

LSM 3.4 SP2 SmartUserGuide

Handbok

29.10.2019

Simons  Voss
technologies

Innehållsförteckning

1	Grundfunktioner	4
1.1	Skapa nytt låssystem	4
1.2	Skapa ny transpondergrupp.....	4
1.3	Skapa ny transponder	4
1.4	Tilldela en transponder till en transpondergrupp i efterhand.....	5
1.5	Skapa nytt område	5
1.6	Skapa nytt lås.....	5
1.7	Tilldela låset ett område.....	5
1.8	Tilldela/frånta behörighet	6
1.9	GDPR-funktioner	6
1.9.1	Exportera data.....	6
1.9.2	Radera data	9
1.10	Skapa pinkodsknappsats	11
1.10.1	Konfigurera pinkodsknappsats.....	11
1.10.2	Skapa pinkodsknappsats i låsschemat	12
1.10.3	Programmera pinkodsknappsats.....	12
1.11	Genomsök matris.....	12
1.12	Genomför gruppåtgärder.....	13
1.13	Programmera transponder	14
1.14	Programmera lås	14
1.15	Definiera tidszonsschema (med helgdagar och semestrar).....	15
1.16	Återställning av komponenter	16
1.17	Ersätt defekt lås.....	16
1.18	Ersätta defekta, borttappande eller stulna transpondrar	17
1.19	Kontrollera och utvärdera låsens batteristatus.....	19
1.20	Övergripande låsnivå	20
1.20.1	Skapa övergripande låsnivå.....	20
1.20.2	Länka lås.....	21
1.20.3	Länka transpondrar.....	22
1.20.4	Tilldela transpondrar behörigheter	23
1.21	Skapa brandkårstransponder	24
1.22	Konfigurera DoorMonitoring-komponenter	24
1.23	Programmering via LSM Mobile.....	25
1.23.1	Med Pocket PC/PDA	25
1.23.2	Med laptop, netbook eller surfplatta.....	26
1.24	Återställa lagringsläge hos G1-lås	26

1.25	Hantering av tillträdeslistor.....	27
1.26	Hantera användare (BUSINESS).....	28
1.27	Korthantering.....	28
1.27.1	Ändra konfigurationen.....	29
1.27.2	Översikt.....	31
2	Genomförande av vanliga WaveNet-baserade uppgifter i LSM Business.....	33
2.1	Upprätta en trådlöst WaveNet-nätverk och integrera ett lås.....	33
2.1.1	Förbereda LSM Software.....	33
2.1.2	Första programmering av låskomponenterna.....	33
2.1.3	Förbereda hårdvaran.....	34
2.1.4	Skapa kommunikationsnoder.....	34
2.1.5	Konfigurera nätverk och importera till LSM.....	35
2.2	Driftsättning av DoorMonitoring-låscylindern.....	36
2.2.1	Skapa DoorMonitoring-låscylinder.....	36
2.2.2	Integrera DoorMonitoring-låscylinder i nätverket.....	37
2.2.3	Överför en WaveNet-konfiguration.....	37
2.2.4	Tilldela LockNode till ett lås.....	38
2.2.5	Aktivera låsets inputhändelser.....	38
2.3	Konfigurera RingCast.....	38
2.3.1	Förbereda routern för RingCast.....	39
2.3.2	Skapa RingCast.....	39
2.3.3	Funktionstest.....	40
2.4	Konfigurera eventmanagement (händelser).....	40
2.4.1	Konfigurera en e-postserver.....	40
2.4.2	Ställa in tasktjänst.....	40
2.4.3	Vidarebefordra inputhändelser via RouterNode2.....	41
2.4.4	Vidarebefordra inputhändelser via SREL3-ADV-systemet.....	41
2.4.5	Skapa reaktion.....	43
2.4.6	Skapa händelse.....	44
2.5	Hantera virtuellt nätverk (VN).....	44
2.5.1	Konfigurera låssystem.....	45
2.5.2	Konfigurera VN-tjänst.....	45
2.5.3	Skapa komponenter och konfigurera LSM-Software.....	45
2.5.4	Exportera behörighetsändringar.....	45
2.5.5	Importera behörighetsändringar.....	47
2.5.6	Tipps om VN.....	47
2.6	Identifiering av sabotage.....	47
2.7	DoorMonitoring (SmartHandle) – händelser med trycket.....	47
3	Hjälp och ytterligare information.....	48

1 Grundfunktioner

I detta kapitel beskrivs de grundläggande processerna i LSM Software. I LSM Software kan man ofta komma till de önskade funktionerna på olika sätt. I dessa grundfunktioner förklaras i regel det snabbaste och enklaste sättet.

I SimonsVoss SmartUserGuide beskrivs utförligt hur man skapar och hanterar ett låssystem med hjälp av ett tydligt exempel.

1.1 Skapa nytt låssystem

- ✓ Installationen har genomförts korrekt och en säkerhetskopia har skapats.
- 1. Välj *Redigera/Nytt låssystem* i menyraden.
- 2. Fastställ de önskade alternativen för låssystemet.
 - ↳ För övergripande låsnivåer ska du välja en färg för "Använd som övergripande låsnivå". *Övergripande låsnivåer används som extranivåer till befintliga standardlåssystem. Se Övergripande låsnivå.*
- 3. Klicka på knappen "Spara".
- 4. Klicka på knappen "Avsluta".

1.2 Skapa ny transpondergrupp

- ✓ Ett låssystem har redan skapats.
- 1. Högerklicka på transpondergrupper i "Grupper-Område" i LSM Software.
- 2. Klicka på "Nytt".
- 3. Ge den nya transpondergruppen ett namn och genomför ev. ytterligare inställningar.
- 4. Klicka på knappen "Spara".
- 5. Klicka på knappen "Avsluta".

1.3 Skapa ny transponder

- ✓ Ett låssystem har redan skapats.
- 1. Välj *Redigera/Ny transponder*.
- 2. Fyll i alla attribut och genomför ev. ytterligare inställningar med knappen "Konfiguration".
- 3. Klicka på knappen "Spara och fortsätt".
- 4. Klicka på knappen "Avsluta".

1.4 Tilldela en transponder till en transpondergrupp i efterhand

- ✓ Transpondern och en transpondergrupp har redan skapats.
- 1. Öppna låssystemets egenskaper, t.ex. via menyraden *Redigera/Egenskaper: Låssystem*.
- 2. Välj registerfliken "Transponder".
- 3. I tabellen ska du välja den transponder som du vill tilldela en transpondergrupp.
- 4. Vid "Ändra tilldelning till transpondergrupper" i rullgardinsmenyn ska du välja den transpondergrupp som ska tilldelas transpondern.
- 5. Klicka på knappen "Genomför".
- 6. Klicka på knappen "Spara".
- 7. Klicka på knappen "Avsluta".

När en ny transponder skapas kan den direkt tilldelas en befintlig transpondergrupp.

1.5 Skapa nytt område

- ✓ Ett låssystem har redan skapats.
- 1. Högerklicka på områden i "Områden-Område" i LSM Software.
- 2. Klicka på "Nytt".
- 3. Ge det nya området ett namn och genomför ev. ytterligare inställningar.
- 4. Klicka på knappen "Spara".
- 5. Klicka på knappen "Avsluta".

1.6 Skapa nytt lås

- ✓ Ett låssystem har redan skapats.
- 1. Välj *Redigera/Nytt lås*.
- 2. Fyll i alla attribut och genomför ev. ytterligare inställningar med knappen "Konfiguration".
- 3. Klicka på knappen "Spara och fortsätt".
- 4. Klicka på knappen "Avsluta".

1.7 Tilldela låset ett område

- ✓ Låset och ett område har redan skapats.
- 1. Öppna låssystemets egenskaper, t.ex. via menyraden *Redigera/Egenskaper: Låssystem*.
- 2. Välj registerfliken "Dörrar".
- 3. I tabellen ska du välja den dörr som du vill tilldela ett område.
- 4. Vid "Ändra tilldelning till område" i rullgardinsmenyn ska du välja det område som ska tilldelas dörren.

5. Klicka på knappen "Genomför".
6. Klicka på knappen "Spara".
7. Klicka på knappen "Avsluta".

När ett nytt lås skapas kan det direkt tilldelas ett befintligt område.

1.8 Tilldela/frånta behörighet

Behörigheter kan tilldelas och fråntas i matrisen. I standardinställningen räcker det att man klickar på ett behörighetsfält för att ändra behörigheten.

Behörigheter kan endast tilldelas eller fråntas mellan ett lås och en transponder.

Beakta de båda vyerna:

■ Vy/Dörrar och Personer

I den här vyn ändras behörigheterna för önskad transponder.

■ Vy/Områden och Transpondergrupper

I den här vyn ändras behörigheterna för kompletta grupper.

1.9 GDPR-funktioner

Sedan den 25 maj 2018 gäller dataskyddsförordningen i hela EU. Den reglerar behandlingen av personuppgifter i syfte att säkerställa uppgifternas skydd och fria rörlighet på den europeiska inre marknaden. Först och främst är åtkomst till databasen via det grafiska användargränssnittet bara möjlig med lösenord och motsvarande användarbehörighet. Därutöver sparas inga särskilda kategorier med personuppgifter enligt artikel 9 i dataskyddsförordningen i LSM-programmet. De obligatoriskafälten för en person används uteslutande för att skapa en unik tilldelning av identifikationsmedier inom låssystemet. De obligatoriska uppgifterna behövs bara i systemet så länge som personen besitter ett identifikationsmedium (t.ex. företagstillhörighet). Administratören av låssystemet kan ange hur länge uppgifter ska sparas (se Alternativ/Loggning).

1.9.1 Exportera data



INFO

Texter på främmande språk

För texterna i de exporterade filerna används samma språk som i LSM-Software.

Personer

Du kan exportera de sparade personuppgifterna för personerna i låssystemet som CSV-filer. I så fall genereras tre filer:

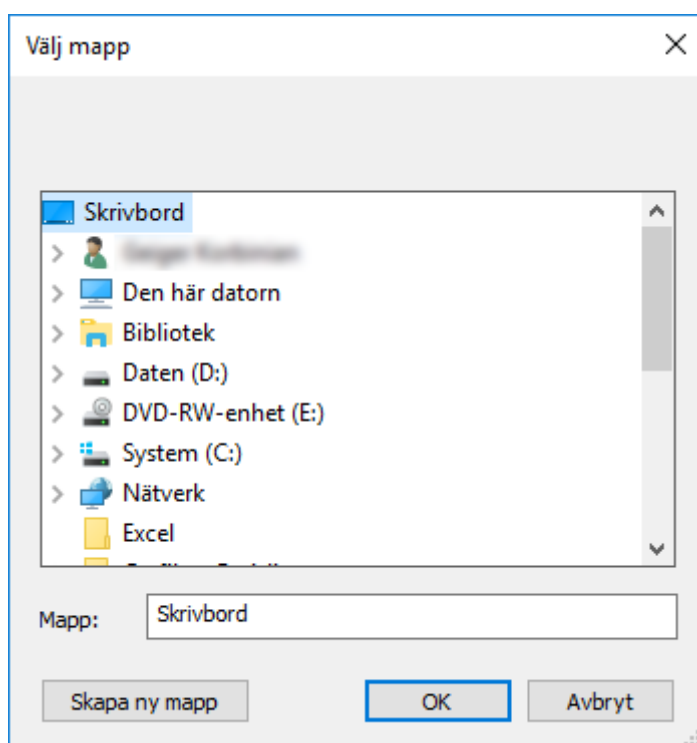
Person	Denna fil innehåller de personuppgifter med vilka en person kan identifieras (t.ex. efternamn, adress eller bild).
PersonHistory	Denna fil innehåller datumet för skapade och radering av datasatsen.
PersonLog	Denna fil innehåller historiken för de redigeringar som genomförts på datasatsen till denna person (till exempel behörighetsändringar eller programmeringar).



INFO

GDPR-funktionerna har åtkomst till personalhanteringen. De måste därför vara tilldelade en användargrupp som är behörig att hantera personal.

- ✓ LSM öppen.
- 1. Välj via | Alternativ | posten **GDPR-funktioner**.
 - ↳ Fönstret "GDPR-funktioner" öppnas.
- 2. I området "Personer" markerar du posten för den person vars uppgifter ska exporteras.
- 3. I området "Personer" klickar du på knappen **Exportera personuppgifter**.
 - ↳ Fönstret "Sökmapp" öppnas.



4. Ange den mapp filerna ska exporteras.
 5. Klicka på knappen **OK**.
- ↳ Uppgifterna exporteras.

Användare

Du kan exportera de sparade personuppgifterna för användarna av LSM-Software som CSV-filer. I så fall genereras två filer:

User	Denna fil innehåller uppgifter om användaren (t.ex. användarnamn och användargrupp).
UserLog	Denna fil innehåller historiken för de redigeringar som genomförts av denna användare (t.ex. skapande av ett nytt lås).



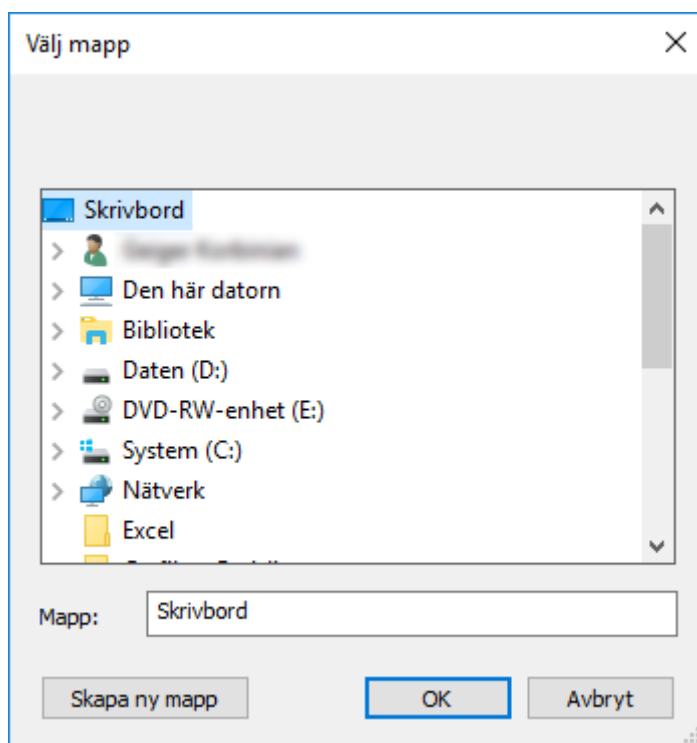
INFO

GDPR-funktionerna har åtkomst till administrationsfunktioner. De måste därför vara tilldelade en användargrupp som har administrationsbehörighet.

- ✓ LSM öppen.
1. Välj via | Alternativ | posten **GDPR-funktioner**.
↳ Fönstret "GDPR-funktioner" öppnas.
 2. I området "Användare" markerar du posten för den användare vars uppgifter ska exporteras.

3. I området "Användare" klickar du på knappen **Exportera personuppgifter**.

↳ Fönstret "Sökmapp" öppnas.



4. Ange den mapp filerna ska exporteras.

5. Klicka på knappen **OK**.

↳ Uppgifterna exporteras.

1.9.2 Radera data

Med GDPR-modulen kan du även enkelt radera personuppgifter.

Personer



INFO

GDPR-funktionerna har åtkomst till personalhanteringen. De måste därför vara tilldelade en användargrupp som är behörig att hantera personal.

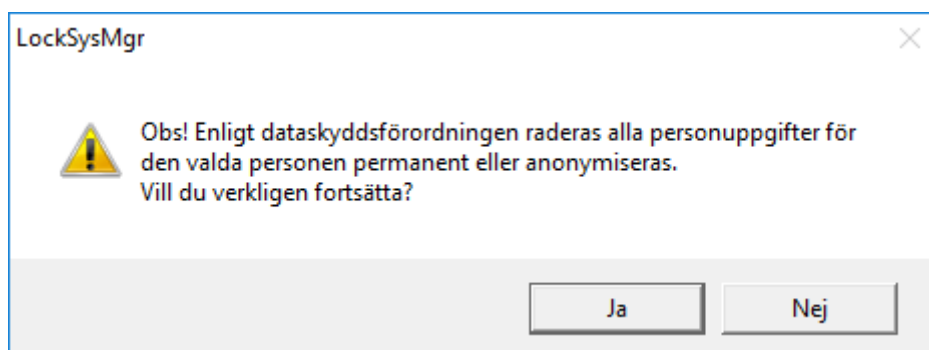
- ✓ LSM öppen.

1. Välj via | Alternativ | posten **GDPR-funktioner**.

↳ Fönstret "GDPR-funktioner" öppnas.

2. I området "Personer" markerar du posten för den person vars uppgifter ska raderas.

3. I området "Personer" klickar du på knappen **Radera personuppgifter permanent**.
↳ Fönstret "LockSysMgr" öppnas.



4. Klicka på knappen **Ja**.
↳ Personuppgifterna för den markerade personen raderas eller anonymiseras.



INFO

Radering av restuppgifter från föregående raderingar

Personuppgifter kan även raderas med knappen **✕** i fliken [Namn] till de tilldelade ID-medierna. I motsats till radering via GDPR-modulen raderas i så fall inte loggarna, utan dessa blir kvar i systemet. Det innebär att endast en del av personuppgifterna raderas. Personer som raderas på detta sätt visas inte mer i GDPR-modulen. För kraven i GDPR ska uppfyllas och även dessa filer tas bort använder du knappen **Radera** i området "Databas".

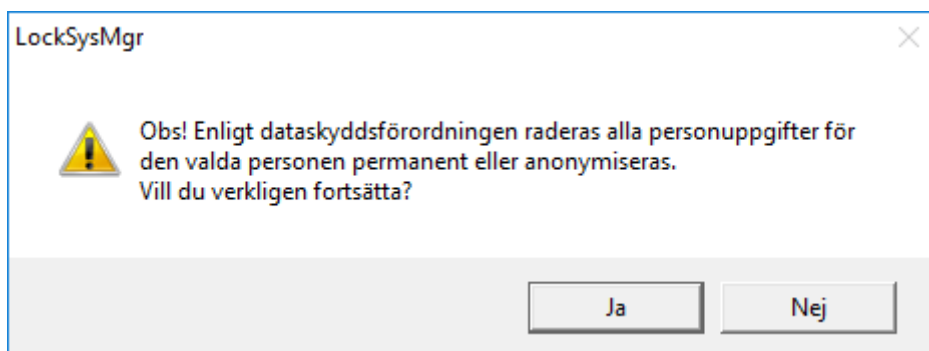
Användare



INFO

GDPR-funktionerna har åtkomst till administrationsfunktioner. De måste därför vara tilldelade en användargrupp som har administrationsbehörighet.

- ✓ LSM öppen.
- 1. Välj via | Alternativ | posten **GDPR-funktioner**.
↳ Fönstret "GDPR-funktioner" öppnas.
- 2. I området "Användare" markerar du posten för den användare vars uppgifter ska raderas.
- 3. I området "Användare" klickar du på knappen **Radera personuppgifter permanent**.
↳ Fönstret "LockSysMgr" öppnas.



4. Klicka på knappen **Ja**.

↳ Personuppgifterna för den markerade användaren raderas eller anonymiseras.

1.10 Skapa pinkodsknappsats

En pinkodsknappsats kan inte användas i rena G2-låssystem. De tre användarpinkoderna uppför sig som G1-transpondrar.

1.10.1 Konfigurera pinkodsknappsats

Ändra masterpinkod

Det här steget behöver endast genomföras om det ännu inte har programmerats en ny masterpinkod.

1. Ange 0 0 0 0
2. Inmatning gammal masterpinkod: 1 2 3 4 5 6 7 8
3. Inmatning ny masterpinkod
 - ↳ Den nya masterpinkoden måste bestå av 8 tecken som inte får vara fortlöpande eller identiska. Koden ska heller inte börja med en nolla.
4. Mata in den nya masterpinkoden igen



INFO

Masterpinkoden är nödvändig för att man ska kunna använda pinkodsknappsatsen och kan varken läsas av eller återställas. Skriv upp masterpinkoden och förvara den på en säker plats som inte kan komma åt av obehöriga. *Personer som känner till masterpinkoden kan öppna och spärra låsen till pinkodsknappsatsen, genom att själv skapa nya användarpinkoder!*

Programmera användarpinkod

I pinkodsknappsatsen kan man tilldela upp till tre användarpinkoder. En användarpinkod kan vara mellan 4 och 8 tecken som inte får vara fortlöpande eller identiska.

Förtydligande: Varje användarpinkod beter sig som en transponder. Därför ska de enskilda användarpinkoderna programmeras i respektive (interna) transpondrar (1, 2 och 3).

1. Inmatning 0
2. Inmatning masterpinkod
3. Inmatning användarpinkod – t.ex. 1 för användarpinkod 1
4. Inmatning av längden på användarpinkoden – t.ex. 4 för en 4-siffrig användarpinkod
5. Inmatning användarpinkod

Upprepa processen för att programmera fler användarpinkoder i pinkodsknappsatsen.

1.10.2 Skapa pinkodsknappsats i låsschemat

För varje användarpinkod måste egen transponder skapas!

1. Välj *Redigera/Ny transponder* i menyraden.
2. Vid alternativet typ i rullgardinsmenyn ska du välja posten "G1-pinkod" och fylla i övriga uppgifter.
 - ↳ Posten kan redigeras detaljerat vid en senare tidpunkt som en transponder.
3. Välj *Spara och fortsätt*.
4. Välj *Avsluta*.

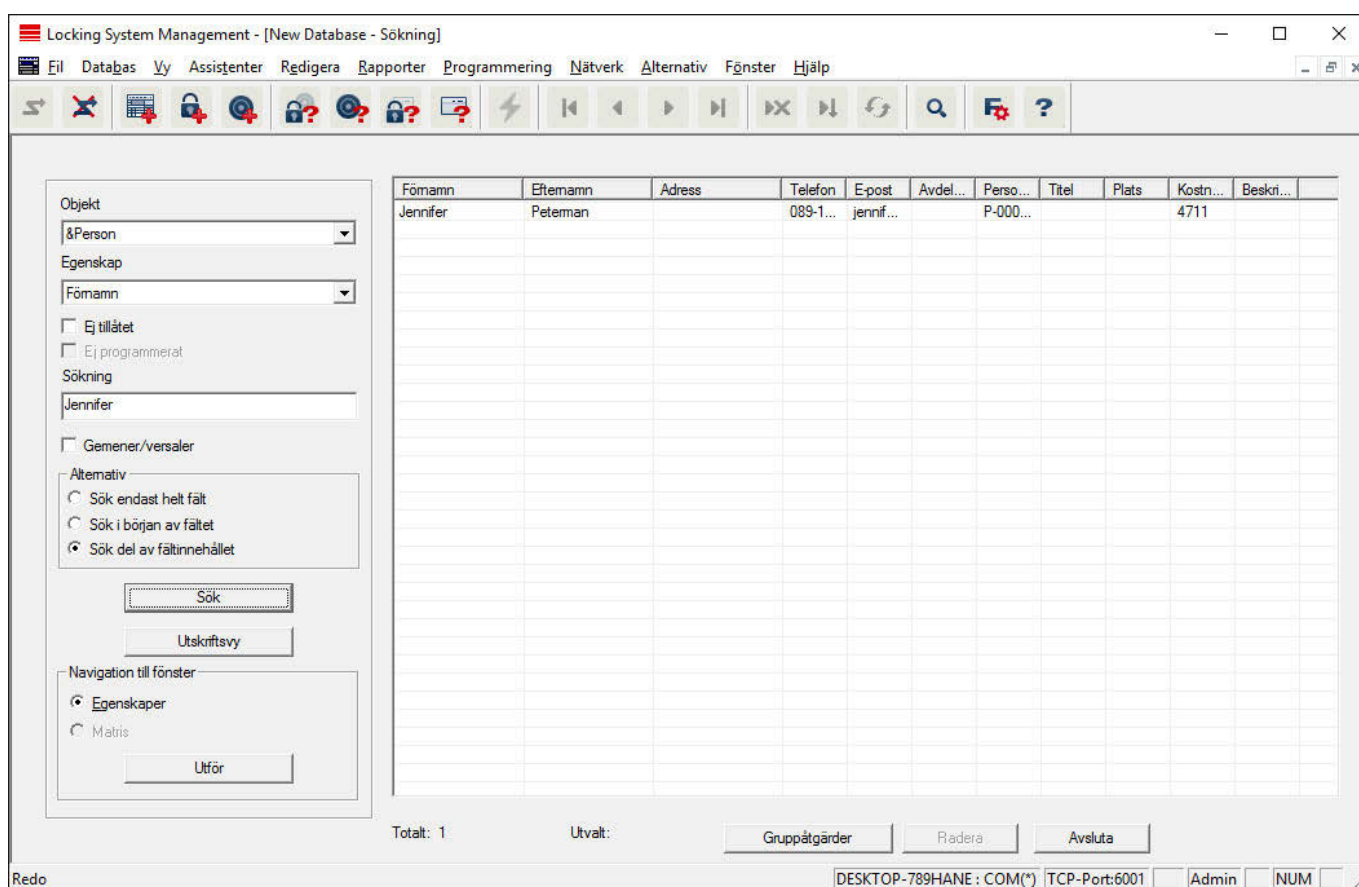
1.10.3 Programmera pinkodsknappsats

1. LSM: Högerklicka på Transponder/Pinkod i låsschemat och välj *Programmera*.
 - ↳ Fönstret "Programmera transponder" öppnas.
2. Pinkodsknappsats: Inmatning 0 0 + masterpinkod
3. LSM: Välj *Programmera*.
 - ↳ Starta programmeringen.
4. Pinkodsknappsats: Tryck på t.ex. 1 för användarpinkod 1/Intern transponder 1 så fort LSM visar meddelandet "Tryck nu kort en gång på knappen på transpondern...".
 - ↳ Programmeringen är nu slutförd.

Upprepa processen för att programmera fler användarpinkoder i låsschemat.

1.11 Genomsök matris

Med sökningen kan man på ett enkelt sätt söka efter olika objekt, till exempel en viss dörr eller en viss transponder.



- ✓ I låssystemet har det redan skapats element som man kan söka efter.

 1. Klicka på förstoringsglaset i symbolraden.
 2. Välj ett objekt som du vill leta efter. Du kan välja t.ex. personer, transpondrar, dörrar, lås, etc.
 3. Välj en egenskap hos det sökta objektet, t.ex. efternamn eller förnamn.
 4. Ange ett sökbegrepp i sökfältet.
 5. Klicka på "Sök" för att starta sökningen.

1.12 Genomför gruppåtgärder

Inställningar kan genomföras samtidigt på olika komponenter i ett enda steg. I det här exemplet ska egenskaperna (*t.ex. Aktivera passerkontroll*) hos flera G2-lås ändras på samma gång.

1. Klicka på förstoringsglaset i symbolraden.
2. Sök till exempel efter alla objekt av typen "lås".
 - ↳ Vid sökning efter alla lås behöver inga uppgifter anges i fältet "Sökning".
3. Välj olika lås genom att till exempel filtrera efter typ eller område.
4. Klicka på knappen "Gruppåtgärder".
 - ↳ Om G2-lås har valts i det föregående steget, väljs de riktiga parametrarna ("*Konfigurationsändringar hos G2-lås*" och "*G2-låscylinder aktiv/hybrid*") direkt.

5. Tryck på knappen "Genomför" för att börja med ändringarna på de valda låsen.
6. Genomför vid behov ändringarna.
7. Spara de nya inställningarna med knappen "Avsluta".



INFO

Med denna metod kan man ändra många inställningar på ett enkelt sätt. Tänk på att alla ändrade komponenter måste programmeras om.

1.13 Programmera transponder

- ✓ En transponder har skapats i låssystemet och är synlig i matrisen.

1. Högerklicka på önskad transponder.
2. Klicka på programmering.
3. Följ anvisningarna i LSM Software.

Tänk på att välja motsvarande programmeringsenhet.

Med knappen "TIDs för avaktivering" öppnar du en lista där du kan välja upp till två transponder-ID:n som ska spärras (se *Ersätta defekta, borttappande eller stulna transpondrar* [[▶ 17](#)]).



INFO

Identifiera G2-kort automatiskt

Kort som används som ID-medier kan inte alltid skiljas åt sinsemellan. Om det finns flera kort måste det kort som ska programmeras först läsas av för att man ska kunna välja rätt kort för programmering i LSM. Detta steg kan hoppas över om man kryssar för alternativet "Identifiera G2-kort automatiskt". När LSM känner igen det aktuella kortet väljs och programmeras passande datasats automatiskt.

1.14 Programmera lås

- ✓ Ett lås har skapats i låssystemet och är synligt i matrisen.

1. Högerklicka på önskat lås.
2. Klicka på programmering.
3. Följ anvisningarna i LSM Software.

Tänk på att välja motsvarande programmeringsenhet.



INFO

Endast ett lås får befinna sig i närheten av programmeringsenheten!!

1.15 Definiera tidszonsschema (med helgdagar och semestrar)



INFO

Avvikande tider vid G2-lås

G2-låsens interna tidsenhet har en tekniskt betingad tolerans på upp till \pm 15 minuter per år.

Vi rekommenderar att man använder tidszonsscheman för hela transpondergrupper och områden. Det är emellertid även möjligt att koppla tidszonsscheman direkt till lås och transpondrar.

- ✓ Lås (eller områden) och transponder (eller transpondergrupper) har redan skapats.
- 1. Klicka på *Redigera/Tidszonsschema* i menyraden.
 - ↳ Ett tomt tidszonsschema öppnas. Om ett befintligt tidszonsschema visas ska du klicka på "Nytt" för att skapa ett nytt, tomt tidszonsschema.
- 2. Fyll i fälten "Namn" och "Beskrivning".
- 3. Välj vid behov helgdagslistan för ditt förbundsland (gäller Tyskland). Gör på följande sätt när du till exempel vill definiera ej återkommande fabrikssemester:
 - ↳ Klicka på fältet "..." intill rullgardinslistan för urval av helgdagar.
 - ↳ Klicka på knappen "Ny helgdag".
 - ↳ Ange ett namn, till exempel "Fabrikssemester 2017".
 - ↳ Nydefinierade helgdagar kan ha en tidsperiod. I så fall måste fältet "Semester" aktiveras. Därefter kan en tidsperiod (från-till) anges.
 - ↳ Välj hur den nya helgdagen ska behandlas, till exempel som "Söndag".
 - ↳ Klicka på knappen "Spara" och därefter på "Avsluta".
 - ↳ Klicka på knappen "Helgdagsadministration".
 - ↳ Infoga din nya helgdag (*i vänster spalt*) med knappen "Infoga" i helgdagslistan (*i höger spalt*).
 - ↳ Klicka på knappen "OK" och därefter på "Avsluta" för att gå tillbaka till tidszonsschemats huvudmeny.
- 4. Välj en grupp i tabellen och redigera veckoschemat för denna.
 - ↳ En blå rad visar en behörighet för denna tid.
 - ↳ Fälten kan väljas enskilt eller markeras alla på samma gång.

↳ Varje gång man klickar på ett fält eller ett område inverteras behörigheten.



5. Klicka på knappen "Spara".
6. Klicka på knappen "Avsluta".

Tilldela tidszonsschemat ett område:

1. Högerklicka på det område som ska tilldelas tidszonsschemat.
2. Välj "Egenskaper".
3. Välj respektive tidszonsschema vid "Tidszon" i rullgardinsmenyn.
4. Klicka på knappen "Spara".
5. Klicka på knappen "Avsluta".

Tidszonsschemat kan även tilldelas direkt till ett lås.

Tilldela tidsgruppen en transpondergrupp:

1. Högerklicka på den transpondergrupp som ska tilldelas tidsgruppen.
2. Välj "Egenskaper".
3. Välj respektive tidsgrupp vid "Tidszonsgrupp" i rullgardinsmenyn.
4. Klicka på knappen "Spara".
5. Klicka på knappen "Avsluta".

Tidsgruppen kan även tilldelas direkt till en transponder.

1.16 Återställning av komponenter

Alla SimonsVoss-komponenter kan återställas när som helst. Även SimonsVoss-komponenter som inte hör till låssystemet kan återställas. I detta fall behöver du lösenordet till tillhörande låssystem.

Komponenter kan behöva återställas av flera anledningar. Särskilt vid möjliga felfunktioner rekommenderar vi att respektive komponenter återställs och omprogrammeras.

1. Läs av de berörda komponenterna via *Programmering/Komponenter*.
2. Klicka på knappen "Återställ" för att starta återställningen.
3. Följ anvisningarna i LSM Software.
 - ↳ Du uppmanas att ange låssystemets lösenord eller välja den datasats som ska raderas.

1.17 Ersätt defekt lås

Det kan hända att lås skadas eller får en defekt.

Ett defekt lås kan bytas ut mot ett nytt på följande sätt:

1. Ta bort det defekta låset från dörren.
 - ↳ Ibland kan det vara svårt att ta bort en cylinder från en låst dörr. Om du är tveksam, vänd dig till den återförsäljare där du köpte dina SimonsVoss-produkter.
2. Införskaffa ett ersättningslås.
 - ↳ Dubbelklicka på det defekta låset i LSM Software så visas alla uppgifter om låset under registerfliken "Utrustning".
3. Genomför en programåterställning av låset i LSM Software.
 - ↳ Genom att dubbelklicka på det defekta låset under registerkortet "Konfiguration/Data" hamnar du vid knappen "Software Reset".
 - ↳ Efter återställningen signaleras programmeringsbehov vid det defekta låset.
4. Genomför programmering av ersättningslåset.
5. Montera tillbaka ersättningslåset i dörren och testa funktionen.



INFO

Om det uppstår fel ska du först försöka återställa låset själv genom en avläsning! Efter återställning kan låset eventuellt programmeras om.



INFO

Om möjligt ska du alltid återställa lås innan du skickar tillbaka dem till en återförsäljare eller till SimonsVoss Technologies GmbH!

1.18 Ersätta defekta, borttappande eller stulna transpondrar

Ibland kan transpondrar tappas bort, skadas eller bli stulna. I alla dessa fall måste den gamla transpondern återställas i låsschemat och en ersättningstransponder måste skapas.



INFO

Av säkerhetsskäl måste behörigheterna för den raderade transpondern tas bort i alla lås. Detta sker genom en omprogrammering av alla lås.

Följ anvisningarna nedan för att ersätta en "gammal" transponder mot en ny, ej programmerad transponder.

1. Införskaffa en ersättningstransponder.
 - ↳ Dubbelklicka på den defekta transpondern i LSM Software så visas alla uppgifter om transpondern under registerfliken "Utrustning".

2. Högerklicka på den defekta, borttappade eller stulna transpondern och välj "Transponderförlust".
 - ↳ Transpondern i fråga förbereds för spärrning.
 - ↳ Ange orsaken till varför denna åtgärd är nödvändig. *Om du väljer "Transponder borttappad/stulen" kan du direkt därefter programmera en ny transponder med samma behörigheter. I G2-protokollet spärrar denna transponder den borttappade transpondern varje gång den används vid ett behörigt lås. Det är trots detta nödvändigt att programmera om alla lås.*
3. Ta hand om alla programmeringsbehov som uppstått på alla komponenter.

Kringgå efterprogrammering av låsen

När en ny ersättningstransponder skapas uppstår programmeringsbehov på alla lås. Dessa speciella programmeringsuppgifter kan dock även genomföras direkt med den nya ersättningstranspondern:

- ✓ Ersättningstranspondern har programmerats korrekt.
1. Aktivera den nya ersättningstranspondern vid alla lås.
 2. Programmera den nya ersättningstranspondern igen. I fönstret "Programmera transponder" ska du aktivera rutan "Läs av avaktiveringskvitteringar/batterivarningar".
 3. Uppdatera matrisen. Det finns inte programmeringsbehov längre.

Från och med LSM 3.4 SP2 är det möjligt att ange upp till två andra transponder-ID:n som ska spärras för valfria transponddrar.

Programmera de TID som ska spärras direkt

De ID som ska spärras sparas på transpondern under programmeringen.

- ✓ Transpondern är fysiskt tillgänglig.
 - ✓ Transponderns programmeringsfönster är öppet.
1. Klicka på knappen "TIDs för avaktivering".
 - ↳ Listan öppnas.
 2. Markera upp till två alternativ i spalten TID för att spara de TID som ska raderas på transpondern.
 3. Bekräfta uppgifterna med knappen "OK".
 4. Fortsätt med programmeringen.
- ↳ Markerade TID sparas på transpondern som TID som ska raderas. När transpondern används vid ett relevant lås spärras de TID som ska raderas vid låset.

De TID som ska raderas sparas i egenskaperna

De ID som ska spärras sparas på transpondern antingen i samband med nästa programmering eller vid nästa aktivering på en gateway.

- ✓ Transponderns egenskapsfönster är öppet.
- 1. Växla till fliken "Konfiguration".
- 2. Klicka på knappen "TIDs för avaktivering".
 - ↳ Listan öppnas.
- 3. Markera upp till två alternativ i spalten TID för att spara de TID som ska raderas på transpondern.
- 4. Bekräfta uppgifterna med knappen "OK".
- ↳ Markerade ID sparas på transpondern antingen i samband med nästa programmering eller vid nästa aktivering på en gateway.

1.19 Kontrollera och utvärdera låsens batteristatus

Batteristatusen på ett lås kan kontrolleras på flera olika sätt. I vanliga Office-låssystem (och VN) måste batteristatusarna först överföras till LSM-Software innan de sedan kan utvärderas på olika sätt.

Överföra batteristatusarna till LSM-Software

Snabbt och effektivt: "Samla" batteristatusar via transponder

1. Använd en transponder som har behörighet till alla lås. Aktivera denna transponder två gånger vid varje lås.
2. Programmera transpondern igen. I fönstret "Programmera transponder" ska du aktivera rutan "Läs av avaktiveringskvitteringar/batterivarningar".

Importera batteristatusar via avläsning av lås

Läs av önskade lås separat via "Programmering/Läs av lås".

Överföra batteristatusarna till LSM-Software via LSM Mobile

Låsens batteristatusar kan läsas av direkt via LSM-Mobile eller överföras till LSM-Software. Följ anvisningarna i handboken "LSM Mobile". Du hittar den på SimonsVoss webbplats (www.simons-voss.com) i supportområdet under Dokument.

Visa batteristatusar

Grundläggande tillvägagångssätt för alla LSM-versioner:

✓ De aktuella batterivarningarna för respektive lås har överförts till LSM-Software.

1. Dubbelklicka på ett lås för att visa låsets egenskaper.
2. Välj registerfliken "Status".
3. Batteristatusen visas i fältet "Status vid senaste avläsning".

Visa batterivarningar i översikt för LSM BASIC Online och LSM BUSINESS:

Generera en lista där alla lås med batterivarningar visas.

✓ De aktuella batterivarningarna för respektive lås har överförts till LSM-Software.

1. Välj "Rapporter/Byggnadsstruktur" i menyraden.
2. Välj egenskapen "Lås med batterivarningar".
3. Klicka på knappen "Visa".

Visa batterivarningar automatiskt för LSM BUSINESS

Skapa en varning som visar batterivarningar direkt.

✓ De aktuella batterivarningarna för respektive lås har överförts till LSM-Software.

1. Välj "Rapporter/Hantera varningar" i menyraden.
2. Skapa en ny varning med "Nytt".
3. Skapa önskad typ av varning. Välj typen "Batterivarning lås".
4. Glöm inte att tilldela denna varning respektive lås! Fältet "Lås" bör inte vara tomt.
5. Bekräfta den nya varningen med "OK".
6. Stäng dialogen med "Avsluta".

1.20 Övergripande låsnivå

Övergripande låsnivåer kan endast drivas med aktiva komponenter. Övergripande låsnivåer kan inte användas tillsammans med passiva korttekniker resp. SmartTags!

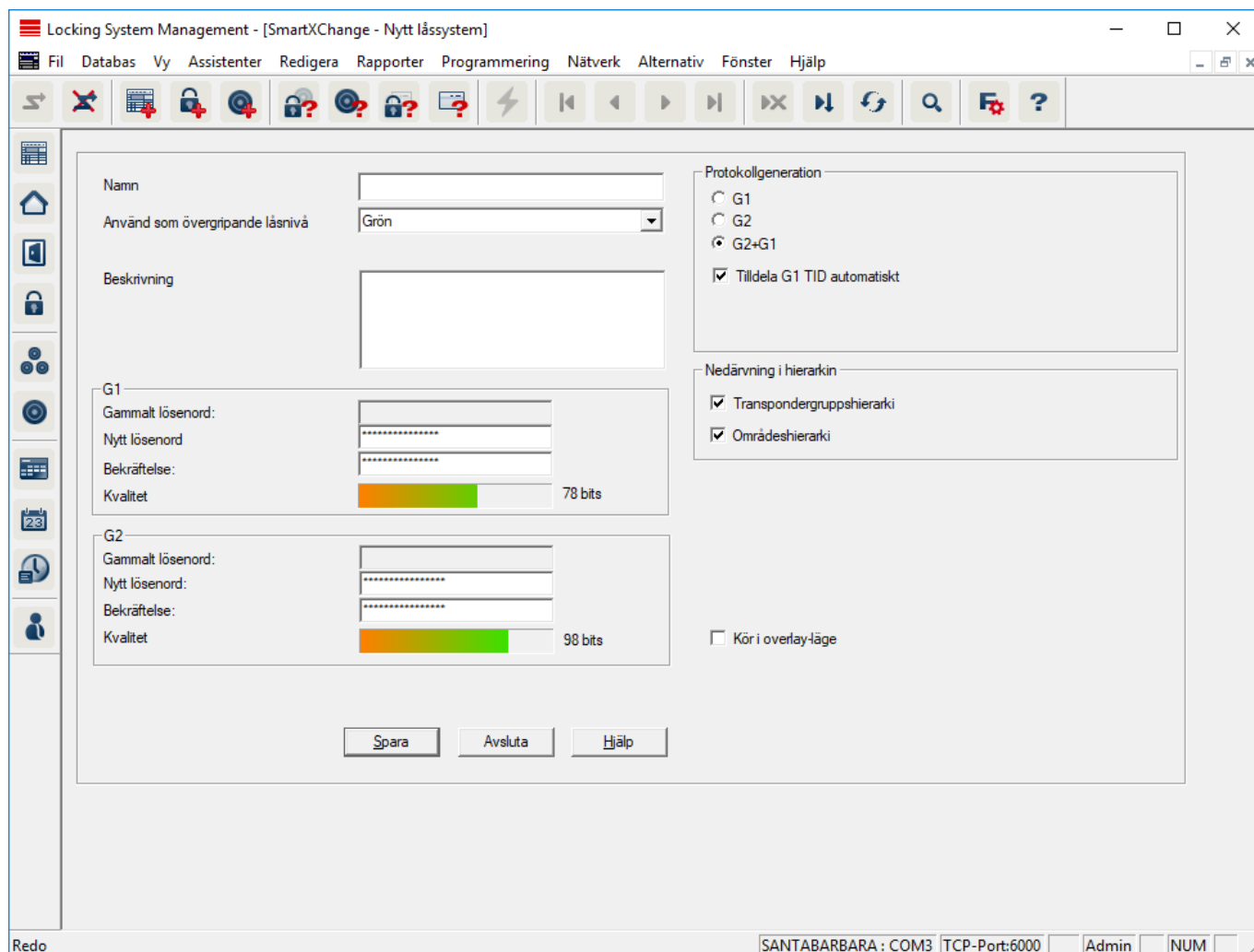
1.20.1 Skapa övergripande låsnivå

Beakta alltid följande i samband med övergripande låsnivåer:

- Övergripande låsnivåer måste ha samma protokollgenerationer.
- Den röda låsnivån bör endast användas av brandkår eller annan räddningstjänst, eftersom den har utvecklats speciellt för detta syfte.

En övergripande låsnivå skapas i princip som alla andra låssystem, t.ex. med knappen "Nytt låssystem" i symbolraden:

- Välj valfri färg under "Använd som övergripande låsnivå".



1.20.2 Länka lås

- ✓ En övergripande låsnivå har redan skapats.
1. I den övergripande låsnivån ska du högerklicka på ett område och välja "Egenskaper".
 2. Klicka på "Dörrhantering".

- I den högra tabellen visas samtliga transpondrar i alla andra låssystem som omfattas av projektet. Välj önskade transpondrar med knappen "Lägg till".

Transponderhantering

Transpondergrupp: [Systemgrupp]

Tilldelat G1 Maximum: 200

Innehavare	Serienummer	Typ	St:
Hansen, Daniel	T-00003	G2-transponder	
Miller, James	000017N	G2-transponder	
Peteman, Jennifer	040L922	G2-transponder	

< - Lägg till alla

< - Lägg till

Ta bort - >

Ta bort alla - >

Ledig

Innehavare	Serienummer	Typ	St:
cleaning, 3	T-00001	G2-transponder	
cleaning, 2	T-00006	G2-transponder	
cleaning, 1	T-00007	G2-transponder	

Totalt: 3 (G1: 3) Utvalt: 0

Status: * - Tilldelningen hos en avaktiverad transponder kan inte ändras!

OK Avbryt

1.20.4 Tilldela transpondrar behörigheter

Precis som i alla övergripande låsnivåer kan man även i den "röda nivån" tilldela valda transpondergrupper behörigheter till alla lås. Den här funktionen lämpar sig särskilt för brandkåstranspondrar.

- ✓ Du har redan skapat en övergripande låsnivå i färgen "röd".
- Öppna det överordnade låssystemet.
 - Skapa en transpondergrupp som ska ha behörighet till alla områden som är relevanta för brandkåren.
 - I transpondergruppens egenskaper ska du klicka på knappen "Behörigheter" vid Hantering.
 - Med hjälp av kryssrutorna ska du välja önskade områden/lås för att säkerställa att transpondergruppen har tillträde till alla dörrar.

1.21 Skapa brandkårstransponder

- ✓ Du har redan skapat minst ett låssystem.
- 1. Skapa en ny, övergripande låsnivå i färgen "röd", t.ex. via *Bearbeta/Nytt låssystem*.
- 2. Lägg till ett nytt område, t.ex. "Alla lås" och tilldela detta till alla önskade lås via "Dörrhantering".
- 3. Skapa den nya transpondergruppen "Brandkår" i den övergripande låsnivån.
- 4. I egenskaperna för transpondergruppen "Brandkår" ska du klicka på knappen "Behörigheter".
- 5. Kryssa för rutan "Skapa alla" för att ge denna transpondergrupp allmän behörighet till alla lås.
- 6. Spara inställningarna med "OK".
- 7. Skapa en ny transponder (t.ex. "Brandkårstransponder 1") i transpondergruppen och programmera den. *Alla lås måste dessutom programmeras om. Beakta att det uppkommit ett nytt programmeringsbehov.*

Transpondern "Brandkårstransponder 1" som skapas i detta steg har behörighet till alla lås. Även avaktiverade lås kan öppnas (i den röda nivån), vilket utgör den stora skillnaden gentemot den "gröna" och "blå" låsnivån.

1.22 Konfigurera DoorMonitoring-komponenter

DoorMonitoring-funktionen är en extrafunktion för att visa dörrstatusar i LSM Software. SmartHandles och låscylindrar med DoorMonitoring-funktion konfigureras precis på samma sätt som vanliga låskomponenter i LSM Software.

- Lägg till ny DoorMonitoring-låscylinder: Välj låstypen "G2 DoorMonitoring-cylinder" i rullgardinsmenyn.
- Lägg till nytt DoorMonitoring-SmartHandle: Välj låstypen "G2 DoorMonitoring SmartHandle" i rullgardinsmenyn.

Registerflik: Konfiguration/data

Genomför fler inställningar under knappen "Monitoring-konfiguration".

Registerflik: DoorMonitoring-status

I den här registerfliken visas dörrrens aktuella status. Den aktuella dörrstatusen visas i realtid.

För att visningen alltid ska vara aktuell krävs en direkt anslutning mellan LSM Software och låskomponent (t.ex. WaveNet). Närmare information om konfiguration av ett trådlöst WaveNet-nätverk hittar du i WaveNet-handboken.

1.23 Programmering via LSM Mobile

Via LSM Mobile kan programmering genomföras direkt vid låsen med mobila enheter. Denna typ av programmering sker på följande sätt:

1. En lista med komponenter som behöver programmeras exporteras från LSM Software till den mobila LSM Mobile-enheten. *Antingen direkt på Pocket PC eller som fil för en notebook, netbook eller surfplatta.*
2. LSM Mobile startas på den mobila enheten. Via exporten i LSM Software kan programmeringen av komponenterna påbörjas.
3. LSM Software måste därefter få information om vilka komponenter som programmerats via LSM Mobile. Detta görs genom en import resp. synkronisering från LSM Mobile till LSM Software.

1.23.1 Med Pocket PC/PDA



INFO

Programmering via LSM Mobile med en Pocket PC resp. PDA fungerar endast i G1-protokollet.

Programmering med LSM Mobile genomförs på följande sätt:

- ✓ I LSM Software finns komponenter som behöver programmeras.
 - ✓ På dessa komponenter har det redan genomförts en första programmering.
 - ✓ LSM Mobile har installerats korrekt på den mobila enheten. Versionsnumren är identiska.
 - ✓ Programmeringsenheten SMARTCD.G2 är laddad och ansluten till PDA via Bluetooth.
 - ✓ Drivrutinen till Pocket PC har installerats korrekt och det har upprättats en anslutning.
1. Välj *Programmering/LSM Mobile/Export till LSM Mobile/LSM Mobile PDA*.
 2. Följ anvisningarna i LSM Software och överför programmeringsuppgifterna till PDA.
 3. Starta LSM Mobile på PDA och logga in på önskat låssystem.
 4. Genomför programmeringarna på önskade komponenter med hjälp av programmeringsenheten.

5. Välj *Programmering/LSM Mobile/Import från LSM Mobile/LSM Mobile PDA*.
6. Följ anvisningarna i LSM Software och synkronisera programmeringsuppgifterna.

Programmeringsuppgifterna har överförts till PDA. När synkroniseringen i det sista steget har genomförts, försvinner blixterna som indikerar programmeringsbehov i LSM Software.

1.23.2 Med laptop, netbook eller surfplatta

Programmering med LSM Mobile genomförs på följande sätt:

- ✓ I LSM Software finns komponenter som behöver programmeras.
- ✓ På dessa komponenter har det redan genomförts en första programmering.
- ✓ LSM Mobile har installerats korrekt på den mobila enheten. Versionsnumren är identiska.
- ✓ Drivrutinerna till programmeringsenheterna SMARTCD.G2 och SMARTCD.MP (efter behov) är korrekt installerade.

1. Välj *Programmering/LSM Mobile/Export till LSM Mobile/LSM Mobile PC*.
2. Följ anvisningarna i LSM Software och exportera programmeringsuppgifterna till en fil.
3. Starta LSM Mobile på den mobila enheten och importera filen med programmeringsuppgifterna i LSM Mobile.
4. Följ anvisningarna i LSM Mobile.
5. Genomför programmeringarna på önskade komponenter med hjälp av programmeringsenheten.
6. Exportera statusen för programmeringsuppgifterna.
7. Välj *Programmering/LSM Mobile/Import från LSM Mobile/LSM Mobile PC*.
8. Följ anvisningarna i LSM Software och importera filen ur LSM Mobile.

Programmeringsuppgifterna har genomförts på den externa enheten. När importen i det sista steget har genomförts, försvinner blixterna som indikerar programmeringsbehov i LSM Software.

1.24 Återställa lagringsläge hos G1-lås

Om batterivarningarna i G1-lås inte beaktas, växlar låsen i fråga till lagringsläget. Detta förhindrar att batterierna laddas ur helt. Lagringsläget kan avslutas genom att låset programmeras om. Därefter måste låset omedelbart öppnas med en behörig transponder och batterierna bytas ut.

1.25 Hantering av tillträdeslistor

Avläsningen av passer- och tillträdeslistor kan inskränkas kraftigt för att skydda den personliga integriteten. I LSM BASIC är som standard en separat användare "AdminAL" (Admin Access List) skapad i detta syfte.. I LSM BUSINESS kan en motsvarande användare skapas manuellt, se *Hantera användare (BUSINESS)* [▶ 28].

I detta kapitel beskrivs följande scenario: Endast en person (t.ex. företagsråd inloggad som AdminAL) ska kunna läsa av passer- och tillträdeslistor. Låssystemets allmänna administratör tilldelas inte denna rättighet.

Konfigurera AdminAL och tillåt avläsning av tillträdeslistor

1. Logga in på projektet med användarnamnet "Admin" och ditt lösenord.
2. Öppna hanteringen av användargrupper via "Redigera/Användargrupp".
3. Använd navigationspilarna för att gå till användargruppen "Hantering tillträdeslistor" (resp. till en valfri, tidigare skapad användargrupp i LSM BUSINESS).
4. Under "Roller" ska du kontrollera att rättigheterna "Hantering tillträdeslistor" och "Hantera tillträdeslistor" är förkryssade.
5. Klicka på fältet "Redigera" under området "Roll".
6. Aktivera önskat låssystem både i transpondergrupperna och i områdena. Om du har skapat områden resp. transpondergrupper måste du dessutom aktivera alla önskade områden resp. transpondergrupper separat!
7. Stäng fönstret med "OK".
8. Bekräfta dina inställningar med "Ta över" och "Avsluta".
9. Logga ut från det aktuella projektet "Databas/Logga ut".

Frånta rättigheten att läsa av tillträdeslistor från Admin



INFO

Rättigheten "Hantering tillträdeslistor" måste alltid innehas av en användare/användargrupp och får inte fråntas båda!

1. Logga in på projektet med användarnamnet "AdminAL".
 - ↳ Standardlösenordet i LSM BASIC är "system3060".
 - ↳ Ändra omedelbart detta lösenord!
2. Öppna hanteringen av användargrupper via "Redigera/Användargrupp".
3. Använd navigationspilarna för att gå till användargruppen "Admin".

4. Avaktivera rollen "Hantering tillträdeslistor" och "Hantera tillträdeslistor".
5. Bekräfta dina inställningar med "Ta över" och "Avsluta".
 - ↳ Konfigureringen är avslutad. Passer- och tillträdeslistor kan nu endast läsas av eller visas från användarkontot "AdminAL".

1.26 Hantera användare (BUSINESS)

Tilldela användare en användargrupp

1. Klicka på "Redigera/Användargrupp".
2. Använd navigationspilarna för att gå till en användargrupp (eller skapa en ny användargrupp med knappen "Nytt").
3. Klicka på knappen "Redigera".
4. Markera önskad användare och tilldela användaren en användargrupp med knappen "Lägg till".
5. Bekräfta dina inställningar med "OK".
6. *Korrigera vid behov rollerna.*
 - ↳ Klicka på fältet "Redigera" under området "Roll".
 - ↳ Aktivera önskat låssystem både i transpondergrupperna och i områdena. Om du har skapat områden resp. transpondergrupper måste du dessutom aktivera alla önskade områden resp. transpondergrupper separat!
 - ↳ Stäng fönstret med "OK".
7. Bekräfta dina inställningar med "Ta över" och "Avsluta".

Skapa ny användare

1. Klicka på "Redigera/Användare".
2. Klicka på "Nytt" för att skapa en ny användare.
3. Ge användaren ett användarnamn och ställ in ett lösenord.
4. Bekräfta dina inställningar med "Ta över" och "Avsluta".

1.27 Korthantering

Nedan ser du de olika korttyperna och fördelningen av lagringsutrymme i förbindelse med SimonsVoss-låssystemet.

OBS

MIFARE DESFire rekommenderas

MIFARE DESFire använder en mer avancerad kryptering jämfört med MIFARE Classic, med stöd på mikroprocessornivå enligt AES-128, som tillgodoser även höga säkerhetskrav.

- SimonsVoss rekommenderar användning av transpondrar eller MIFARE-DESFire-produkter.



INFO

Olika mallar för AX-produkter

När du vill använda MIFARE-produkter för SimonsVoss-AX-produkter måste skriv- och läsmallarna som används vara identiska.

1.27.1 Ändra konfigurationen


Kort kan användas på två sätt.

- Du kan använda kort som redan används.
- Du kan använda nya kort.

I båda fallen anger du korttypen, konfigurationen och vid behov sektorerna som ska beskrivas (se *Översikt [▶ 31]*).

Konfigurera kort

- ✓ LSM öppen.

1. Gå till det låssystem, vars korthantering du vill ändra.
2. Öppna låssystemets egenskaper genom att klicka på knappen .

3. Gå till registerkortet [Korthantering G2].

Namn | Lås | Dörrar | Transponder | Transpondergrupper | Områden | Lösenord | Special-TID:n | Pinkodsterninal | Korthantering G1 | Korthantering G2

Låssystem: HIMYM Nivå: Standard

Korttyp: Mifare Classic

Konfiguration: MC1000L_AV

Minnesbehov: 528 Bytes

Låsings-ID:n: 128-1127 i kortprofilen

Tilträden i protokollet: 19

Virtuellt nätverk: OK

Parameter:

Namn	Värde	Beskrivning
SectList	2,3,4,5,6,7,8,9,10,11,12,13,14,15	Sector List
TransportSectorT...	*****	Transport Settings

Utskriftsvy

- 4. Välj din korttyp i rullgardinsmenyn ▼ Korttyp.
- 5. Välj din konfiguration i rullgardinsmenyn ▼ Konfiguration.
- 6. Ange vid behov ytterligare parametrar såsom sektorer (t.ex.: 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15).

Namn	Värde	Beskrivning
SectList	2,3,4,5,6,7,8,9,10,11,12,13,14,15	Sector List
TransportSectorT...	*****	Transport Settings

- 7. Klicka på knappen Spara .
- ↳ Du har nu ändrat konfigurationen.

1.27.2 Översikt

	MIFARE DESFire	MIFARE DESFire Predefined	MIFARE DESFire Predefined DB1
MDBasic	✓	✓	✗
MD1200L	✓	✓	✗
MD3800L	✓	✓	✗
MD2500L_AV	✓	✓	✗
MD4000L_AV	✓	✓	✗
MD10000L_AV	✓	✓	✗
MD32000L_AV	✓	✓	✗
MD2400L_AV	✗	✗	✓
MD3650L_AV	✗	✗	✓

	MIFARE Classic	MIFARE Classic Predefined A	MIFARE Classic Predefined B	MIFARE Classic + DESFire	MIFARE Plus S/X
MCBasic	✓	✓	✓	✗	✓
MC1200L	✓	✓	✓	✗	✓
MC3800L	✓	✓	✓	✗	✓
MC1000L_AV	✗	✓	✓	✗	✓
MC2400L_A V	✗	✓	✓	✗	✓
MC8000L_A V	✗	✓	✓	✗	✓
MBasic	✗	✗	✗	✓	✗
M1200L	✗	✗	✗	✓	✗
M3800L	✗	✗	✗	✓	✗
M1000L_AV	✗	✗	✗	✓	✗
M4000L_AV	✗	✗	✗	✓	✗
M8000L_AV	✗	✗	✗	✓	✗
M10000L_AV	✗	✗	✗	✓	✗

	G1/G2	Lock-IDs	Anzahl der Schließu ngen	Begehun gsliste	Sektoren	Benötigte r Speicher platz	Virtuelles Netzwerk
MCBasic	G1	✗	✗	✗	2-15	48	✗
MC1200L	G2	128-1327	1200	✗	2-15	192	✗

	G1/G2	Lock-IDs	Anzahl der Schließu ngen	Begehun gsliste	Sektoren	Benötigte r Speicher platz	Virtuelles Netzwerk
MC3800 L	G2	128-3927	3800	✘	2-15	528	✘
MC1000L _AV	G2	128-1127	1000	19	2-15	528	✓
MC2400L _AV	G2	128-2527	2400	70	2-15 + 31-39	900	✓
MC8000 L_AV	G2	128-8127	8000	125	2-15 + 31-39	2048	✓
MBasic	G1	✘	✘	✘	2-15	48	✘
M1200L	G2	128-1327	1200	✘	2-15	192	✘
M3800L	G2	128-3927	3800	✘	2-15	528	✘
M1000L_ AV	G2	128-1127	1000	16	2-15	528	✓
M4000L_ AV	G2	128-4127	4000	100	2-15 + 31-39	1600	✓
M8000L_ AV	G2	128-8127	8000	124	2-15 + 31-39	2048	✓
M10000L _AV	G2	128-10127	10000	225	2-15 + 31-39	3048	✓
MDBasic	G1	✘	✘	✘	2-15	48	✘
MD1200L	G2	128-1327	1200	✘	2-15	192	✘
MD3800 L	G2	128-3927	3800	✘	n.a. (DESFire)	528	✘
MD2500L _AV	G2	128-2627	2500	58	n.a. (DESFire)	1024	✓
MD4000 L_AV	G2	128-4127	4000	100	n.a. (DESFire)	1600	✓
MD1000L _AV	G2	128-10127	10000	225	n.a. (DESFire)	3048	✓
MD3200L _AV	G2	128-32127	32000	470	n.a. (DESFire)	7000	✓
MD2400L _AV	G2	128-2527	2400	34	n.a. (DESFire)	830	✓
MD3650L _AV	G2	128-3777	3650	2	n.a. (DESFire)	830	✓

2 Genomförande av vanliga WaveNet-baserade uppgifter i LSM Business

I det här exemplet beskrivs de viktigaste stegen för upprättande och administration av ett trådlöst WaveNet-nätverk via LSM Business. Exempelen gäller för vissa installationer och hjälper dig att lära känna WaveNet-funktionen närmare.

2.1 Upprätta en trådlöst WaveNet-nätverk och integrera ett lås

I detta inledande exempel beskrivs hur ett trådlöst WaveNet-nätverk skapas från grunden. Målet är att aktivera ett lås via en aktuell RouterNode2.

2.1.1 Förbereda LSM Software

För att SimonsVoss-låskomponenter ska kunna kopplas upp i ett nätverk måste LSM-Software ha installerats korrekt och en lämplig nätverksmodul ha licensierats!

1. Installera CommNode-servern och försäkra dig om att tjänsten har startats.
2. Installera den aktuella versionen av WaveNet Manager. (Se Installation av WaveNet Manager)
3. Öppna LSM-Software och välj "Nätverk/WaveNet Manager".
 - ↳ Ange installationskatalogen för WaveNet Managers och välj en katalog för utmatningsfilen.
 - ↳ Starta WaveNet Manager med knappen "Starta".
4. Ställ in ett lösenord för att öka säkerheten för ditt nätverk.
 - ↳ WaveNet Manager startar och inställningarna sparas för framtiden. Avsluta WaveNet Manager för att genomföra fler inställningar.

2.1.2 Första programmering av låskomponenterna

Innan lås kan integreras i nätverket måste dessa först programmeras.

2.1.2.1 Skapa nytt lås

- ✓ Ett låssystem har redan skapats.
1. Välj *Redigera/Nytt lås*.
 2. Fyll i alla attribut och genomför ev. ytterligare inställningar med knappen "Konfiguration".
 3. Klicka på knappen "Spara och fortsätt".
 4. Klicka på knappen "Avsluta".

2.1.2.2 Programmera lås

✓ Ett lås har skapats i låssystemet och är synligt i matrisen.

1. Högerklicka på önskat lås.
2. Klicka på programmering.
3. Följ anvisningarna i LSM Software.

Tänk på att välja motsvarande programmeringsenhet.



INFO

Endast ett lås får befinna sig i närheten av programmeringsenheten!!

2.1.3 Förbereda hårdvaran

Aktuell RouterNode2 är snabb och enkel att ta i drift. Anslut RouterNode2 med hjälp av medföljande snabbguide. RouterNode2 är inställd från fabrik så att den hämtar sin IP-adress från en DHCP-server. Med hjälp av OAM-verktyget (*kan laddas ned gratis i supportområdet under Infomaterial/ Software-Downloads*) kan du snabbt fastställa denna IP-adress.



INFO

Standardinställningar:

IP-adress: 192 168 100 100

Användarnamn: SimonsVoss | Lösenord: SimonsVoss

Om låset inte är utrustat med en LockNode (LN.I) från fabrik måste denna installeras i efterhand via lämpligt tillbehör.



INFO

Notera IP-adressen för RouterNode2 och chip-ID för låset efter att du har förberett hårdvaran korrekt.

2.1.4 Skapa kommunikationsnoder

Kommunikationsnoderna utgör gränssnittet mellan CommNode-servern och LSM-Software. För att du ska kunna skapa konfigurations-XML måste du använda LSM-Software som administratör.

1. Öppna LSM-Software.
2. Välj "Nätverk/Kommunikationsnod".

3. Fyll i uppgifterna "Namn", "Datornamn" och "Beskrivning",
↳ *t.ex. WaveNet-nätverk_123; Dator_BS21; Kommunikationsnod för det trådlösa WaveNet-nätverket 123*
4. Klicka på "konfig.filer"
5. Försäkra dig om att sökvägen hänvisar till installationskatalogen för CommNode-servern och klicka på "OK".
6. Kvittera meddelandet med "Nej" och bekräfta med "OK". *De tre konfigurations-XML (appcfg, msgcfg och netcfg) måste ligga direkt i installationskatalogen för CommNode-servern.*
7. Spara inställningarna med "Ta över".
8. Kvittera meddelandet med "OK".
9. Stäng dialogen med "Avsluta".

2.1.5 Konfigurera nätverk och importera till LSM

2.1.5.1 Skapa en WaveNet-konfiguration

Om alla förutsättningar är uppfyllda kan du börja med konfigureringen av nätverket:

- ✓ LSM är korrekt installerad och en nätverksmodul är licensierad.
 - ✓ CommNode-servern har installerats och tjänsten har startats.
 - ✓ Konfigurationsfilerna för CommNode-servern har skapats.
 - ✓ Den senaste versionen av WaveNet-managern har installerats.
 - ✓ En kommunikationsnod har skapats i LSM-Software.
 - ✓ Den första programmeringen av de lås som ska integreras i nätverket har genomförts korrekt.
 - ✓ RouterNode2 kan nås via nätverket och du känner till IP-adressen.
 - ✓ Det programmerade låset har en monterad LockNode, vars chip-ID du känner till.
1. Starta Wavenet-Manager via "Nätverk/WaveNet Manager" och tryck på "Starta".
 2. Ange lösenordet.
 3. Högerklicka på "WaveNet_xx_x".
 4. Initiera först RouterNode2, till exempel via alternativet "Lägg till: IP eller USB Router".
↳ Följ anvisningarna i dialogen och integrera RouterNode2 via dess IP-adress i ditt trådlösa WaveNet-nätverk.
 5. Initiera LockNode för låset genom att högerklicka på den nya RouterNode2 och välja alternativet "Sök efter ChipID".
↳ Följ anvisningarna i dialogen och tilldela låset resp. tillhörande LockNode via dess ChipID till RouterNode2 .

6. Klicka i tur och ordning på knapparna "Spara", "Avsluta" och "Ja" för att stänga WaveNet-Manager.
7. Importera de nya inställningarna och tilldela dem till respektive kommunikationsnod.

2.1.5.2 Överför en WaveNet-konfiguration

De nya inställningarna måste överföras till CommNode-servern:

1. Välj "Nätverk/Kommunikationsnod".
2. Välj RouterNode2 i listan över anslutningar och klicka på knappen "Överför".
3. Spara inställningarna med "Ta över".
4. Stäng dialogen med "Avsluta".

2.1.5.3 Tilldela LockNode till ett lås

Initierad LockNode måste kopplas till ett lås. Detta sker enklast som samlingsuppdrag (särskilt om det finns flera LockNodes):

1. Välj "Nätverk/Samlingsuppdrag/WaveNet-nod".
2. Välj alla LockNodes (*WNNode_xxxx*) som ännu inte tilldelats. *Ännu inte tilldelade LockNodes har ingen post i spalten "Dörr"*.
3. Klicka på "Konfigurera automatiskt".
↳ Autokonfigurationen startar genast.
4. Stäng dialogen med "Avsluta".

2.1.5.4 Testa en WaveNet-konfiguration

För att snabbt kunna testa nätverksuppkopplingen kan du när som helst omprogrammera låset via nätverket "högerklick/programmera". Om programmering sker korrekt arbetar nätverket som det ska.

2.2 Driftsättning av DoorMonitoring-låscylindern

I det här exemplet visas vilka inställningar som ska genomföras vid konfiguration av DoorMonitoring-låscylindern. Förutsättningarna för detta hittar du i kapitel "*Upprätta en trådlöst WaveNet-nätverk och integrera ett lås [▶ 33]*".

2.2.1 Skapa DoorMonitoring-låscylinder

Först måste DM-låscylindern skapas och programmeras korrekt i LSM:

1. Tryck på knappen "Skapa lås" för att öppna dialogen för ett nytt lås.
2. Välj låstypen "G2 Door Monitoring-cylinder" och fyll i övriga uppgifter efter behov.
3. Avsluta dialogen för att skapa låset i matrisen.

4. Öppna låsets egenskaper genom att dubbelklicka på dem och växla till fliken "Konfiguration/Data".
5. Genomför inställningarna i låsets börområde efter behov.
6. Klicka på knappen "Monitoring-konfiguration" och genomför (minst) följande inställningar:
 - ↳ Avkänningsintervall cylinderskruv: t.ex. 5 sekunder. I detta fall kontrolleras dörrstatusen var femte sekund.
 - ↳ Varv på låset: t.ex. 1 varv. Den här inställningen är viktig för att regelns status ska kunna registreras korrekt.
7. Spara inställningarna och gå tillbaka till matrisen.
8. Genomför en första programmering med hjälp av en lämplig programmeringsenhet.

2.2.2 Integrera DoorMonitoring-låscylinder i nätverket

DM-låscylindern integreras i WaveNet-nätverket på följande sätt:

- ✓ WaveNet-Manager har redan konfigurerats.
 - ✓ Den router som det nya låset ska tilldelas är redan konfigurerad och "online".
 - ✓ En LockNode är korrekt monterad på DM-låscylindern och du känner till dess chip-ID.
1. Starta WaveNet-Manager.
 2. Initiera LockNode för låset genom att högerklicka på den nya routern och välja alternativet "Sök efter ChipID".
 - ↳ Följ anvisningarna i dialogen och tilldela låset resp. tillhörande LockNode via dess ChipID till RouterNode2 .
 3. Klicka med höger musknapp på den nya DM-LockNode.
 4. Aktivera kryssrutan "I/O-konfiguration" och klicka på knappen "OK".
 5. Aktivera kryssrutan "Skicka alla händelser till I/O-router" och klicka på knappen "OK".
 6. Klicka i tur och ordning på knapparna "Spara", "Avsluta" och "Ja" för att stänga WaveNet-Manager.
 7. Importera de nya inställningarna och tilldela dem till respektive kommunikationsnod.

2.2.3 Överför en WaveNet-konfiguration

De nya inställningarna måste överföras till CommNode-servern:

1. Välj "Nätverk/Kommunikationsnod".
2. Välj RouterNode2 i listan över anslutningar och klicka på knappen "Överför".
3. Spara inställningarna med "Ta över".
4. Stäng dialogen med "Avsluta".

2.2.4 Tilldela LockNode till ett lås

Initierad LockNode måste kopplas till ett lås. Detta sker enklast som samlingsuppdrag (särskilt om det finns flera LockNodes):

1. Välj "Nätverk/Samlingsuppdrag/WaveNet-nod".
2. Välj alla LockNodes (*WNNode_xxxx*) som ännu inte tilldelats. *Ännu inte tilldelade LockNodes har ingen post i spalten "Dörr"*.
3. Klicka på "Konfigurera automatiskt".
↳ Autokonfigurationen startar genast.
4. Stäng dialogen med "Avsluta".

2.2.5 Aktivera låsets inputhändelser

För att dörrstatusarna ska visas korrekt i LSM-Software måste du genomföra även följande inställningar:

1. Välj "Nätverk/Samlingsuppdrag/WaveNet-nod".
2. Välj DoorMonitoring-cylindern (*eller valfri cylinder som ska vidarebefordra händelser*).
3. Klicka på "Aktivera inputhändelser".
↳ Programmeringen startar genast.
4. Klicka på "Avsluta" när alla lås har programmerats.

2.3 Konfigurera RingCast

Nedan beskrivs konfigurationen av en RingCast. Via RingCast kan en inputhändelse hos en RouterNode2 vidarebefordras parallellt till flera RouterNode2 i samma trådlösa WaveNet-nätverk. I detta exempel ska en nödaktivering av låsen genomföras. När ett brandlarmsystem aktiverar input 1 för en RouterNode2 ska alla tillhörande lås öppnas. Varje lås förblir sedan öppet tills det får ett explicit kommando för en fjärröppning.

Med RingCast kan självklart även andra uppgifter genomföras, till exempel blocklåsfunktion, fjärröppning och amokfunktion.

I detta exempel förutsätts ett konfigurerat trådlöst WaveNet-nätverk med två RouterNode2. Varje RouterNode2 är kopplad till ett lås. Så fort input 1 tillfälligt kopplas till en RouterNode2 ska alla lås omedelbart öppnas. På så sätt kan personer få tillträde till alla rum för att söka skydd mot brand eller rök.



INFO

Om RouterNode2 är nätverksuppkopplad via Ethernet, stöds RingCast först hos modeller som levererats från och med omkring 2017. En RouterNode2 som inte lyckats upprätta en Ethernet-anslutning till en annan

RouterNode2 försöker upprätta den nya anslutningen trådlöst. Räckvidden för den trådlösa kommunikationen är upp till 30 m (ej garanterat, beror på omgivningen).

2.3.1 Förbereda routern för RingCast

Först måste de båda RouterNode2 förkonfigureras:

- ✓ I det trådlösa Wavenet-nätverket har två olika RouterNode2 konfigurerats och är "online".
 - ✓ Varje RouterNode2 har tilldelats ett lås. Båda låsen är "online".
1. Öppna WaveNet-Manager.
 2. Klicka med höger musknapp på den första RouterNode2.
 3. Aktivera kryssrutan "I/O-konfiguration" och klicka på knappen "OK".
 4. Valfritt: Välj till exempel "Input kvittering statisk" för utgång 1 för att kunna styra en signalenhet under avaktiveringen.
 5. Välj ingången "Nödaktivering" för ingång 1.
 6. Som fördröjning väljs alternativet "RingCast".
 7. Kontrollera att alla önskade LockNodes har valts med knappen "Välj LN". (*Vid första inställningen av routerns I/O-konfiguration tas alla LockNodes med.*)
 8. Välj din protokollgeneration och ange låssystemets lösenord.
 9. Avsluta konfigurationen med "OK".
 10. Genom inställningarna även på den andra RouterNode2.

2.3.2 Skapa RingCast

När RouterNode2 har konfigurerats på lämpligt sätt kan RingCast skapas:

1. Klicka med höger musknapp på "WaveNet_xx_x" i Wavenet-Manager.
2. Aktivera kryssrutan "RingCast" och klicka på knappen "OK".
3. Vid "Välj domän" väljer du "Input 1".
 - ↳ I fältet "Valda routrar" visas de båda RouterNode2, för vilka du har ställt in I/O-konfigurationen för RingCast.
4. Markera de båda RouterNode2, för vilka du har ställt in I/O-konfigurationen för RingCast.
5. Klicka på knappen "Spara".
6. Klicka på knappen "Avsluta".
7. Klicka på "Ja" för att uppdatera ändringarna.
 - ↳ RingCast har skapats och syns efter en kort stund i WaveNet-Manager.

De genomförda inställningarna har redan skrivits i RouterNode2. Spara de nya inställningarna och avsluta WaveNet-Manager.

Se även

➔ *Förbereda routern för RingCast* [▶ 39]

2.3.3 Funktionstest

De genomförda inställningarna börjar genast gälla. När input 1 kopplar, avaktiveras låset och utgång 1 kopplar.

Eftersom inputkabeln eller andra delar kan skadas vid en brand, stannar alla låsen upp i läget "Nödöppning". Denna status lämnas inte förrän varje lås får ett kommando gällande fjärröppning.

2.4 Konfigurera eventmanagement (händelser)

Nätverksuppkopplingen av lås via RouterNode2 erbjuder många fördelar. En avgörande fördel är kommunikationen mellan RouterNode2 och lås.

I det här exemplet ska ett fördefinierat e-postmeddelande skickas via LSM-Software så fort en transponder används vid ett specifikt lås under natten.

I detta fall gäller följande förutsättningar:

- Ett trådlöst WaveNet-nätverk har konfigurerats på det sätt som beskrivs i exemplet *Upprätta en trådlöst WaveNet-nätverk och integrera ett lås* [▶ 33].
- Dessutom har vidarebefordringen av händelser aktiverats vid låset enligt steget *Aktivera låsets inputhändelser* [▶ 38].

2.4.1 Konfigurera en e-postserver

I LSM-Software finns en rudimentär e-postklient för försändelse av e-post. För att kunna skicka e-postmeddelanden behöver du ett eget konto som stöder SMTP-formatet.

1. Välj "Nätverk/E-postmeddelanden"
2. Klicka på knappen "E-post".
3. Ange alla SMTP-inställningar för din e-postleverantör.
4. Klicka på knappen "OK".
5. Klicka på knappen "OK".

2.4.2 Ställa in tasktjänst

1. Välj "Nätverk/Taskmanager".
2. Välj din kommunikationsnod under "Tasktjänst".
3. Klicka på knappen "Spara".
4. Klicka på knappen "Avsluta".

2.4.3 Vidarebefordra inpuhändelser via RouterNode2

Så fort händelser (*t.ex. en transponder som aktiveras vid ett nätverksuppkopplat lås*) vidarebefordras via RouterNode2 till CommNode-servern, måste detta aktiveras i routerns I/O-konfiguration.

1. Öppna WaveNet-Manager.
2. Klicka med höger musknapp på routern och välj "I/O-konfiguration".
3. I rullgardinsmenyn ska du vid "Överför händelser till managementsystem" välja "Alla LN-händelser".
4. Tryck på "OK" och avsluta WaveNet-Manager.

2.4.4 Vidarebefordra inpuhändelser via SREL3-ADV-systemet

SREL3-ADV-systemet gör det möjligt att vidarebefordra inpuhändelser till LSM.

2.4.4.1 Utvärdera styrenhetens ingångar

De digitala ingångarna på styrenheten till SREL3-ADV-systemet kan vidarebefordras till LSM och aktivera åtgärder där.

Skapa händelse

Om du vill utvärdera en ingång via LSM eller SmartSurveil (se SmartSurveil) måste du först skapa respektive ingång i LSM som händelse. Först därefter kommer ändringar på ingången att sparas även i LSM-databasen.

- ✓ LSM öppen.
 - ✓ SREL3-ADV-systemet skapat i matrisen.
1. Välj via | Nätverk | posten **Händelsehanterare**.
 - ↳ Fönstret "Hanterare av nätverkshändelser" öppnas.
 2. Klicka på knappen **Nytt**.
 - ↳ Fönstret "Ny händelse" öppnas.

3. Ange ett namn för händelse.
4. Ange en valfri beskrivning av händelsen.
5. Ange ett valfritt meddelande.
6. Öppna rullgardinsmenyn ▼ Typ.
7. Välj posten "Inpuhändelse".

8. Klicka på knappen **Konfigurera händelse** .
↳ Fönstret "Inpuhändelse" öppnas.

Inputhändelse

Inputs till en lock-node ska beaktas på följande sätt:

Välj input

Input 1
 Input 2
 Input 3

Input ändras

från 0 till 1
 från 1 till 0
 båda

OK Avbryt

9. I området "Välj input" väljer du önskad ingång.
 10. I området "Input ändras" väljer du den statusändring som ska lösa ut händelsen.
 11. Klicka på knappen **OK**.
 12. Klicka på knappen **Välj** för att tilldela händelsen ett lås.
 - ↳ Fönstret "Hantering" öppnas.
 13. Markera ett eller flera lås.
 14. Klicka på knappen **Lägg till**.
 15. Klicka på knappen **OK**.
 - ↳ Fönstret stänger.
 - ↳ Låset har tilldelats händelsen.
 16. Om du vill ställa in en åtgärd kan du tilldela en åtgärd med knappen **Nytt** resp. **Lägg till**.
 17. Klicka på knappen **OK**.
 - ↳ Fönstret stänger.
 - ↳ Händelsen visas i området "Händelser".
 18. Klicka på knappen **Avsluta**.
 - ↳ Fönstret stänger.
- ↳ Ingången har skapats som händelse och löser ut en åtgärd beroende på inställning.

2.4.5 Skapa reaktion

Skapa först en reaktion. Denna reaktion kan väljas vid ett senare tillfälle när ett visst scenario inträffar.

1. Välj "Nätverk/Händelsemanager".
2. Klicka på knappen "Nytt" i det högra området under "Reaktioner".

3. Ange ett namn och en beskrivning av reaktionen.
4. Välj typen "E-post".
5. Klicka på "Konfigurera reaktion".
6. Klicka på knappen "Nytt".
7. Ange mottagarens e-postadress samt ett ämne och en meddelandetext. *Med knappen "Testa" kan du genast testa e-postkonfigurationen.*
8. Avsluta dialogen genom att trycka tre gånger på "OK". Tryck på "Avsluta" för att gå tillbaka till matrisen.

2.4.6 Skapa händelse

När du har skapat en reaktion kan du som nästa steg skapa en händelse.

1. Välj "Nätverk/Händelsemanager".
2. Klicka på knappen "Nytt" i det vänstra området under "Händelser".
3. Ange ett namn och en beskrivning av reaktionen.
4. Välj typen "Tillträde".
5. Klicka på "Konfigurera händelse".
6. Kryssa för rutan "Reagera på alla transpondrar". *Händelsen ska utlösas varje gång en enskild transponder aktiveras. Alternativt kan du begränsa händelsen till en enda transponder.*
7. Åtgärden kan anpassas ytterligare i området "Tidsinställning".
8. Klicka på knappen "OK".
9. Klicka på knappen "Välj" i området "Lås".
10. Lägg till alla lås för vilka händelsen ska lösas ut när en transponder aktiveras och bekräfta ditt val med "OK".
11. Klicka på knappen "Lägg till" i området "Tillhörande åtgärder".
12. Lägg till den reaktion som skapats.
13. Klicka på "Konfigurera tid".
14. Ange tiden för nattperioden. Händelsen utförs nu aktivt endast under den tidsperiod som definierats.
15. Avsluta dialogen genom att trycka tre gånger på "OK". Tryck på "Avsluta" för att gå tillbaka till matrisen.

2.5 Hantera virtuellt nätverk (VN)

Via ett virtuellt nätverk (VN-nätverk) kan man snabbt och enkelt ändra och anpassa behörigheter även utan fullständig nätverksuppkoppling. Behörigheten för lås (och spärr-ID för spärrade ID-medier) sparas direkt i ID-mediet och vidarebefordras vid varje aktivering av låset. I virtuella nätverk är det därför viktigt att boka alla ID-medier i en gateway med jämna mellanrum.

I det här exemplet beskrivs konfigurationen av ett virtuellt nätverk.

2.5.1 Konfigurera låssystem

I ett (rent) G2-låssystem ska rutan "Virtuellt nätverk" vara aktiverad. Om denna inställning används i ett befintligt låssystem kan det uppstå omfattande programmeringsbehov.

2.5.2 Konfigurera VN-tjänst

1. Välj "Nätverk/VN-tjänst".
2. Välj VN-servern (t.ex. kommunikationsnoden).
3. Ange installationssökvägen till VN-servern. *För en LSM Business-installation installeras VN-servern i en separat mapp i huvudkatalogen.*
4. Klicka på knappen "Spara".
5. Klicka på knappen "Avsluta".

2.5.3 Skapa komponenter och konfigurera LSM-Software

Innan du börjar med configurationen ska du i LSM-Software genomföra de viktigaste inställningarna för drift av ett nätverk, och RouterNode2 måste vara driftklar.

■ *Förbereda LSM Software [► 33]*

■ *Förbereda hårdvaran [► 34]*

■ *Skapa kommunikationsnoder [► 34]*

■ *Ställa in tasktjänst [► 40]*

1. Skapa de olika komponenterna (t.ex. transponder) och låsen (t.ex. aktiv låscynder).
2. Genomför den första programmeringen av de komponenter som skapats.
3. Skapa ett SmartRelä2 och ge behörighet till alla ID-medier, vilka senare ska få nya behörigheter här.
 - ↳ I låsegenskaperna för SREL2 måste rutan "Gateway" alltid vara aktiverad i fliken!
4. Genomför den första programmeringen av SREL2 och se till att denna har en korrekt ansluten LockNode.
5. Konfigurera RouterNode2 via WaveNet-Manager och tilldela denna till gateway (t.ex. SREL2).
 - ↳ *Se Konfigurera nätverk och importera till LSM [► 35].*

2.5.4 Exportera behörighetsändringar

Exporten av behörighetsändringar fungerar endast när det finns minst en ändring. För att testa detta ska du till exempel återkalla behörigheten från transponder 1 till låscynder 1.

1. Välj "Programmering/Virtuellt nätverk/Export till Vnätverk".

2. Välj alla SREL2 till vilka ändringar ska skickas eller exporteras.
3. Kontrollera att rätt låssystem har valts.
4. Klicka på knappen "Förbered"
 - ↳ I listan "Personer" visas alla ändringar som ska exporteras.
5. Klicka på knappen "Exportera"
 - ↳ Exporten startar. Ändringarna skickas till Gateway.

Behörighetsändringar finns nu på gateway. Nu finns det tre olika scenarier:

- Transponder 1 bokas vid gateway. Lås 1 kommer senare att känna av att transponder 1 inte längre har behörighet och tillträdet nekas.
- En annan transponder (ej transponder 1) bokar först vid gateway och får behörighet till lås 1. Spärr-ID för transponder 1 meddelas låscylinde 1.

Från och med LSM 3.4 SP2 är det möjligt att ange upp till två andra transponder-ID:n som ska spärras för valfria transpondrar.

Programmera de TID som ska spärras direkt

De ID som ska spärras sparas på transpondern under programmeringen.

- ✓ Transpondern är fysiskt tillgänglig.
 - ✓ Transponderns programmeringsfönster är öppet.
1. Klicka på knappen "TIDs för avaktivering".
 - ↳ Listan öppnas.
 2. Markera upp till två alternativ i spalten TID för att spara de TID som ska raderas på transpondern.
 3. Bekräfta uppgifterna med knappen "OK".
 4. Fortsätt med programmeringen.
- ↳ Markerade TID sparas på transpondern som TID som ska raderas. När transpondern används vid ett relevant lås spärras de TID som ska raderas vid låset.

De TID som ska raderas sparas i egenskaperna

De ID som ska spärras sparas på transpondern antingen i samband med nästa programmering eller vid nästa aktivering på en gateway.

- ✓ Transponderns egenskapsfönster är öppet.
1. Växla till fliken "Konfiguration".
 2. Klicka på knappen "TIDs för avaktivering".
 - ↳ Listan öppnas.
 3. Markera upp till två alternativ i spalten TID för att spara de TID som ska raderas på transpondern.
 4. Bekräfta uppgifterna med knappen "OK".
- ↳ Markerade ID sparas på transpondern antingen i samband med nästa programmering eller vid nästa aktivering på en gateway.

2.5.5 Importera behörighetsändringar

När ändringarna har exporterats till gateway kan man i LSM-Software till en början inte se vilka ändringar som redan hämtats från gateway. Detta visas först vid en import.

1. Välj "Programmering/Virtuellt nätverk/Import synkronisering".
↳ Importen startar.
2. Klicka på knappen "Avsluta".

2.5.6 Tips om VN

- För att snabbt fördela ändringar "offline" i låssystemet är det viktigt att alla transpondrar bokas med korta, jämna mellanrum. Här kan man arbeta med tidsbudgetar:

Med alternativet "Dynamiskt tidsfönster" i låssystemets egenskaper kan man påtvinga transpondrar en tidsbudget. På så sätt kommer användaren att vara tvungen att med jämna mellanrum ladda ID-mediet vid gateway. I annat fall spärras ID-mediet för detta låssystem.

- Import och export av ändringar till gateway kan ske automatiskt. Inställningarna kan genomföras direkt i "Nätverk/VN-tjänst".

OBS

Belastning av WaveNet vid import och export

Om många ändringar importeras och exporteras samtidigt belastas WaveNet kraftigt. Det kan störa andra funktioner som också har åtkomst till WaveNet.

2.6 Identifiering av sabotage

Från LSM kan du identifiera sabotageförsök på SmartHandle AX och på SmartRelä 3 Advanced. Om höljet som används där öppnas, identifierar elektroniken detta och skickar informationen till LSM. Om du vill utvärdera informationen kan du skapa en händelse av den och reagera på den (se *Konfigurera eventmanagement (händelser)* [▶ 40]).

2.7 DoorMonitoring (SmartHandle) – händelser med trycket

Från LSM 3.4 SP2 kan du identifiera tryckets status på SmartHandle AX. När trycket är nedtryckt identifierar elektroniken detta och skickar informationen till LSM. Om du vill utvärdera informationen kan du skapa en händelse av den och reagera på den (se *Konfigurera eventmanagement (händelser)* [▶ 40]).

3 Hjälp och ytterligare information

Infomaterial/dokument

Detaljerad information om drift och konfiguration samt andra dokument finns på SimonsVoss webbplats under rubriken Dokument (<https://www.simons-voss.com/se/nerladdningar/dokument.html>).

Programvara och drivrutiner

Programvara och drivrutiner finns på SimonsVoss webbplats under rubriken Programnedladdningar (<https://www.simons-voss.com/se/nerladdningar/nerladdning-av-programvara.html>).

Försäkringar om överensstämmelse

Försäkringar om överensstämmelse för denna produkt finns på SimonsVoss webbplats under rubriken Certifikat (<https://www.simons-voss.com/se/certifikat.html>).

Hotline

Vid tekniska frågor, kontakta SimonsVoss servicehotline på +49 (0) 89 99 228 333 (samtal i det fasta nätet i Tyskland, samtalstaxa beroende på leverantör).

E-post

Vill du hellre skriva ett e-postmeddelande?

support@simons-voss.com

FAQ

Information om och hjälp med SimonsVoss produkter finns på SimonsVoss webbplats under rubriken Vanliga frågor (<https://www.simons-voss.com/se/nerladdningar/support.html>).

SimonsVoss Technologies GmbH
Feringastrasse 4
85774 Unterföhring
Tyskland



Om SimonsVoss

SimonsVoss är teknikledande inom digitala låssystem.

Som pionjär för fjärrstyrd, kabellös låsteknik erbjuder vi systemlösningar med ett brett produktutbud för små och medelstora verksamheter, stora företag samt offentliga inrättningar.

SimonsVoss låssystem förenar intelligenta funktioner, hög kvalitet och prisbelönad design made i Germany. SimonsVoss är innovativ

systemleverantör med fokus på skalbara system, hög säkerhet, tillförlitliga komponenter, effektiv programvara och enkel användning.

Mod till innovation, hållbart tänkande och handlande samt uppskattning av våra medarbetare och samarbetspartner är nyckeln till vår framgång. Företaget med säte i Unterföhring nära München och produktion i Osterfeld (Sachsen-Anhalt) sysselsätter omkring 300 medarbetare i åtta länder.

SimonsVoss är ett företag inom ALLEGION-gruppen – ett globalt verksamt nätverk på området för säkerhet. Allegion representeras i omkring 130 över hela världen (www.allegion.com).

© 2019, SimonsVoss Technologies GmbH, Unterföhring

Med ensamrätt. Texter, bilder och grafiker är upphovsrättsskyddade.

Innehållet i detta dokument får varken kopieras, distribueras eller ändras. För mer information, besök SimonsVoss hemsida. Reservation för tekniska ändringar.

SimonsVoss och MobileKey är registrerade varumärken som tillhör SimonsVoss Technologies GmbH.

