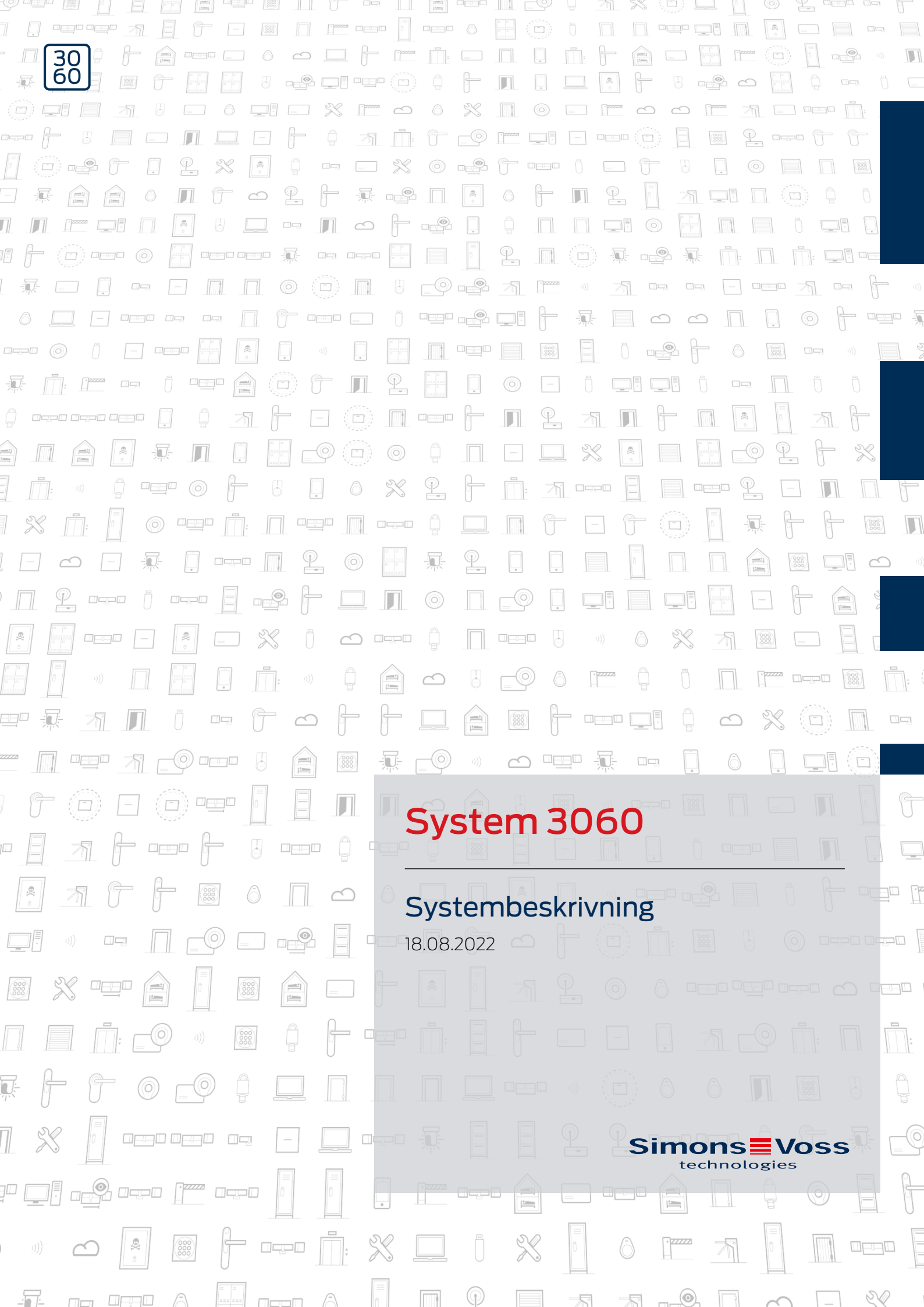




System 3060

Systembeskrivning

18.08.2022

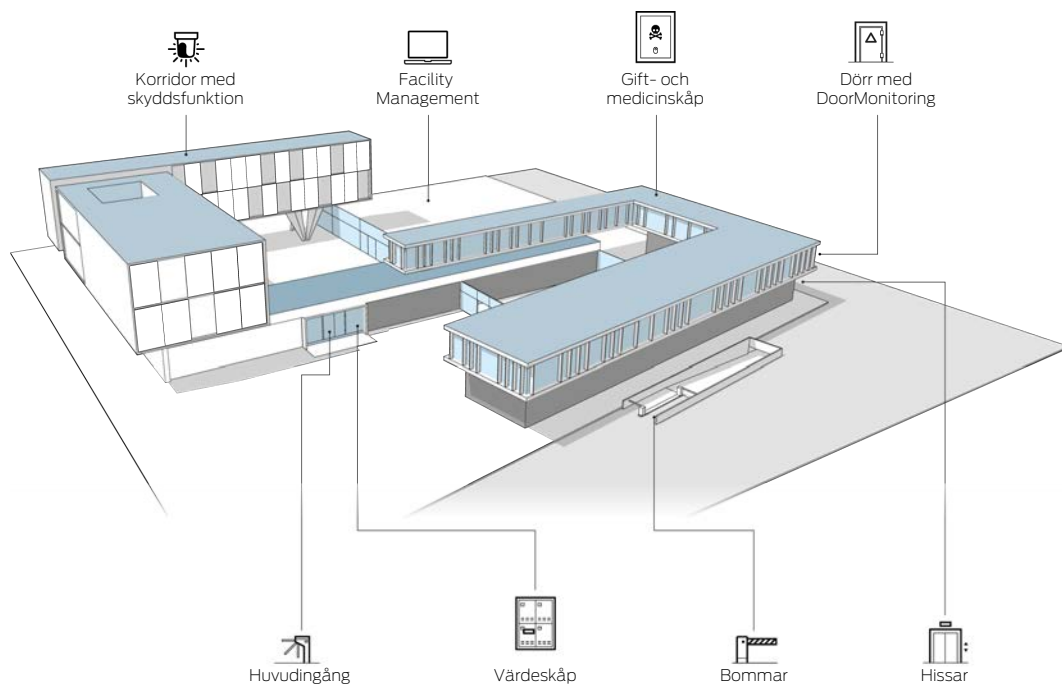
Simons Voss
technologies

Innehållsförteckning

1	Allmänt funktionssätt	3
2	Komponenter	5
2.1	Programvara	5
2.1.1	Locking System Management (LSM)	5
2.1.2	Extra programvara	6
2.1.3	Protokollgeneration	8
2.2	Programmeringsenheter	8
2.2.1	Aktiv	8
2.2.2	Passiv	9
2.3	Lås	9
2.3.1	Låscylinder	10
2.3.2	SmartHandle	11
2.3.3	Smartrelä	12
2.3.4	Hänglås	14
2.3.5	Möbellås	14
2.4	Identifikationsmedier	15
2.4.1	Transponder (aktiv)	15
2.4.2	RFID (passiv)	15
2.4.3	CompactReader (hybrid)	16
2.4.4	Pinkod	17
2.4.5	Blocklås	18
3	Funktioner och utrustning	19
3.1	Tillträdesloggning	19
3.2	Tidzonsstyrning	19
3.3	DoorMonitoring	20
4	Nätverksanslutning	22
4.1	Offline	23
4.2	WaveNet	24
4.2.1	Eventhantering	25
4.3	Virtuell	25
5	Hjälp och ytterligare information	27

1 Allmänt funktionssätt

Det digitala lås- och tillträdeskontrollsystemet 3060 har en modulär uppbyggnad. Det kan användas i enkla låssystem för enskilda dörrar upp till komplexa datorstyrda system för tillträdeskontroll.



Identifikationsmedier

Digitala identifikationsmedier ersätter de vanliga mekaniska nycklarna.

- Transponder
- RFID-medier
- Pinkodsknappsatser

Normalt har varje användare en egen transponder eller eget RFID-medium. Digitala nycklar är i jämförelse med mekaniska nycklar en bättre lösning: De erbjuder fler funktioner och bättre driftsäkerhet. En förlorad digital nyckel kan spärras inom ett par minuter och går då inte längre att använda.

Lås

Dessa identifikationsmedier används för upplåsning och låsning av lås i bland annat:

- Dörrar
- Portar
- Bommar
- Möbler
- Hissar

Flera krypteringsförfaranden i den moderna tekniken skyddar kommunikationen mellan identifikationsmedier och lås. På så sätt kan angrepp utifrån uteslutas tekniskt. Jämfört med mekaniska lås erbjuder de

digitala låsen fördelar: Ett digitalt lås kan till exempel tillfälligt avaktiveras under aktivering av ett larmsystem och kan då under denna tid inte öppnas av någon ("blocklåsfunktion", se [Blocklås \[► 18\]](#)).

Behörigheter

Varje identifikationsmedium programmeras individuellt för ett lås. Varje låssystem innehåller ett låsschema som du använder för att styra identifikationsmediernas behörighet till låsen.

Du kan dela ut behörigheter för varje medarbetare individuellt eller till flera medarbetare samtidigt (till exempel alla medarbetare på en avdelning).

Full kontroll

Med det olika funktionerna i låssystemet har du nu full överblick:

- Vem får öppna vilket lås?
- Vem har öppnat vilket lås?
- När var vilken dörr öppen för länge?
- Vilka dörrar är öppna, vilka är stängda och vilka är låsta?

Framtidssäkerhet

SimonsVoss-låssystem är framtidsäkra. Förändra och utöka systemet helt efter dina personliga behov. Bygg ditt personliga låssystem med komponenterna i 3060-portföljen.

2 Komponenter

2.1 Programvara

2.1.1 Locking System Management (LSM)



Programvaran för låsschemat (Locking System Management, kort LSM) är hjärnan i låssystemet. LSM kan köras på Windows 7 eller senare (beroende på systemets komplexitet kan en Windows-server krävas). Detaljerad information om systemförutsättningarna finns LSM-handboken.på ([SimonsVoss webbplats](#)). Med LSM kan du fritt programmera alla komponenter.

Ett låssystemet kan vara mycket omfattande:

- 64 000 identifikationsmedier
- 64 000 lås

Är det inte tillräckligt? Du kan använda varje transponder i upp till fyra låssystem.

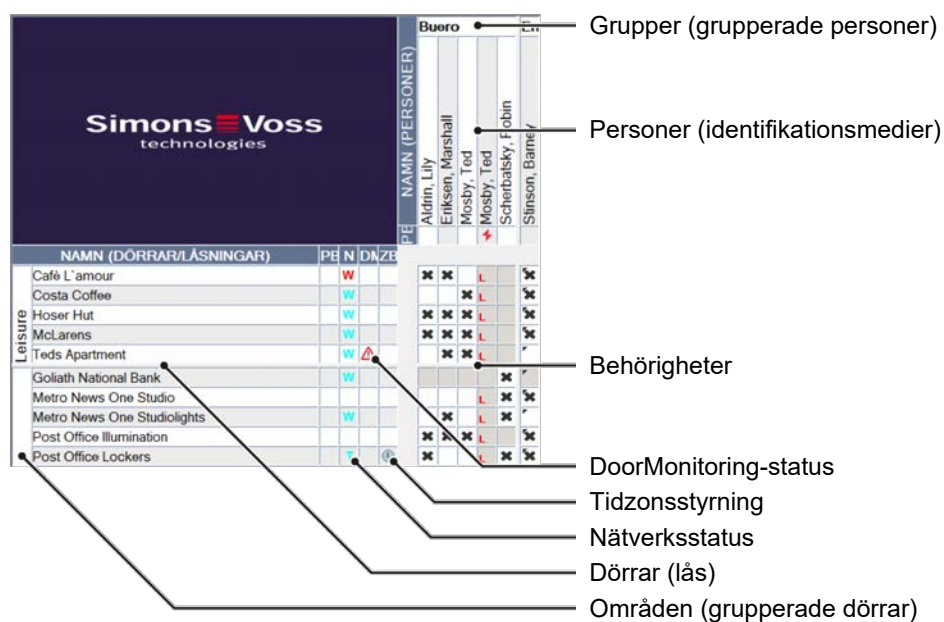
Är fyra låssystem per transponder inte heller tillräckligt? Med överordnade låsnivåer har du möjlighet att använda samma transpondrar i ännu fler låssystem.

Enkel kontroll

Samtidigt är det mycket enkelt att dela och och ändra behörigheter:

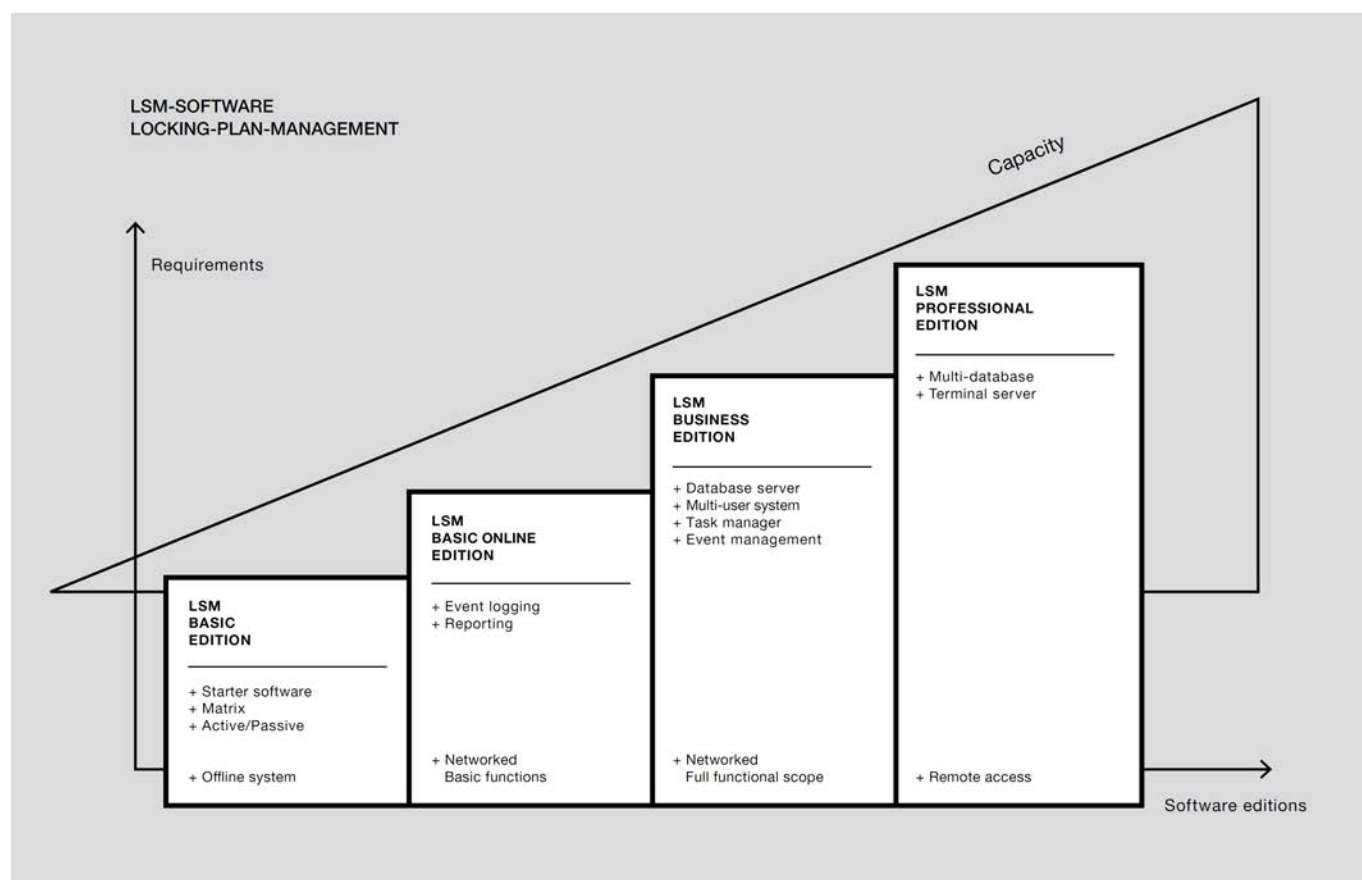
1. Musclick.
2. Programmering.
3. Klart.

Du kan använda områden, grupper och filter för att skapa överblick även i stora låssystem. Visa kolumner eller rader efter behov. I exemplet visas kolumner om nätverksstatus, DoorMonitoring-status och tidszonsstyrning.



Versioner

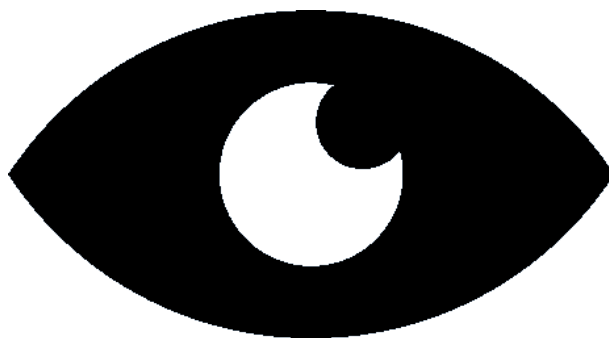
LSM kan fås i olika versioner som bygger på varandra. Den enklaste versionen är LSM Starter som bara har stöd för aktiv teknik (transpondrar).



2.1.2 Extra programvara

SimonsVoss gör livet lättare för dig tack vare smart programvara.

Smart.Surveil



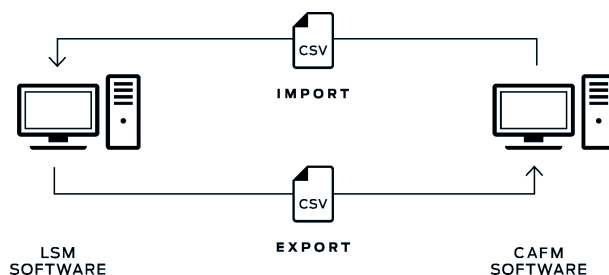
Smart.Surveil är ett övervakningsverktyg som du kan använda för att alltid ha koll på nätverksanslutna dörrar med DoorMonitoring-lås även utan LSM och styra dem på distans (se [DoorMonitoring \[► 20\]](#)).

Exempel

Smart.Surveil lämpar sig för användning i ett övervakningsrum. Tillsammans med ett kamerasystem vet du alltid vad som händer.



Smart.XChange



Smart.XChange är ett gränssnitt för automatiserad dataöverföring mellan LSM och ett externt system (till exempel ett HR-system).

2.1.3 Protokollgeneration

```
01110001 00001100 10101001 01100000 01001101 10110111
00111011 01111100 00111101 01111101 10000011 10100110
11010110 00010111 10011101 00000011 01010001 00000001
00010110 01011111 10111101 10001000 01011110 01100111
```

SimonsVoss-protokollen som reglerar kommunikationen mellan lås och identifikationsmedium är redan i den andra generationen. Jämfört med den första generationen är G2-protokollen:

- **Kraftfullare:** Med G2 kan du administrera många fler lås och identifikationsmedier.
- **Flexiblere:** En stor fördel är valfriheten när det gäller nya behörigheter. Till skillnad från G1 kan du nu spara behörigheten antingen i låset eller på identifikationsmediet. Det sparar mycket tid framför allt i låssystem som omfattar stora ytor.

SimonsVoss lägger stor vikt vid investeringssäkerhet. Därför är det en självklarhet för oss att G1- och G2-komponenter ska kunna blandas så att redan befintliga G1-komponenter kan fortsätta användas.

2.2 Programmeringsenheter

Med programmeringsenheter sparar du behörigheterna från dina låsscheman på identifikationsmedierna och i låsen. Beroende på typ av identifikationsmedier kan du använda olika programmeringsenheter:

- **Aktiv** [► 8]: Transponder
- **Passiv** [► 9]: RFID-identifikationsmedier

Programmeringen sker av princip trådlöst och krypterat. I nätanslutna system kan du även bekvämt programmera ändringar via WaveNet från din arbetsplats.

2.2.1 Aktiv



SmartCD.G2:

SmartCD.G2 kan användas från LSM Basic och högre för programmering av transpondrar och aktiva lås eller hybridlås.

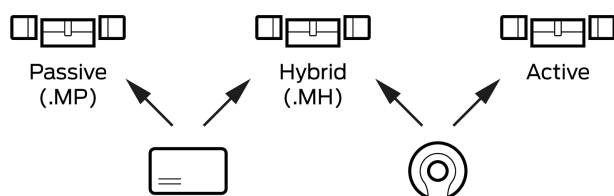
	CD.Starter.G2: CD.Starter.G2 kan endast användas i LSM Starter för programmering av transpondrar och aktiva lås.
---	--

2.2.2 Passiv

	SmartCD.MP: Med SmartCD.MP programmerar du din RFID-identifikationsmedier samt passiva lås eller hybridlås.
	SmartCD.HF: Med SmartCD.HF programmerar du snabbt dina RFID-identifikationsmedier.

2.3 Lås

I System 3060 är ett lås allt som man kan låsa, låsa upp och koppla om med ett identifikationsmedium. I grunden finns det tre typer av lås:



- Aktiva lås (25 kHz): Kan bara aktiveras med aktiva identifikationsmedier, till exempel en transponder.
- Passiva lås (13,56 MHz): Kan bara aktiveras med passiva identifikationsmedier, till exempel ett kort.
- Hybridlås (25 kHz och 13,56 MHz): Kan aktiveras med aktiva och/eller passiva identifikationsmedier.

Det finns många lås med ytterligare utrustningskategorier. I kapitlet *Funktioner och utrustning* [19] beskrivs några av dessa kategorier. Mer information finns i dokumentationen och produktkatalogen. Alla SimonsVoss-lås klarar olika öppningssätt, bland annat:

- Impulsöppning under valfri varaktighet (låset kopplas därefter ur).

- Flipflop-läge (låset öppnas och stängs först när identifikationsmediet hålls upp igen)

2.3.1 Låscylinder



Låscylindern 3061 är klassikern bland SimonsVoss-låsen. Legitimerar dig med ett identifikationsmedium och vrid helt enkelt på knoppen i stället för att använda en mekanisk nyckel.

- Cylinderprofilen är som hos en mekanisk låscylinder: Låscylindern 3061 är mekaniskt fullt kompatibel.
- Batterierna för strömförsörjning är integrerade i knoppen: Det krävs inga omständliga kabeldragningar.

Monteringen är så enkel att den bara tar några få minuter:

1. Demontera den gamla låscylindern.
2. Montera låscylindern 3061.
3. Klart.
4. Låscylinder 3061 finns i en mängd olika varianter, bland annat:

- Permanent inkopplad på insidan
- Halvcylinder
- Friroterande på båda sidor
- Väderbeständig
- VdS-överensstämmande
- Mässingsfärgad
- Med knapp på insidan
- Utförande för paniklås
- Extra greppvänliga knoppar
- ...

Batterilivslängden är mycket lång med fler än 300 000 aktiveringar eller upp till 10 års standby. När batterierna så småningom börjar förlora kapaciteten finns ett batterivarningssystem som i flera steg uppmärksammar dig om detta, i nätanslutna låssystem skickas till och med varningen direkt till LSM.

2.3.2 SmartHandle

SmartHandle 3062



SmartHandle 3062 är den digitala ersättningen för ditt vanliga dörrhandtag. Legitimerar dig med ett identifikationsmedium och tryck på handtaget för att öppna dörren.

Tack vare det breda sortimentet lämpar sig SmartHandle för många monteringssituationer – särskilt utomhus.

Lång batterilivslängd möjliggör underhållsfri drift tills dess att batterivarningssystemet varnar om för låg batterinivå (upp till 150 000 eller upp till tio års standby hos den aktiva varianten).

SmartHandle AX



SmartHandle AX är en vidareutveckling av SmartHandle 3062. Tack vare sin adaptiva design kan de moteras på befintliga rosetter enligt DIN 18251 utan någon borrar. Här drar även det visuella samspelet med metallelement ögonen till sig.

SmartHandle AX är dessutom intelligent och förberett för framtiden med funktioner som BLE* och Phone2Door* (preliminärt tillgängligt från 2021).

Även här erbjuder det breda sortimentet lösningar för ett stort antal monteringssituationer.

SmartHandle AX har en enastående batterilivslängd (upp till 300 000 aktiveringar eller upp till tio års standby hos den aktiva varianten). Även här finns ett integrerat batterivarningssystem.

2.3.3 Smartrelä

SmartRelä-enheterna från SimonsVoss är elektroniska omkopplare som kan aktiveras med identifikationsmedier eller via nätverket.

Du tilldelar enkelt behörigheterna för identifikationsmedierna som för varje lås via LSM.

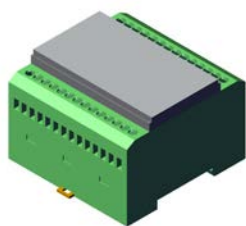


SmartRelä:

Det här SmartReläet är så litet att det får plats i en infälld väggdosa. Trots detta kan det enkelt administreras via LSM.

	SmartRelä 2: Höljet till SmartRelä 2 är elegant, kompakt och som tillval vattenbeständigt. Det kan även läsa av passiva identifikationsmedier.
	SmartRelä 3: SmartRelä 3 höjer kapacitetsribban. Tack vare det PoE-kompatibel Ethernet-gränssnittet kan även stora datamängder snabbt överföras och man slipper tröga nätkomponenter.

Om du behöver ett stort antal utgångar kan du ansluta så kallade SmartOutput-moduler till ett SmartRelä eller ett SmartRelä 3. Du kan ansluta upp till 15 moduler och erhåller på så sätt upp till 115 utgångar som kan styras individuellt.



2.3.4 Hänglås



SimonsVoss-hänglåset kan användas som en låscylinder 3061. Därmed kan du exempelvis skydda källarvåningar eller trädgårdsbyggnader utan att behöva hålla reda på mekaniska nycklar.

Det finns som manuell eller självlåsande variant och med olika bygeldiametrar. En säkerhetskedja förhindrar att det faller ner eller blir stulet.

Batterilivslängden är mycket lång med fler än 300 000 aktiveringar eller upp till 10 års standby. När batterierna så småningom börjar förlora kapaciteten finns ett batterivarningssystem som i flera steg uppmärksammar dig om detta, i nätanslutna låssystem skickas till och med varningen direkt till LSM.

2.3.5 Möbellås

Administrera även dina möbler i System 3060 med möbellås.

Programmera behörigheterna som vanligt, öppna med transpondrar och notera om så önskas vem som har öppnat vad och när.



Skjutstångslås:

Skjutstångslåset lämpar sig för svängdörrar med ett eller flera dörrblad.

	Skåplås: Skjutstångslåset lämpar sig för skåp och lådor.
---	---

2.4 Identifikationsmedier

I System 3060 är ett identifikationsmedium allt som kan låsa upp, låsa eller koppla om ett lås.

2.4.1 Transponder (aktiv)



Transponder 3064 är den mest kända SimonsVoss-produkten och den administreras också i LSM. Den låser upp och låser alla aktiva lås eller hybridlås beröringsfritt. Den ersätter inte bara mekaniska nycklar utan övertar även funktionen som ID-kort.

Som standard levereras transpondrar med blå knapp. På begäran kan du även få dem med brun eller röd knapp och dessutom göra dem RFID-kompatibla.

2.4.2 RFID (passiv)

	SmartCard: I System 3060 går det även att använda SmartCards av typen MIFARE® Classic, MIFARE Plus® och MIFARE® DESFire®. Detta är särskilt praktiskt när ett företag redan använder kort, till exempel som personal-ID eller för tidsregistrering.
	SmartTag: Vill du heller ha SmartTags i stället för SmartCards? I System 3060 går det även att använda SmartTags av typen MIFARE® Classic, MIFARE Plus® och MIFARE® DESFire®.

2.4.3 CompactReader (hybrid)

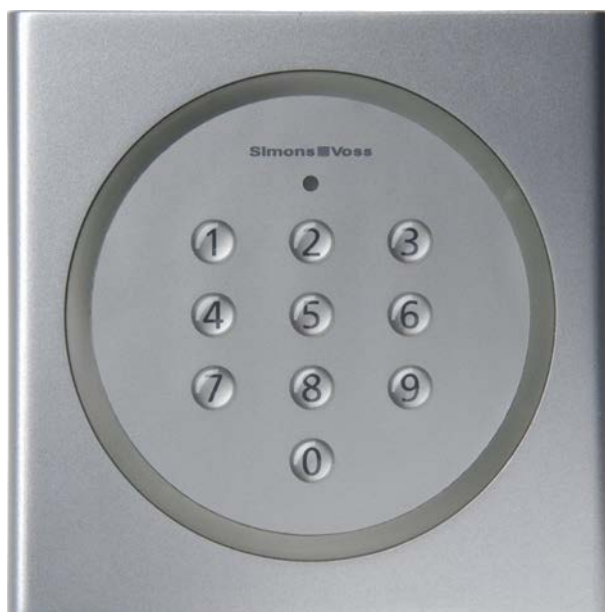


Med CompactReader skapar du i en handvändning hybridlås av dina aktiva lås som även kan läsa av passiva RFID-identifikationsmedier, till exempel ett kort. CompactReader får en fast koppling till låset vid programmering. Enheten läser av kortet och skickar informationen vidare till låset.

Monteringen sker utan kablar och bara två skruvar behövs. Alternativt limmar du helt enkelt fast CompactReader-enheten.

Därefter behöver du inte ägna den en tanke i upp till 80 000 aktiveringar eller upp till 6 års standby. CompactReader varnar dig i god tid när batterierna börjar bli svaga.

2.4.4 Pinkod



I System 3060 erbjuder SimonsVoss två produkter när man kan ange PIN-koder:

- *Pinkodsknappsats*
- *Pinkodsterminal*

Den avgörande skillnaden är att pinkodsterminalen utöver PIN-koden efterfrågar ytterligare ett identifiering (tvåfaktorautentisering).

Efter programmering och enkel montering (limma eller skruva) är båda produkterna underhållsfria tills du får en varning om att batterierna börjar bli svaga (efter upp till 100 000 aktiveringar eller upp till 10 års standby).

Pinkodsknappsats

Med en master-PIN som du väljer själv kan du skapa upp till tre användar-PIN-koder. Dessa användar-PIN-koder kan du ge behörighet till ett lås oberoende av varandra via LSM. När korrekt PIN-kod har angetts öppnas låset i fråga.

Användning av en pinkodsknappsats lämpar sig framför allt när det är opraktiskt med fysiska identifikationsmedier, till exempel vid en konferens.

Pinkodsterminal

Beroende på drifttyp behöver pinkodsterminalen följande:

- Inmatning av en fritt valbar användar-PIN-kod och transponder-ID
- Användning av identifikationsmedium och inmatning av en fritt valbar användar-PIN
- Användning av identifikationsmedium och inmatning av en fast användar-PIN

Pinkodsterminalens drifttyp anges via LSM. En enskild pinkodsterminal har stöd för upp till 500 användar-PIN-koder.

Tvåfaktorautentiseringen förhöjer säkerheten i systemet. En potentiell tjuv måste då inte bara lägga beslag på transpondern utan även ta reda på den tillhörande användar-PIN-koden.

2.4.5 Blocklås



Blocklåset är praktiskt när du använder ett larmsystem. Blocklåset finns även som VdS-utförande.

Aktivera larmsystemet från en central punkt. I detta ögonblick avaktiverar blocklåset alla övervakade dörrar och spärrar dem därmed även för behöriga identifikationsmedier. På så sätt förhindras irriterande och dyra fellarm.

Efter övervakningstidsperioden avaktiverar du larmsystemet igen från den centrala punkten och aktiverar då samtidigt de övervakade dörrarna.

3 Funktioner och utrustning

3.1 Tillträdesloggning

Lås med tillträdesloggning (.ZK) loggar tillträdesförsök med behöriga och eventuellt obehöriga identifikationsmedier.

Du kan läsa av tillträdeslistan och visa den i LSM. Det finns flera olika avläsningsmöjligheter:

- Avläsning med en programmeringsenhet
- Avläsning via WaveNet (nätanslutna lås)
- Avläsning via nätverksanslutningen (SmartRelä 3)

Antalet tillträden som kan sparas beror på det konkreta låset. För varje tillträde eller tillträdesförsök sparas följande:

- Datum
- Tid
- Transponder-ID

LSM jämför avläsningen med den interna tillträdeslistan och övertar endast nya poster till den interna tillträdeslistan. I LSM kan 10 000 tillträden sparas per lås.



INFO

Tillträdesloggning och tidszonsstyrning kan inte kompletteras i efterhand

Utrustningskategori .ZK kan inte kompletteras i efterhand.

- Beställ .ZK-lås om du behöver tillträdesloggning och/eller tidszonsstyrning.

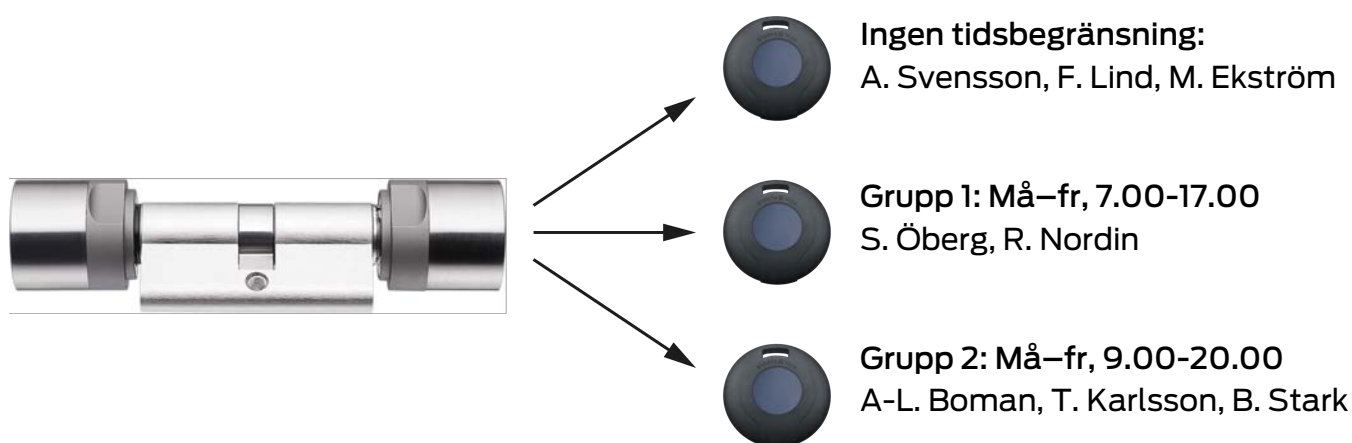
3.2 Tidzonsstyrning

Tidszonskompatibla lås kan inte bara styras via matrisen utan dessutom via datum och tid.

- Koppla in och/eller ur automatiskt vid ett bestämt klockslag
- Grupper av transpondrar är bara behöriga under bestämda tider.

Totalt har du tillgång till 100 tidsgrupper som du kan använda för att reglera transpondrars behörigheter tidsmässigt.

En möjlig tillämpning vore till exempel tidsmässigt begränsade behörigheter för olika användargrupper till ett och samma lås. Vissa behörigheter kan alltid öppna låset, vissa bara mellan 7.00 och 17.00 och vissa bara mellan 9.00 och 20.00.



Självklart kan man även ta hänsyn till söndagar och helgdagar.



INFO

Tillträdesloggning och tidszonsstyrning kan inte kompletteras i efterhand

Utrustningskategori .ZK kan inte kompletteras i efterhand.

- Beställ .ZK-lås om du behöver tillträdesloggning och/eller tidszonsstyrning.

3.3 DoorMonitoring

DoorMonitoring är en elektronisk vaktare i miniatyrformat. I kombination med genomtåkt integrerade sensorer kan låset exempelvis registrera följande status:

- Dörr är öppen.
- Dörr är stängd.
- Dörr är låst.
- Dörr är säkert (dubbelt) låst
- Handtag nedtryckt/inte nedtryckt (SmartHandle, SmartHandle AX)
- Lock borttaget/inte borttaget (SmartHandle AX, SmartRelä 3)

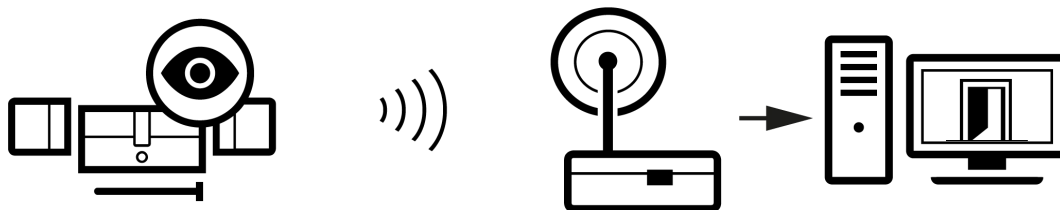
Med SmartRelä 3 kan du övervaka tre ingångar som DoorMonitoring-händelse.

DoorMonitoring kräver varken kablar eller borring.

Med LSM och nätanslutna lås kan du reagera omedelbart på olika dörrstatusar och till exempel få information om när en dörr öppen för länge (se [Eventhantering \[► 25\]](#)). Dessutom kan du använda Smart.Surveil (se [Extra programvara \[► 6\]](#)). Här får du överblick över status hos alla dörrar. Du kan välja att visa den som en lista eller som byggnadsritning.

Exempel

Efter undervisningen ska alla dörrar stängas. De nätanslutna låsen registrerar att en dörr står öppen. De skickar informationen via WaveNet till LSM-databasen. Därifrån visas informationen för dig i LSM eller Smart.Surveil.



4 Nätverksanslutning

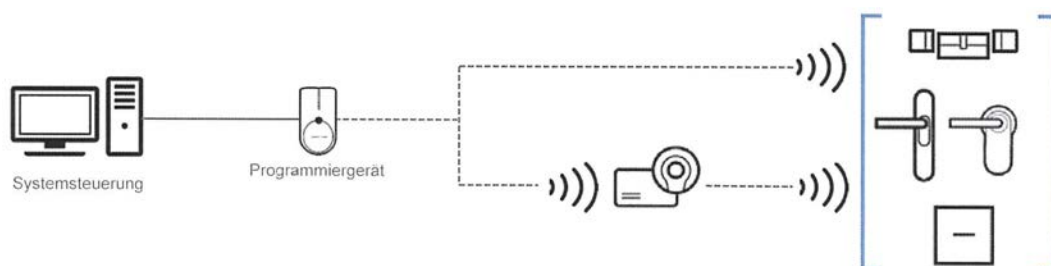
Nätanslutna lås innebär mindre arbete och fler funktioner. Du kan välja mellan: två nätanslutningskoncept som du självklart även kan kombinera.

	WaveNet (online)	Virtuell nätverksanslutning (virtuell)	Offline (ingen nätanslutning)
Funktionsprincip	Överföring av data med nätanslutna WaveNet-enheter. (Se WaveNet [► 24])	Överföring av data med identifikationsmedier (utom programmeringsdata). (Se Virtuell [► 25])	Överföring av data med identifikationsmedier (utom programmeringsdata). (Se Offline [► 23])
Utbredning	WaveNet-enheter är anslutna genom olika överföringsmedier. Alla typer av data överförs med hjälp av dessa överföringsmedier.	I det virtuella nätverket överförs bestämda data till identifikationsmedierna med hjälp av en gateway (poster till svarta listan). När dessa identifikationsmedier används med ett virtuellt anslutet lås överförs sparade data till låset.	Lås som inte är nätverksanslutna kan bara utbyta data med hjälp av programmeringsenheten. Du måste gå med programmeringsenheten till respektive lås.
Programmeringsinsats	Liten.	Liten.	Insatsen beror på låssystemets storlek. ■ Litet låssystem: Liten insats. ■ Medelstort låssystem: Medelstor insats. ■ Stort låssystem: Stor insats.
Överföringshastighet vid datautbyte	Omedelbar. Datautbyte med olika överföringsmedier.	Hastigheten mellan gateway och lås är starkt beroende av hur intensivt låsen används. Identifikationsmedier är överföringsmedier – utan identifikation ingen överföring.	Långsam.

	WaveNet (online)	Virtuell nätverksanslutning (virtuell)	Offline (ingen nätanslutning)
Central aktivering/avaktivering av lås	Möjlig.	Inte möjlig.	Inte möjlig.
Aktivering/avaktivering kan spåras centralt	Möjlig.	Inte möjlig.	Inte möjlig.
Fjärröppning	Möjlig.	Inte möjlig.	Inte möjlig.
Fjärrövervakning (DoorMonitoring, se DoorMonitoring [► 20])	Möjlig.	Inte möjlig.	Inte möjlig.
Eventhantering	Möjlig.	Inte möjlig.	Inte möjlig.
Central visning av passerlistor	Möjlig.	Inte möjlig (utom SREL 3).	Inte möjlig.
Program-/serveroberoende skyddsfunktion	Möjlig.	Inte möjlig.	Inte möjlig.
Omedelbar reaktion i hela låssystemet i kritiska situationer (tillgänglighet hos skyddsfunktioner).	Möjlig.	Inte möjlig.	Inte möjlig.

4.1 Offline

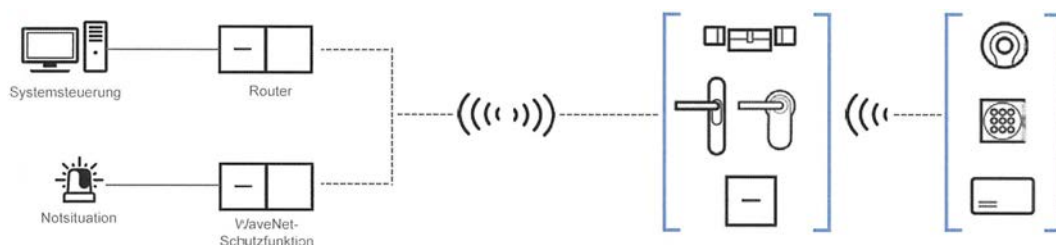
Drift utan nätanslutning lämpar sig framför allt i små system. Du kan programmera allt med programmeringsenheten, det vill säga antingen identifikationsmediet eller låset.



För att läsa av informationen i låsen måste du gå till respektive dörr och läsa av med programmeringsenheten.

Arbetsinsatsen för denna drifttyp ökar avsevärt i takt med att låssystemet byggs ut. Här lämpar sig nätansluten eller virtuellt nätansluten drift.

4.2 WaveNet



Vid direkt nätanslutning skapar du ett trådlöst 868 Mhz-nätverk med basstationer ("RouterNodes") och nätverkskort ("LockNodes") som är integrerade i låsen. Låsen och programvaran kan kommunicera med varandra via RouterNode-enheterna.

- Programmering
- Fjärröppning
- Meddelanden om händelser

Jämfört med icke nätverksanslutna system är bekvämlighetsvinsten avsevärd: Det mesta kan bekvämt utföras från arbetsplatsen.

WaveNet konfigureras automatiskt och behöver inte anslutas med kablar vid dörren.

Extrafunktioner

Tillvalsskyddsfunktionerna till WaveNet ökar säkerheten i hela systemet.

Dessutom står många fler intressanta funktioner och inställningsmöjligheter till förfogande:

- Aktivering och avaktivering av lås
- Fjärröppning av lås
- Nödaktivering av lås
- Skottlarmsfunktion

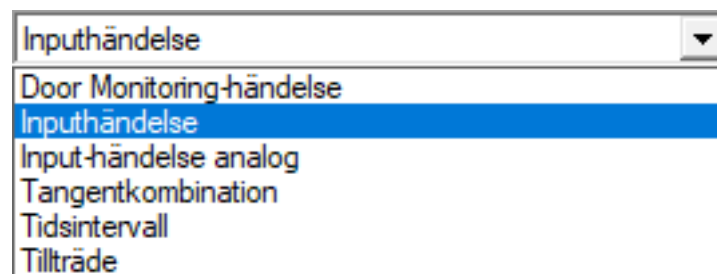
Detaljerad information finns i WaveNet-handboken.

4.2.1 Eventhantering

System 3060 kan även arbeta utan din inblandning och utföra olika uppgifter. Dess uppgifter kan startas på två sätt:

- Tidsstyrt
 - En gång: Starta på ett bestämt datum
 - Regelbundet: Startar med bestämda tidsintervall
- Händelsestyrt: En konfigurerbar händelse (till exempel en dörr som står öppen för länge) utlöser ett valfritt antal konfigurerbara uppgifter.

Välj från ett stort antal händelser som ska utlösa en uppgift.



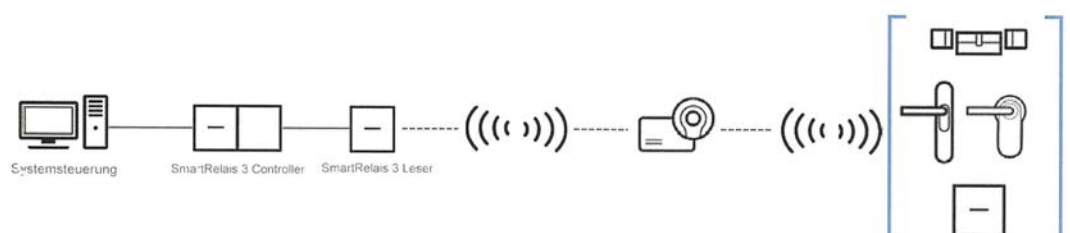
Exempel

En person med en obehörig transponder försöker komma in i skolbyggnaden. Låset registrerar det obehöriga tillträdesförsöket och skickar information via nätverket. Via händelsehanteringen aktiveras ett anslutet SmartRelä som i sin tur aktiverar en kamera.

4.3 Virtuell

En direkt anslutning ("WaveNet") kräver ett nätverkskort ("LockNode") i varje anslutet lås och tillräckligt många basstationer ("RouterNode"), så att alla LockNodes går att nå.

Som alternativ kan ett virtuellt nätverk användas. Det virtuella nätverket använder inte trådlös dataöverföring utan utnyttjar det faktum att användare med programmerbara identifikationsmedier rör sig inom låssystemet. På några centrala platser ("gateways") skrivs informationen till identifikationsmedierna och överförs till alla lås av användarna under dagens lopp. Samtidigt överför användarna även data från låsen till gateway-enheterna med sina identifikationsmedier.



Dessa gateways är de enda komponenter som har en direkt anslutning till LSM-databasen och de är alltid uppdaterade med den senaste informationen. De fungerar i princip som en förenklad, extern programmeringsenhet.

När ett identifikationsmedium hålls upp kontrollerar gateway-enheten följande.

- Det finns data i databasen som behöver transporteras till låsen (till exempel "spärr transponder 1")
- Det finns data från låset i identifikationsmediet som ska skrivas till databasen (till exempel "transponder 1 är spärrad").

Du kan även skapa en reserv av transpondrar. Programmera några transpondrar och lägg dem i en låda. När någon ska tilldelas en transponder räcker det att dela ut någon av dessa transpondrar. Gateway-enheten registrerar transpondern och programmerar de behörigheterna tilldelade i LSM till den.

5 Hjälp och ytterligare information

Infomaterial/dokument

Detaljerad information om drift och konfiguration samt andra dokument finns på webbplats:

<https://www.simons-voss.com/se/dokument.html>

Försäkringar om överensstämmelse

Förklaringar om överensstämmelse och andra certifikat för denna produkt finns på webbplats:

<https://www.simons-voss.com/se/certifikat.html>

Teknisk support

Vår tekniska support hjälper dig gärna (fast telefon, kostnaden beror på leverantör):

+49 (0) 89 / 99 228 333

Vill du hellre skriva ett e-postmeddelande?

support-simonsvoss@allegion.com

FAQ

Information och hjälp finns på rubriken Vanliga frågor:

<https://faq.simons-voss.com/otrs/public.pl>

Adress

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterföhring
Tyskland



Om SimonsVoss

SimonsVoss, pionjären inom fjärrstyrd, kabellös låsteknik, erbjuder systemlösningar med ett brett produktutbud för områdena SOHO, små och stora företag samt offentliga inrättningar. Låssystemen från SimonsVoss kombinerar intelligent funktionalitet, hög kvalitet och prisbelönt tysk design Made in Germany.

SimonsVoss är en innovativ systemleverantör som sätter värde på skalbara system, hög säkerhet, tillförlitliga komponenter, effektiv programvara och enkel användning.

SimonsVoss är teknikledande inom digitala låssystem och vår fokus på innovation, hållbart tänkande och handlande samt uppskattning av våra medarbetare och samarbetspartner är nyckeln till vår framgång.

SimonsVoss är ett företag i ALLEGION Group – ett globalt nätverk inom området säkerhet. Allegion är representerat i cirka 130 länder runt om i världen (www.allegion.com).

Tysk Kvalitet

För SimonsVoss är „Made in Germany“ inte en slogan utan en garanti. Alla våra produkter och system utvecklas och tillverkas i vårt eget produktionscenter i Osterfeld, Tyskland.

© 2022, 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.

SimonsVoss
technologies

Made in Germany

A BRAND OF

