personen.

Disse informationer kan bruges af andre programmer til adgangsstatistik, betalings-systemer, beregning af opholdstid i et område mv.

### **Eksport til Nortec vaskerisystem**

Eksporttype der automatisk eksporterer personer til Nortec vaskerisystem.

Skal en person benytte Nortec vaskerisystem, tilføjes personens lejemålsnummer i UniLock, og Nortec holdes nu automatisk opdateret fra UniLock. Lejemålsnummeret benyttes i Nortec systemet til booking og afregning over huslejen for benyttelse af de respektive maskiner.

Hver gang en lejlighedsnøgle oprettes/ændres i UniLock, bliver nøglen og beboerdata/lejemålsdata automatisk sendt til Nortec systemet.

### **Eksport til Salto adgangskontrol**

Integrationstype der automatisk eksporterer valgte personer og deres adgangsrettigheder til Salto adgangskontrol.

Operatører skal blot redigere personers adgangsrettigheder i UniLock som normalt.

Er en person medlem af en eller flere valgbare UniLock Persongrupper, bliver personen automatisk eksporteret til Salto, som værende medlem af samme "Bruger gruppe niveauer" i Salto.

Salto "Bruger gruppe niveau" indeholder adgangsrettigheder til Salto døre, som tilknyttes personerne i gruppen.

### **Eksport til NOX-alarm system**

Integrationstype der automatisk eksporterer valgte personer og deres adgangsrettigheder til NOX-alarm system.

Operatører skal blot redigere personers adgangsrettigheder i UniLock som normalt.

Al opsætning af NOX-systemet foretages i NOX, mens administration af personer og deres medlemskab af NOX brugerprofil foretages i UniLock.

NOX brugerprofil definerer rettigheder til alarmens forskellige områder, hvor personer med brugerprofilen således har brugerprofilens definerede rettigheder.

Er en person medlem af en valgbar UniLock Persongrupper, bliver personen automatisk eksporteret til NOX, som værende medlem af den angivne brugerprofil og kan ud fra de rettigheder betjene NOX systemet på tastatur/læser/panel tilsluttet NOX centralen.

### **Import af objekter**

Integrationstype der kan automatisere oprettelse, ændring og sletning af personer mv. Data modtages fra andre programmer fx ID-kortfabrik, lønprogram mv.

I grundlicens skal alle personer oprettes, ændres og slettes ved hjælp af Adgangseditoren, dog er det muligt i installationsfasen at importere persondata mv. fra andet program.

Med dette programmodul kan oprettelse, ændring og sletning af personer mv. automatiseres, således at disse informationer løbende modtages fra andre programmer fx ID-kortfabrik, medarbejderdatabase, lønsystem, bookingsystem mv. På den måde kan det undgås at indtaste de samme data mere end en gang.

Ud over personens stamdata kan alle relevante informationer om personen importeres, såsom adgangsrettigheder, nøglekode, gyldighedsperioder mv. Som noget helt specielt er det endvidere muligt at oprette alle andre typer objekter i UniLock (k-punkter, grupper, tidstabeller mv.), mens k-punkter og delte undtagelser også kan editeres og slettes. Det er således reelt muligt at fjernstyre den administrative del af adgangskontrolsystemet fra et andet program.

Informationer fra andre programmer afleveres i XML format som importfil. Eksisterer import-filen, læses den, og de objekter der er i filen oprettes/ændres/slettes tilsvarende i UniLock databasen, hvorefter import-filen slettes. Kommasepareret importfil (CSV) i tidligere format er også mulig af hensyn til bagud kompatibilitet.

Programmet kan ikke anvendes uden aktiv licens (demo-mode). For nærmere oplysninger se særskilt manual.

### **Import af personbilleder**

Integrationstype der automatiserer indlæsning af personbilleder til databasen.

Placér blot billedfiler i billedmappen, og billederne vil automatisk blive anvendt til de korrekte personer og gemt i UniLock databasen.

Automatikken letter arbejdsgangen med at tildele personbillede til personer, da fotoautomat, fotograf, fotoansvarlig mv. blot skal placere billeder i billedmappen.

Personbilleder er automatisk inkluderet i backup, da billederne gemmes i databasen.

Billedfiler kan automatisk slettes efter indlæsning i databasen, så personbilleder kun eksisterer i UniLock databasen.

### **Import fra Active Directory**

Integrationstype der automatisk henter operatører/personer og deres data fra Active Directory.

Når ansatte mv. og deres rettigheder administreres i Active Directory - så administreres disse også automatisk i UniLock.

Active Directory anvendes bl.a. til at styre personers adgang til virksomhedens IT-systemer, hvor det nu også kan kombineres med styring af personers fysiske adgangsrettigheder til virksomhedens lokationer, bygninger, kontorer, lokaler mv.

Når personer oprettes i et Windows miljø sker dette typisk i Active Directory, hvorfra andre systemer automatisk kan hente personers stamdata, login, mailadresse, grupperettigheder mv. Personers placering og grupperettigheder i Active Directory kan fx fortælle noget om, hvilken afdeling personerne hører til, og hvilke systemer personerne må anvende.

Med denne integration kan operatørers/personers stamdata og rettigheder automatisk hentes af UniLock adgangskontrol. Oprettes Julia fx i Active Directory med medlemskab af gruppen for kontoransatte, så kan Julia automatisk oplåse døre og frakoble tyverialarmer i kontorområdet styret af UniLock.

Opret, rediger eller slet blot personer og deres rettigheder i Active Directory og UniLock sørger automatisk for at personernes adgang i døre tilrettes og operatørers rettigheder i programmet tilrettes.

### **Import fra Outlook-kalender (Microsoft Exchange)**

Integrationstype der automatisk henter lokalebookinger fra Outlook-kalender (Microsoft Exchange).

En lokalebooking i Outlook kan automatisk medføre at UniLock sørger for at lokalet er klar til at modtage gæsterne i bookingtiden ved fx at oplåses døre, frakoble tyverialarm, tænde lys, tænde ventilation mv. Når bookingtiden udløber vender alt automatisk tilbage til almindelig drift.

Microsoft Exchange Server indeholder hver lokales kalender, hvorfra systemer som fx UniLock kan aflæse bookingtider.

UniLock aflæser løbende bookingtider i hvert anvendt lokales kalender fra Exchange Serveren (lokal Exchange Server eller Exchange Online (Office 365)), og gemmer de førstkomende bookingtider fra lokalets kalender i de delte undtagelser og indsættes som gyldighedsperioder for mødedeltagernes medlemskab af de valgte persongrupper, som er

valgt til at følge lokalet. I lokalernes bookingtider aktiveres således de valgte delte undtagelser og medlemskab af persongrupper i UniLock.

### **Import fra Pronestor Mødebooking**

Integrationstype der automatisk henter lokalebookinger fra Pronestor mødebooking.

En lokalebooking i Pronestor kan automatisk medføre at UniLock sørger for at lokalet er klar til at modtage gæsterne i bookingtiden ved fx at oplåses døre, frakoble tyverialarm, tænde lys, tænde ventilation mv. Når bookingtiden udløber vender alt automatisk tilbage til almindelig drift.

Pronester indeholder hver lokales kalender, hvorfra systemer som fx UniLock kan aflæse bookingtider.

UniLock aflæser løbende bookingtider i hvert anvendt lokales kalender fra Pronestor, og gemmer de førstkomende bookingtider fra lokalets kalender i de delte undtagelser og indsættes som gyldighedsperioder for mødedeltagernes medlemskab af de valgte persongrupper, som er valgt til at følge lokalet. I lokalernes bookingtider aktiveres således de valgte delte undtagelser og medlemskab af persongrupper i UniLock.

### **Import fra Conventus – Online foreningsadministration**

Importtype der automatisk henter medlemmers medlemskab af hold i Conventus.

Conventus systemet kører på hjemmesiden [www.conventus.dk](http://www.conventus.dk), hvor foreninger mv. har online adgang til at administrere fx sine hold og medlemmer. I Conventus kan foreningens medlemmer online tilmelde sig på hold.

Editering af medlemmer foregår i Conventus. Medlemmers personlige nøgle indlæses i Conventus med en Unitek bordlæser og udleveres efterfølgende til medlemmet.

Anvendes telefon som nøgle, har medlemmet mulighed for selv at indtaste sit telefonnummer, hvilket er en stor fordel ved kortvarige medlemskaber for gæster, turister mv.

UniLock henter automatisk hvert minut de nyeste informationer om foreningens medlemmer fra Conventus, og sikrer at medlemmerne får adgang i døre jævnfør de hold medlemmerne er tilmeldt.

### **Import fra WinKAS – Webbaseret administrationssystem**

Integrationstype der automatisk henter ressourcebookinger og personers adgang fra WinKAS.

En ressourcebooking i WinKAS kan automatisk medføre at UniLock sørger for at lokalet er klar i bookingtiden ved fx at oplåse døre automatisk eller give adgang med PIN-kode/nøgle, frakoble tyverialarmer, tænde lys, tænde ventilation mv. Når bookingtiden udløber vender alt automatisk tilbage til normal drift.

Med integration med WinKAS kan kommuner og andre fx tilbyde online booking af lokaler med automatisk oplåsning/låsning eller adgang med PIN-kode/nøgle.

UniLock forbinder til WinKAS Cloud, som indeholder data for ressourcer i kommunen, organisationen, foreningen mv.

I UniLock indstilles hvilke adgangsrettigheder (persongrupper) bookingers ansvarlige skal gøres gyldige jævnfør, når WinKAS ressourcen er booket.

I UniLock indstilles også hvilke delte undtagelser, de enkelte ressourcers kalender skal styre. En delt undtagelse kan bruges til ekstraordinært at ændre sikkerhedsniveau i døre, til- og frakobling af tyverialarmer, ændre k-punktudganges niveau mv.

### **4.3.16 WebAPI**

**Programmodul der giver mulighed for at en tovejs krypteret webforbindelse for eksterne systemer til den administrative del af UniLock.**

Eksterne systemer som fx overvågningssystemer, SCADA, PSIM, cloudsystemer, smart-phone Apps, kan udføre driftsovervågning, fjernkontrol og administration af UniLock adgangskontrol.

Driftsovervågning udføres ved abonnere på aktuel status for relevante døre, DAS, tyverialarmer, indgange og udgange, logninger, alarmer mv.

Fjernkontrol giver også mulighed for at fjernkontrollere døre og DAS (tyverialarmer).

Administration giver mulighed for at oprette/hente/opdatere/slette personer, persongrupper, k-punkter, DAS, tidsstyringer mv.

WebAPI anvender SignalR til kommunikation, som giver real-time tovejs funktionalitet via en Web forbindelse (WebSocket) mellem klienter og UniLock. Udover at udveksle data giver dette også mulighed for at overvåge selve forbindelsen. UniLock WebAPI anvender krypteret forbindelse (HTTPS) til kommunikationsforbindelsen. Til kryptering kan operatøren vælge sit eget certifikat eller generere et self-signed UniLock certifikat til evaluering og test.

For at hjælpe udviklere godt i gang med at kommunikere med UniLock WebAPI medfølger udviklingsværktøjer med eksempler (SDK) med fuldt funktionsdygtigt klientprogram inklusiv .NET kildekode og Visual Studio projekt. Derudover kan udviklingsværktøjet Swagger aktiveres i udviklingsfasen.

### **4.3.17 Opdateringsaftale**

**Et kalenderår plus løbende år efter erhvervelse af licensen er det ikke muligt at opdatere programmet mere, med mindre der erhverves en opdateringsaftale.**

Ved erhvervelse af en ny licens er der inkluderet et års opdateringsaftale plus løbende år. Hvis der efter dette tidspunkt stadig ønskes mulighed for at opdatere UniLock programmet, skal der erhverves en opdateringsaftale, som erhverves for et kalenderår af gangen.

#### **Nye versioner**

Der videreudvikles konstant på UniLock programmet med nye funktioner, fejlrettelser og tilpasninger til nye versioner af Windows operativsystemet mv.

Der frigives normalt en ny programrevision mindst én gang om måneden. Alvorlige fejlrettelser har første prioritet i vores udviklingsafdeling, og derfor vil mange fejl også blive rettet med det samme, således at der i disse situationer i løbet af få dage er en ny programrevision klar. Nye programrevisioner af programmet vil normalt altid være 100 % bagud kompatibel.

#### **Dækning**

Opdateringsaftalen giver ret til de nyeste programopdateringer af UniLock for Windows. Det påhviler brugeren selv at rekvirere de nye programversioner. I opdateringsaftalen er der

inkluderet hotline gennem leverandøren. Hotline dækker kun programmæssige problemer og fejl ved UniLock programmet, og dækker ikke undervisning i og fejlretning af Windows eller højtlesning af manualen, hvilket faktureres til normal pris.

Der ydes ikke support på programversioner der er over et år gammel.

**Pris i licensenheder**

Prisen i licensenheder for en opdateringsaftale udgør 10 % pr. år af det antal licensenheder, der er i installationen. Prisen i licensenheder for opdatering af en given installation vil kunne aflæses i menuen [Licens], [Opdateringsaftale].

Hvis fx en installation har kørt i 3 år uden opdateringsaftale og der herefter ønskes at opdatere programmet er prisen herfor  $3 \times 10 \% = 30 \%$  af antal licensenheder i installationen på opdateringstidspunktet.

## 5. Licens

### 5.1 Indledning

Inden licensnummeret og licensnøglen er indtastet, kører programmet uden aktiv licens (demo-mode) og der er (næsten) ingen begrænsninger i programmets anvendelsesmuligheder, alle programmer og programmoduler er åbne for gennemsyn og test.

Licensnummer og licensnøgle ligger i databasen. Selve licens-rettighederne ligger i en krypteret licensfil (CFG-fil) med navnet Unitek.cfg, denne fil er fælles for alle installationssteder.

Licensnøglens opgave er at aktivere licensnummeret. Når licensnummeret er aktiveret, kan programmet læse licensrettighederne til den aktuelle installation i selve licensfilen (CFG-filen).

### 5.2 Licensbestilling

Licensen bestilles gennem leverandøren. Bestillingen kan eventuelt foretages på formularen ”Licensbestilling” og efterfølgende sendes til leverandøren/licensudstederen. Efter modtagelse af licensnummer, licensnøgle og nyeste licensfil (CFG-fil) er licensen klar til aktivering.

#### Aktivering af licens

Licensen aktiveres fra programmet Adgangseditor i menuen [Licens].

Efter at licensnummer og licensnøgle er indtastet, vil programmet automatisk gemme disse i databasen. Vær opmærksom på, at licensfilen (CFG-fil) skal have nyere dato end datoen for selve licensbestillingen. Er pc'en tilsluttet internettet, kan nyeste licensfil (CFG-fil) hentes direkte fra internettet i menuen [Licens], [Fra internet].

Når licensen er aktiveret, går programmet ud af demo-mode, og installationsstedets navn fremkommer nu på titellinjen i programmet.

Er der i demo-mode brugt/aktiveret programmoduler, oprettet flere k-punkter mv. end der er licens til, vil programmet ikke køre korrekt når licensen aktiveres.

#### Licensudvidelse

Når der senere skal bruges en udvidelse af antal k-punkter, et ekstra programmodul bestilles dette gennem leverandøren.

Ved licensudvidelse skal kun licensfilen (CFG-filen) opdateres, denne modtages på et medie eller downloades fra internettet. **Licensudstederen kan kræve at programmet skal opdateres ved en licensudvidelse.**

Hvis der "her og nu" skal bruges en licensudvidelse, er det muligt at deaktivere licensen (demo-mode), hvorved der åbnes for alle programmoduler, og det er muligt at tilføje yderligere k-punkter mv. Det er tilladt at køre uden aktiv licens i den periode, hvor der ventes på ny licensfil. Når der modtages en ny licensfil, skiftes igen væk fra demo-mode og licens forholdene er igen bragt i orden.



### **Opdateringsaftale**

Ved erhvervelse af en ny licens er der inkluderet 1 år plus løbende års programopdateringer. Det påhviler brugeren selv inden for denne periode at rekvirere og udvælge den version af programmet, brugeren er mest tilfreds med.

Et år plus løbende år efter erhvervelse af licensen er det ikke muligt at opdatere programmet mere, med mindre der erhverves en opdateringsaftale, som erhverves for mindst et kalenderår af gangen.

I opdateringsaftalen er der inkluderet hotline gennem leverandøren. Hotline dækker kun programmæssige problemer og fejl ved UniLock programmet, og dækker ikke undervisning i og fejlretning af Windows eller højtlesning af manualer, hvilket faktureres til normal pris.

Ved support forventes det, at kunden har nyeste version af programmet installeret.

Er automatisk opdatering af Windows slået til, så bør UniLock programmet også jævnlige opdateres for at sikre konsistens med Windows.

## **5.3 Ansvarsfraskrivelse**

Uniteks software er udviklet med og baseret på Microsoft produkter. Da Microsoft fraskriver sig ethvert produktansvar må Unitek A/S følgelig gøre det samme.

Unitek A/S eller Uniteks leverandør/forhandler kan under ingen omstændigheder være ansvarlig overfor brugeren for direkte eller indirekte tab forvoldt af Uniteks produkter, herunder tab af forventet avance, driftstab, formuetab, tab af data eller deres reetablering, tab af goodwill, tekniske nedbrud, uvedkommendes adgang eller anden lignede følgeskade, i forbindelse med anvendelsen af systemet.

Unitek A/S eller Uniteks leverandør/forhandlers ansvar for tab eller skade kan i intet tilfælde overskride et beløb, som svarer til det beløb brugeren har betalt.

Det er kundens eget ansvar at lovligheden af det på Unitek A/S leverede anlæg lagrede materiale følger den danske lovgivning, samt overholder skrevne og uskrevne etiske regler omkring data og beskyttelse heraf.

### **Reklamationsret**

Programmet er givet i licens som det er og forefindes uden nogen form for garanti.

For direkte eller indirekte tab herunder driftstab og tabt arbejdsfortjeneste - der påføres køberen på grund af materiale- og fabrikationsfejl, hardware- og softwarefejl, samt for beskadigelse/tab af data og/eller programmer - påtager Unitek og Uniteks forhandler sig ingen erstatningspligt. For levering yder Uniteks forhandler samme reklamationsret, som Unitek A/S og Uniteks forhandler yder ikke herudover nogen form for reklamationsret, medmindre der er indgået en skriftlig aftale om udvidet reklamationsret.

Alvorlige reproducerbare funktionsfejl der skriftligt påpeges og beskrives inden 3 måneder efter erhvervelse af licensen rettes uden beregning. Brugeren er forpligtet til at vedligeholde sit IT-netværk, sin pc og holde pc'ens systemsoftware opdateret.

## 6. Installation / opdatering

### 6.1 Indledning

Dette afsnit beskriver forholdene omkring installationen og opdateringer af UniLock programmet.

Der er gjort meget for at gøre installationen og opdatering af UniLock programmet så automatisk som muligt. Uanset om programmet skal afvikles på en enkeltstående pc eller mange i et netværk, er der kun én ting brugeren skal tage stilling til, og det er, til hvilket drev/mappe programmerne og databasen skal installeres.

Ved en opdatering af programmet skal brugeren gøre nøjagtigt det samme som ved installation, da installationsprogrammet selv finder ud af, at det er en opdatering.

### 6.2 Forudsætninger

Følgende forudsætninger bør være opfyldt, for at få en så problemløs installation som muligt.

- Programinstallatøren bør have et indgående kendskab til adgangskontrolsystemets opbygning og funktionalitet.
- Programinstallatøren bør have et indgående kendskab til Windows, og være bekendt med normale udtryk og begreber indenfor Windows og computere i øvrigt.
- Programinstallatøren skal være systemadministrator på installations-pc'en i installationsfasen af UniLock og SQL server.
- En netværksinstallation kræver et indgående kendskab til det benyttede netværk, og bør altid laves i samarbejde med firmaets net ansvarlige.
- Programmet bør installeres på en sikret pc.
- Brug en relativ ny pc med et nyinstalleret operativsystem og ikke en "gammel" pc med et degenereret operativsystem, der lige tilfældig er blevet "ledig".

### 6.3 Systemkrav

Der stilles selvfølgelig visse tekniske krav til det pc-udstyr der skal bruges, men mange af de krav er igen afhængig af en selv – hvor tålmodig er jeg? Hvor længe vil jeg vente før skærmen er opdateret? Hvor stor en skærm kræver jeg? Hvilket operativsystem skal anvendes? mv.

Generelt kan siges, at det anbefales at købe den pc, der var topmodellen for ½ år siden, da den kan erhverves for en rimelig pris sammenlignet med tidens topmodel. Dog må et minimumskrav være en god skærm med høj opløsning.

#### Operativsystem

Fungerende, opdateret og fejlfri 64-bit Windows 10/11 eller Windows Server 2012R2/2016/2019/2022 operativsystem. Kommunikation mellem installations-pc og arbejdsstationer er beskyttet med TLS, hvor operativsystemets TLS-version anvendes.

## Processor

Programmet kræver minimum en flerkernet processor med en hastighed på 1.6 GHz. Ved store systemer bør anvendes tilsvarende større processor.

## RAM

Min. 8 GB gerne mere.

Det er svært at sige noget generelt om krav til RAM, da det afhænger af, hvor mange andre programmer der skal afvikles på pc'en på samme tid.

## Diskplads

Minimum 20 GB.

## Skærm

Skærmen bør være mindst 17".

1600 x 1200 pixels anbefales, og gerne mere.

Opdateringsfrekvens mindst 60 Hz.

## SQL

Fungerende SQL server skal være version 2014 eller nyere. Standards SQL installation fra UniLock er SQL Express 2022, dog SQL Express 2014 ved ældre Windows versioner.

Bemærk at ved manuel installation af SQL Server på installations-pc, skal Windows brugeren [System] tilføjes til administration af SQL Serveren.

## Netværk

Skal programmet installeres i et netværk, bør den til rådighed værende netværksforbindelse ud til de enkelte arbejdsstationer være på minimum 100 Mbit/sek.

## Internet

Det anbefales at have internetforbindelse på installationspc'en minimum i installationsfasen af hensyn til den automatiske installation af Microsoft komponenter og SQL Server.

## Antivirusprogrammer

Antivirus programmer kan give problemer under installationen af UniLock, derfor bør disse deaktiveres, og i nogle tilfælde kan det være nødvendigt af afinstallere disse.

## Virtuel maskine

Anvendes en virtuel maskine i stedet for en fysisk maskine, skal man være opmærksom på nogle fundamentale ændringer i den måde programmer tildeles ressourcer.

Et virtuelt system er et softwareprogram, som installeres på en fysisk maskine, der emulerer et bestemt computersystem. Et virtuelt system kan emulere flere computersystemer på samme tid, hvor det virtuelle system er ansvarligt for at fordele de faktuelle ressourcer (processorkraft, RAM, disk I/O mv.) fra den fysiske maskine mellem computersystemerne.

På det virtuelle systems emulerede systemer installeres operativsystemer som fx Windows.

Man skal være opmærksom på følgende ved et virtuelt systems virtuelle maskiner:

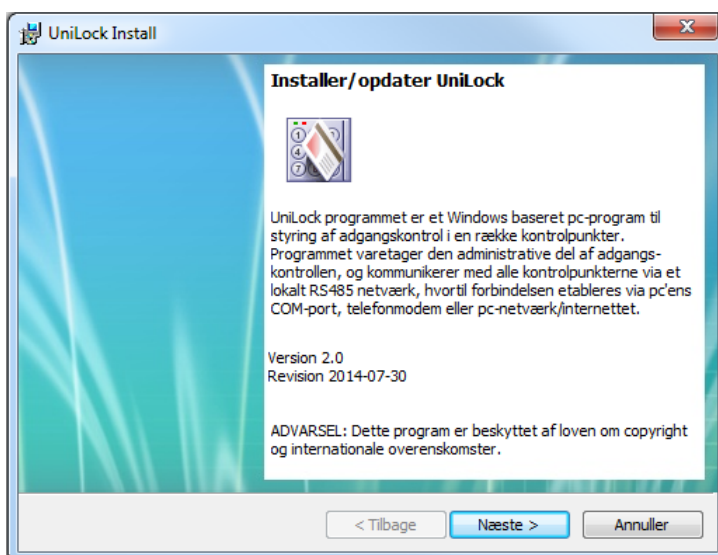
- En virtuel maskine er mindre effektiv end en fysisk maskine, når den skal have adgang til hardwaren.
- Når flere virtuelle maskiner samtidigt afvikles på samme hardware, kan de enkelte virtuelle maskiner udvise varierende / ustabil ydeevne. Stabilitet af ydeevne afhænger af hvor meget systemet påvirkes af andre virtuelle maskiner, og om det virtuelle system kan give tidsmæssig isolation mellem de virtuelle maskiner.

Afvikles UniLock på en virtuel maskine, skal den som minimum have to processorkerner til rådighed, dedikeret fysisk harddisk og sammenlignelige krav som til en fysisk maskine. Opfattes UniLock 'sløv' på den virtuelle maskine, må der tildeles flere ressourcer (processorkraft, RAM, disk I/O hastighed mv.).

## 6.4 Installationsprogram

Installationsprogrammet opretter de nødvendige mapper og undermapper for derefter at kopiere UniLock systemfiler til den valgte destinationsmappe og datafiler til datamappen.

Installationsprogrammet startes ved at dobbeltklikke på installationsfilen "UniLock-Setup.exe".



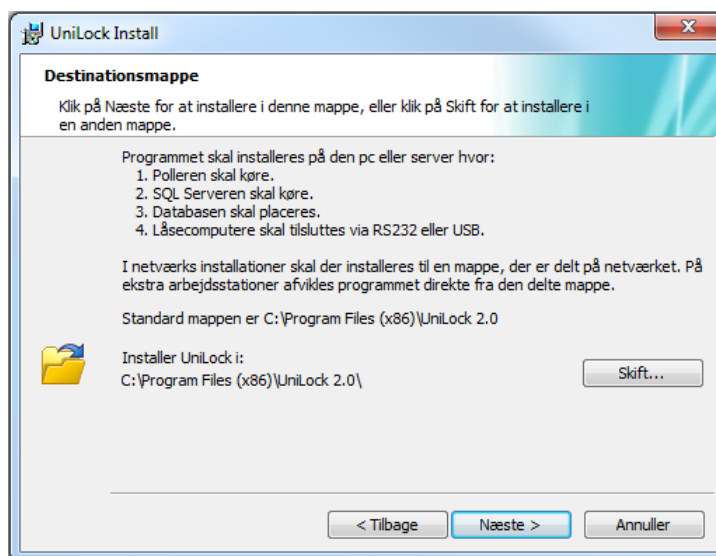
Selve installationen startes ved at aktivere knappen [Næste >].

### Destinationsmappe

I installationsprogrammets dialogboks "Destinationsmappe" angives en programmappe hvortil programfilerne installeres. Som default foreslås "C:\Programmer\UniLock 2.0". Data filer og licensfil installeres automatisk i Windows datamappen "C:\ProgramData\UniLock 2.0".

Destinationsmappen kan udmærket være et drev på en anden pc eller en server, som fx "\\Oles-pc\C\Programmer\UniLock\" eller "\\Server-3\syst\App\UniLock\".

Hvis der før har været foretaget en installation på pc'en, foreslår installationsprogrammet den mappe, der sidst blev installeret til.

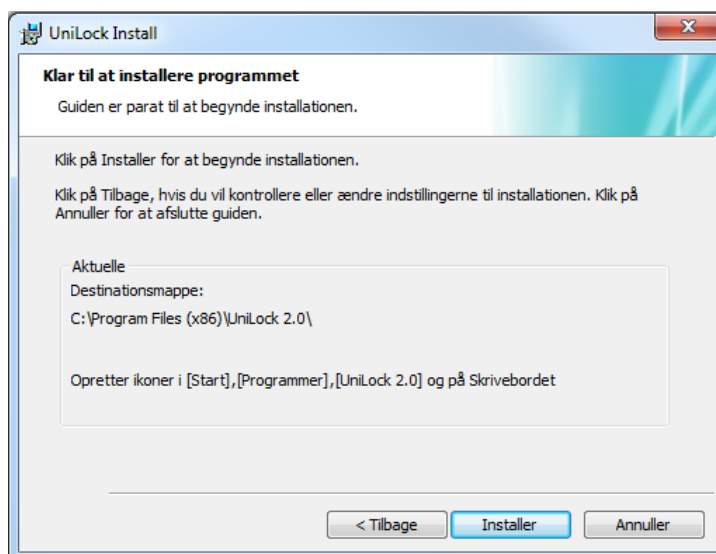


Når destinationsmappe er valgt aktiveres [Næste >].

### Begynd filkopiering

I denne dialogboks vises hvilken mappe programmet installeres i.

Når [Næste >] aktiveres begynder installationsprogrammet filkopieringen til den valgte mappe og datamappen.

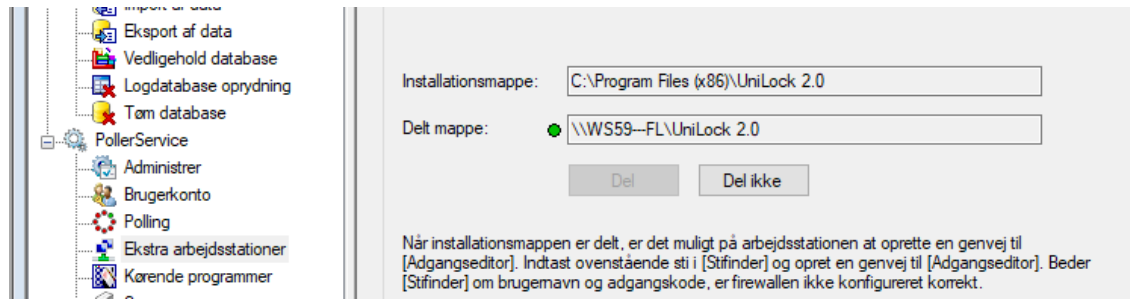


Efter filkopieringen oprettes i menuen [Start], [Programmer], [UniLock 2.0] ikonet der starter UniLock programmet. UniLock ikonet placeres også på Skrivebordet.

## 6.5 Netværksinstallation

Formålet med netværksinstallation er at kunne afvikle UniLock programmet på flere forskellige pc'er i netværket (klienter/arbejdsstationer). Der er reelt ingen forskel på en netværksinstallation og installation på en enkeltstående pc, installationsmappen skal blot være tilgængelig (delt) for klient-pc'erne.

Almindelig deling af installationsmappen kan udføres fra Adgangseditor, [Indstillinger], [PollerService], [Ekstra arbejdsstationer], [Del]:



Den netværksansvarlige skal tildele brugere/klientpc'er alle de nødvendige rettigheder til den delte installationsmappe.

Installationsproceduren på alle pc'er (klienter) er at oprette en genvej til Adgangseditor Launcher-filen (Adgangseditor.exe) på installationspc'en. På klient pc'er afvikles Adgangseditoren fra en lokal kopi (cache) af programmet, som kommunikerer med UniLock PollerService på installations pc'ens port 8734. Launcherens opgave er sikre konsistens mellem programfiler i den lokale cache og programfiler på installationspc'en.

Forbindelsen mellem server og klient er krypteret med TLS. Den TLS version som en klient forbinder til serveren med, vil blive anvendt (Den laveste version UniLock understøtter er i en begrænset periode TLS 1.0 af hensyn til understøttelse af Windows 7).

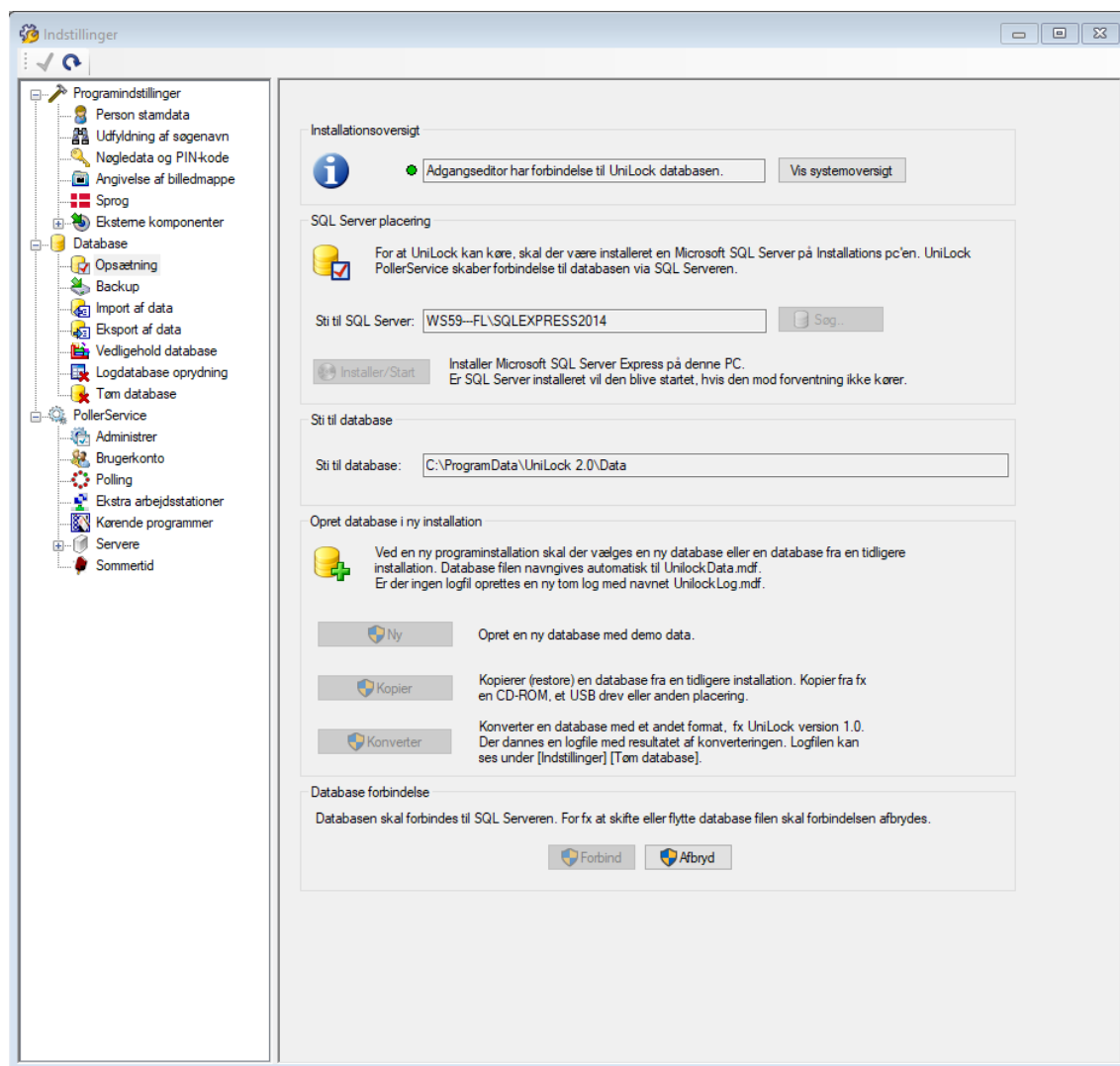
Der anvendes et sikkerhedscertifikat fra serveren (PollerService) til gensidig autentificering mellem server og klienter. Hver gang serveren starter op, bliver der genereret et ny certifikat.

UniLock PollerService udstiller forskellige services, hvor kun status-service er ukrypteret (status for om systemet kører og lignende uden mulighed for manipulation med data).

## 6.6 Database

UniLock anvender SQL Server til håndtering af databaser til henholdsvis data og log.

Første gang programmet startes skal den SQL Server UniLock skal anvende enten vælges eller installeres. Det er ikke muligt at udføre anden opsætning inden der er forbindelse til en SQL Server. Adgangseditor starter automatisk i menuen til databaseopsætning [Indstillinger], [Database], [Opsætning] såfremt der ikke er forbindelse til en SQL Server.



## Installation af database server

Er der ikke en anvendelig SQL Server på pc'en i forvejen, kan programmet hente og automatisk installere en gratis SQL Server fra Microsoft efter tryk på knappen [Installer/Start]. SQL Serveren installeres i "Silent mode", hvor bruger-involvering normalt ikke er nødvendig.

## Valg af database server

For at vælge SQL Server trykkes på knappen [Søg], hvorefter programmet opbygger en liste af fundne SQL Servere på pc'en. Den ønskede SQL Server vælges og efter at programmet har fået forbindelse til SQL Serveren kan databaserne oprettes.

## Opret database

Ved en ny programinstallation skal der vælges en ny database eller en database fra en tidligere installation. Det er muligt at oprette en ny demodatabase, kopiere (restore) fra en tidligere installation eller konvertere en database med et andet format, som fx UniLock 1.0.

Konverteres en database fra en UniLock 1.0 installation, skal UniLock 1.0 være opgraderet til seneste revision inden databasen konverteres.

## Skifte database

I nogle tilfælde kan det være relevant at kunne skifte til en anden database fx fra en tidligere backup eller hvis man skal servicere en database fra en anden installation.

For at skifte database skal forbindelsen til den nuværende database først afbrydes [Afbryd], hvorefter den ønskede database kan kopieres [Kopier].

## 6.7 Efter installation

Efter installationen bør installationsfilen "UniLockSetup.exe" gemmes, til hvis man på en senere tidspunkt får brug for at lave en geninstallation af den "gamle" programversion. Da Unitek A/S altid anbefaler, at anvende den sidst nye programversion, kan Unitek A/S derfor ikke være behjælpelig med at fremskaffe "gamle" installationsprogrammer

### Ikoner

Installationsprogrammet har oprettet ikoner til start af programmet i menuen [Start], [Programmer], [UniLock 2.0], samt på Windows skrivebord.

### Database

Ved en ny installation, oprettes en demodatabase, som indeholder en række personer, k-punkter, tidstabeller mv. Dette er tænkt som et eksempel på, hvordan adgangsstrukturen i en mindre virksomhed kunne være opbygget.

Demodatabasen kan bruges som udgangspunkt for egne indtastninger, således at navnene på k-punkter, personer, tider i tidstabeller mv. tilpasses den pågældende installation. Ønskes det at tømme databasen og derved have en helt tom database som udgangspunkt for sine indtastninger, kan dette gøres i Adgangseditoren i menuen [Indstillinger], [Database], [Tøm database].

### Før indtastning af data

Programmet er et værktøj til administration af firmaets sikkerhedspolitik, programmet kan ikke give firmaet en sikkerhedspolitik. Derfor er det vigtigt at firmaets sikkerhedspolitik defineres før indtastning af programdata.

Sikkerhedspolitikken må derfor indeholde "hvem har adgang til hvilke døre og hvornår", og "hvilket sikkerhedsniveau skal hver dør anvende på forskellige tidspunkter".

Som det ses, kan leverandøren eller programmet ikke løse disse opgaver, men bør være specificeret af installationsstedets sikkerhedsansvarlige før programmet tages i brug. Skriftet "Skemaer og eksempler til adgangskontrol" bør læses, og medfølgende skemaer bør være udfyldt før indtastning af data i programmet.

### Operatører

Skal der oprettes operatører, anbefales det at oprette en ekstra systemoperatør (kopier Systemadministrator) med alle rettigheder, som så bruges i dagligdagen. Gem derefter [Login navn] og [Adgangskode] for operatøren "Systemadministrator" i en bankboks og brug kun denne operatør i nødstilfælde. Glemmes adgangskode for Systemadministrator, er det forbundet med en udgift at få åbnet for adgang til systemet igen.



## Backup

Efter indtastning af mange data, bør der altid tages en sikkerhedskopi af databasen. (se afsnittet "Backup af data").

## Poller

For at Polleren kan kommunikere med k-punkterne skal der vælges en konverter. Dette gøres i Adgangseditoren i menuen [Lokaliteter]. Når "TxD" lampen på konverteren blinker, er der forbindelse til konverteren. Blinker "RxD" lampen, modtages der data fra et k-punkt. For yderligere oplysning se programbeskrivelse af Poller.

## 6.8 Opdatering

Der kommer med jævne mellemrum nye revisioner af programmet og derfor kan det være fornuftigt at opdatere. Det er ikke nødvendigt at afinstallere det eksisterende program før der foretages en opdatering.

En opdatering af UniLock programmet foretages på samme måde som en installation, installationsprogrammet finder selv ud af, at der allerede er en database, og den eksisterende database bevares. Systemfilerne vil blive afinstalleret, hvorefter de nye systemfiler installeres.

### Destinationsmappe

Hvis installationsprogrammet før er afviklet på pc'en, vil installationsprogrammet automatisk foreslå den destinationsmappe, der blev brugt ved sidste kørsel af installationsprogrammet.

### Opdatering i netværk

Når der foretages en systemopdatering på installations pc, vil åbne Adgangseditorer på klient pc'er automatisk blive afsluttet.

Når Adgangseditor startes på en klient pc, vil programcachen på klient pc automatisk blive opdateret til samme revision som på installations pc, hvorefter Adgangseditoren startes. Der skal således ikke udføres manuel systemopdatering på klient pc'er.

## 6.9 Aktivering af licens

Indtil licensnummeret og licensnøglen er indtastet vil programmet køre uden aktiv licens (demo-mode), og der er ingen begrænsninger i programmets anvendelsesmuligheder, alle programmer og programmoduler er åbne for gennemsyn og test.

For at anvende programmet lovligt, skal der erhverves licens til de programmer og programmoduler, som det ønskes at anvende. Læs venligst afsnittet "Licens".

## 6.10 Programfejl

Der er gjort meget for at teste programmet og for at finde de fejl der evt. måtte være i programmet. Alligevel kan der være fejl i programmet, som endnu ikke er opdaget. Hvis der opdages fejl, vil vi selvfølgelig gerne høre det. For at kunne rette fejlen, skal den kunne reproduceres. Det vil i de fleste tilfælde ikke være muligt at rette fejl, der ikke kan reproduceres. Alvorlige reproducerbare funktionsfejl der skriftligt påpeges og beskrives inden 3 måneder efter erhvervelse af licensen rettes uden beregning.

Alvorlige fejlrettelser har første prioritet i vores udviklingsafdeling, og derfor vil mange fejl også blive rettet med det samme, således at der i disse situationer i løbet af få dage er en ny programrevision klar.

Nye programrevisioner af programmet vil normalt altid være 100% bagud kompatible.

## A. Backup af data

Her skal opremses en række gode grunde til jævnligt at tage en sikkerhedskopi af de data, som adgangskontrolsystemets funktionalitet er baseret på.

- Hvis et UniLock program afbrydes, mens det har databasen åben, kan der opstå fejl i databasen. Det kan fx ske ved strømafbrydelse, eller hvis Windows på anden måde lukkes forkert.
- Windows kan være et ustabilt styresystem, som går ned med uforklarlige og uregelmæssige mellemrum.
- Fejl på harddisken kan medføre, at alle data mistes.
- Pc'en med alle data kan blive stjålet.
- Operatøren kan utilsigtet komme til at slette oplysninger i databasen.

### Hvor ofte?

Hvor ofte der bør tages backup afhænger selvfølgelig af, hvor tit og hvor mange ændringer der laves, men der bør altid tages backup før og efter der udføres større ændringer.

Af sikkerhedsgrunde bør en sikkerhedskopi altid gemmes et andet sted end i det rum, hvor pc'en er placeret - og helst uden for huset.

### Backup på papir

En udskrift specielt af alle personer kan også være en god løsning. Det vigtigste er at have nøglekoderne til alle personer. Ud fra disse nøglekoder vil det ved hårdt arbejde være muligt tilnærmelsesvis at rekonstruere databasen, uden at skulle have fat i alle personer og låne deres nøgle for at genindlæse nøglekoden.

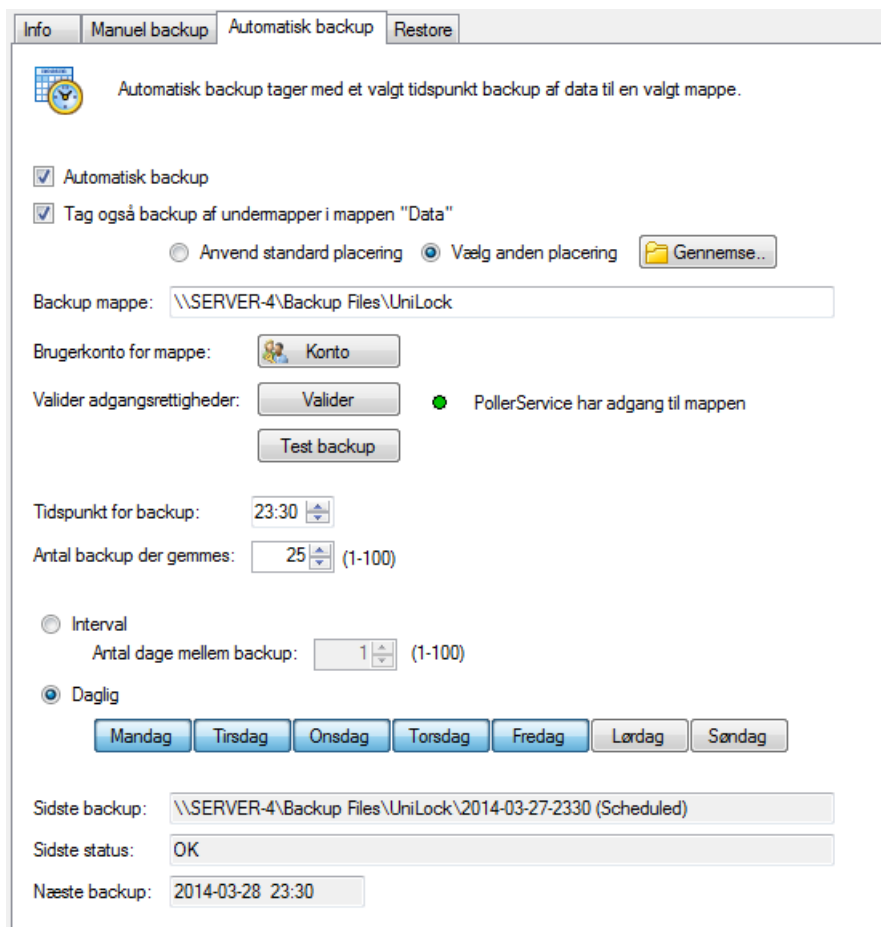
### Filer der bør tages backup af

Hele databasen ligger i filen C:\ProgramData\UniLock 2.0\Data\Database\UniLockData.mdf og loggen ligger i filen C:\ProgramData\UniLock 2.0\Data\Database\UniLockLog.mdb.

Bruges personbilleder er disse inkluderet i databasen.

### Hvordan tages backup

I UniLock kan der manuelt eller automatisk udføres backup til en vilkårlig mappe i netværket.



Det er muligt at inkludere datamappens undermapper i backup. Placeres anden vitale data i undermapper vil UniLock inkludere disse data i backuppen.

Indstilles backupmappen til at være en ekstern mappe, kan det være nødvendigt, at angive den brugerkonto UniLock skal bruge til at få adgang til mappen. En ekstern mappe kan være hvor virksomhedens øvrige backupfiler placeres. Backup af UniLock kan således indgå i virksomhedens samlede backupstrategi.

Når UniLock tager backup bliver backupfilerne først kopieret til default backupmappen på installations pc'en. Er backupmappen en ekstern mappe vil backupfilerne efterfølgende blive kopieret til den eksterne mappe. Uanset om UniLock kan forbinde til den eksterne mappe, vil der således altid være backup fra de ønskede tidspunkter.

Vær opmærksom på at der skal være tilstrækkelig fri plads på harddisk, da Windows kan blive langsom og ustabil ved manglende plads på harddisken.

## B. Lysdiode i læser

### Drift

<b>Grøn</b>	Grøn konstant Slutblik er aktiveret – dør er oplåst.
<b>Rød</b>	Rød konstant i 3,0 sek. 1. Fejlindlæsning af nøgle. 2. PIN-kodetastaturet er aktiveret når det ikke kan/må benyttes. 3. Forkert PIN-kode.
<b>Rød</b>	Rød konstant i 5 minutter Der er lavet 5 forkerte PIN-kode indtastninger efter hinanden. Dette medfører, at tastaturet er blokeret.
<b>Gul</b>	Gul i 5 sek. Når lampe lyser gul, skal PIN-kode eller "stjerne-tal" indtastes. Hver gang en tast aktiveres, tænder gul igen i 5 sek.
<b>Grøn blink</b>	Grøn = 0,5 sek. off = 0,5 sek. Dør er låst.
<b>Grøn blink</b>	Grøn = 0,1 sek. off = 0,1 sek. i 4 sek. 1. Stjerne-indtastning er godkendt. 2. Områdebekræftelse (* + nøgle). 3. Logkort er indlæst (døren oplåses/låses ikke, men nøgle logges).
<b>Grøn blink</b>	Grøn = 0,1 sek. off = 0,1. sek. i op til 15 sek. Frakobling af DAS er sendt til tyverialarm, og der afventes tilbagemelding.
<b>Rød blink</b>	Rød = 0,1 sek. off = 0,1 sek. i 4 sek. Ugyldigt "stjerne-tal".
<b>Rød blink</b>	Rød = 0,2 sek. off = 0,2 sek. 1. Døren er ikke lukket efter en godkendt adgang. 2. Døren er tvangsåbnet.
<b>Gul blink</b>	Gul = 0,1 sek. off = 0,1 sek. i 8 sek. Samme nøgle er benyttet indenfor de sidste 8 sekunder. Der vil gå yderligere 8 sekunder før nøglen kan anvendes igen.
<b>Rød/grøn blink</b>	Rød = 0,2 sek. grøn = 0,2 sek. i 4,0 sek. Nøgle er læst korrekt, men findes ikke i nøgletabellen.
<b>Gul/grøn blink</b>	Gul = 0,3 sek. grøn = 0,2 sek. i 4,0 sek. Nøgle kan anvendes, men ikke på nuværende tidspunkt. 1. Nøglen anvender en tidstabel, der ikke giver adgang nu. 2. Nuværende sikkerhedsniveau er "3", og der er ikke oprettet nogen PIN-kode til den anvendte nøgle. 3. Nuværende sikkerhedsniveau er "4", ingen nøgle kan oplåse på dette niveau. 4. Nuværende sikkerhedsniveau er "0", ingen nøgle kan låse på dette niveau. 5. Nøgle er anvendt i udlæser og døren er allerede oplåst.

### Parameter-fejl

<b>Rød blink</b>	Rød = 0,5 sek. off = 0,5 sek. Døren er låst, og der er parameter-fejl i låsecomputeren.
<b>Grøn/rød blink</b>	Grøn = 2,0 sek. rød = 0,2 sek. Døren er oplåst, og der er parameter-fejl i låsecomputeren.