G2 protokoll

Handbok

29.08.2020

SimonsVoss technologies

Innehållsförteckning

1 Allmänna säkerhetsanvisningar

Signalord (ANSI Z535.6)	Eventuella omedelbara effekter av bristande efterlevnad
FARA	Död eller allvarlig personskada (troligt)
VARNING	Död eller allvarlig skada (möjligt, men osannolikt)
OBSERVERA	Liten skada
OBS	Skador på egendom eller fel
INFO	Låg eller ingen

VARNING

Tillgång spärrad

Felaktigt installerade och/eller programmerade komponenter kan leda till att dörrar spärras. SimonsVoss Technologies GmbH ansvarar inte för konsekvenserna av felaktig installation såsom spärrat tillträde till skadade personer eller personer i risksituationer, materiella skador eller andra typer av skador.

Blockerad åtkomst genom manipulering av produkten

Om du ändrar produkten på egen hand kan fel uppstå och åtkomst via en dörr kan blockeras.

- Ändra endast produkten vid behov och endast på det sätt som beskrivs i dokumentationen.

INFO

Avsedd användning

SimonsVoss-produkter är uteslutande avsedda för öppning och stängning av dörrar och liknande.

- Använd inte SimonsVoss-produkter för andra syften.

Avvikande tider vid G2-lås

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

Kvalifikationer krävs

Installation och idrifttagning kräver specialiserad kunskap.

- Endast utbildad personal får installera och driftsätta produkten.

Den tyska språkversionen är den ursprungliga bruksanvisningen. Andra språk (utarbetande på kontraktsspråket) är översättningar av originalinstruktionerna.

Läs och följ alla installations-, installations- och driftsinstruktioner. Skicka dessa instruktioner och alla underhållsinstruktioner till användaren.

2 Allmänt

G2-protokoll är en helt ny typ av SimonsVoss-kommunikation mellan identifikationsmedier och lås. Många nya funktioner har implementerats för att administrationen av låssystemet ska bli ännu enklare och erbjuda fler möjligheter.

Du kan välja produkter och en fullständigt modulär programvara baserat på G2-protokollen och anpassa låssystemet så att det passar dina personliga behov ännu bättre.

3 G2-protokoll

3.1 Allmän beskrivning

G2-protokollen möjliggör nya funktioner i System 3060 om följande villkor är uppfyllda:

- LSM-version 3.0 eller senare
- G2-produkter

3.1.1 Låssystemets lösenord

Du behöver lösenordet till låssystemet enbart när du skapar låsplanen. Dessutom är säkerheten hos låssystemets lösenord förhöjd:

- Minsta längd 64 bitar
- Integrerat kvalitetsindex i LSM-programmet

LSM-programmet tillåter alltså inte längre osäkra lösenord vilket ger högre säkerhet i låssystemet.

3.1.2 Låssystemets storlek

G2-protokollen definierar nya gränser i låssystemet. Nu kan

- upp till 64 000 lås per låssystem
- upp till 64 000 identifikationsmedier per lås

administreras. Med över fyra miljarder möjliga enskilda behörigheter per låssystem har du alla möjligheter till en kompromisslös anpassning av låssystemet utifrån dina individuella behov.

3.1.3 Övergripande låsnivåer

Du kan ha övergripande låsnivåer för att använda bestämda funktioner i flera låssystem. Dessa funktioner säkras med ett eget lösenord som är oberoende av låssystemet (så kallade tvärlåssystem). Tre överordnande låsnivåer står till förfogande:

- Röd låsnivå
- Grön låsnivå
- Blå låsnivå

En transponder kan höra till någon av de tre nivåerna. I LSM finns 1 024 transponder-ID:n reserverade för varje överordnad låsnivå. Det innebär att du kan tilldela maximalt 1 024 transpondrar till en och samma låsnivå. Du kan tilldela individuella behörigheter till var och en av dessa transpondrar eller spärra dem individuellt.

Transponders som du har tilldelat den röda låsnivån kan också öppna inaktiverade lås. Dessa förblir aktiverade eller öppna under den inställda pulslängden, men är fortfarande inaktiverade. Om du exempelvis sparar en transponder i röd låsnivå i en brandkårsnyckeldepå kan räddningspersonal snabbt ta sig fram i byggnaden i ett nödläge.

3.1.4 Nödaktivering

Om låssystemet är trådlöst anslutet kan du aktivera lås via nätverket (WaveNet). Du skickar då ett kommando från LSM-programmet via nätverket till önskade lås som varaktigt låser upp dessa lås. Alla kan då passera oavsett identifikationsmedium.

De lås som du har öppnat med kommandot för nödaktivering är öppna tills du upphäver nödaktiveringen genom att skicka ett kommando för nödöppning eller fjärröppning.

Ett brandlarmsystem kan utlösa en händelse via en kontakt i LSM-programmet som skickar detta kommando. I händelse av brand öppnas då alla lås som tar emot detta kommando. Instängda personer kan lämna byggnaden och räddningspersonal snabbt ta sig in.

Behöriga identifikationsmedier som används med nödaktiverade lås har ingen funktion.

3.1.5 Nödöppning

Du kan dela ut ett tillfälligt lösenord i LSM-programmet under export till LSM Mobile. Det här lösenordet måste innehålla minst åtta tecken, men har inga ytterligare begränsningar.

Med det här lösenordet kan man nödöppna ett lås på plats utan att behöva känna till lösenordet till låssystemet.

Av säkerhetsskäl kan du som administratör begränsa den här funktionen:

- Antal möjliga nödöppningar
- Tidsrymd under vilken nödöppningar är möjliga

3.1.6 Pulslängd

Du kan välja inkopplingstider på mellan 1 och 25 sekunder för låscylindrar och smartreläer.

Samtidigt kan du ge enskilda identifikationsmedier längre inkopplingstid med LSM-funktionen för lång öppning. Den här funktionen fördubblar inkopplingstiden, men den totala inkopplingstiden är fortfarande begränsad till 25 sekunder.

Påverka inkopplingstider för alla lås	Pulslängden i låsets konfiguration

Påverka inkopplingstider för enskilda identifikationsmedier	Lång öppning i identifikationsmediets konfiguration

3.1.7 Akustisk öppningssignal

Lås sänder ut en akustisk öppningssignal. Den här akustiska öppningssignalen kan vara störande, till exempel i ett sjukhus. Dörrar med en akustisk öppningssignal som öppnas nattetid skulle väcka patienterna.

Du kan avaktivera den här signalen för identifikationsmedierna. Du väljer om du vill avaktivera den för enskilda eller alla identifikationsmedier.

3.2 Behörighetstilldelning

3.2.1 Allmänt

De nya G2-protokollen minskar administrationen när nya identifikationsmedier har delats ut. Tack vare intelligenta mekanismer i protokollen kan den hittills nödvändiga omprogrammeringen av lås i stor utsträckning undvikas.

Som ett alternativ till omprogrammering av låsen på plats kan du överföra behörigheterna till låsen på följande sätt:

- G2 utan nätverksanslutning
  - Direkt överföring: Via identifikationsmedier och lås
  - Spärrningar: Via ersättningsidentifikationsmedier
- Indirekt överföring: G2 med virtuell nätverksanslutning (VN), se *Virtuellt nätverk (VN) [▸ 9]*
- Nätverksöverföring: WaveNet

3.2.2 G2 utan nätverksanslutning

Om du använder ett G2-låssystem utan nätverksanslutning kan du spara mycket tid när du konfigurerar nya lås eller identifikationsmedier. Med G2-protokollen behöver du i detta fall inte längre programmera identifikationsmedier och lås:

Nytt lås	■ Spara behörigheterna på identifikationsmediet (programmering av identifikationsmediet) eller ■ Spara behörigheterna i låset (programmering av låset)
Nytt identifikationsmedium	

Du behöver inte göra någon ytterligare programmering i låssystemet. Som administratör av låssystemet har du ett fullständigt öppet system till förfogande. Vid programmeringen kan du bestämma om du vill spara behörigheterna på identifikationsmediet eller i låset, beroende på vad som är mest bekvämt.

Lås

Du kan administrera upp till 64 000 identifikationsmedier till varje lås, dvs. ge dem individuella behörigheter eller spärra dem.
Programmeringsförloppet är in princip identiskt med förloppet för G1-lås. I varje G2-låssystem kan du spara och administrera upp till 64 000 lås.

Identifikationsmedier

I G2-låssystemen kan du spara information individuellt på varje identifikationsmedium om vilka lås det ska ha behörighet till. De nya G2-transpondrarna kan spara och administrera upp till tre G1-låssystem och fyra G2-låssystemet. Därmed kan hela låsplanen sparas på transpondern i G2-låssystem.

Ersättningstranspondrar och spärr-ID:n

Från och med LSM 3.0 SP2 kan du direkt spärra andra identifikationsmedier (som exempelvis har blivit stulna) med ersättningsidentifikationsmedier. När du programmerar ersättningsidentifikationsmediet väljer du det identifikationsmedium som ska spärras och överför ett spärr-ID. När ersättningsidentifikationsmediet används med ett lås överförs spärr-ID:t till låset och det spärrade identifikationsmediet kan alltså inte längre användas med låset.

Programmeringsbehovet i låsen kvarstår och upphävs inte förrän du efterprogrammerar de lås där det identifikationsmedium som skulle spärras hade behörighet.

3.3 Virtuellt nätverk (VN)

I ett virtuellt nätverk programmeras låsen första gången bara med grundläggande information och godkänns i låssystemet. Behörigheterna sparas uteslutande på identifikationsmedierna.

När behörigheterna ändras måste de uppdateras på identifikationsmedierna. I virtuella nätverk finns det så kallade gateways för detta. Användarna använder identifikationsmedierna med dessa gateways och påbörjar på så sätt dataöverföringen. När det föreligger behörighetsförändringar uppdaterar gateway-resursen behörigheterna på identifikationsmedierna. Som administratör av låssystemet behöver du alltså inte omprogrammera några lås eller identifikationsmedier vid ändrade behörigheter.

3.3.1 Gateways

Gateways finns som onlinevarianter. I ett SimonsVoss-nätverk överförs data mellan gateway och identifikationsmedium:

- Ändrade behörigheter (positiva och negativa) från gateway till identifikationsmedium
- Spärr-ID:n från gateway till identifikationsmedium
- Kvitteringar i låssystemet som sparats på identifikationsmedierna från dessa till gateway-resursen.

Låsen behöver inte programmeras med programmeringsenheten. Låssystemet omprogrammeras istället via gateway-resurserna och användarna av identifikationsmedierna.

I LSM kan du använda smartreläer som gateways i låssystemet.

3.3.2 Direkta behörigheter

Behörighetsändringar som överförts till gateway-resurserna raderar resp. tilldelar behörigheter direkt på identifikationsmediet och fungerar därmed direkt. Om du vill spärra identifikationsmedier kan informationen (spärr-ID) överföras från gateway-resurserna till identifikationsmedierna. Användarna överför sedan den här informationen med sina identifikationsmedier till låsen i låssystemet.

Låsen sparar mottagningen av ändrade behörigheter från ett identifikationsmedium som feedback till efterföljande identifikationsmedier (kvitteringshantering). Identifikationsmediernas användare överför sedan denna feedback tillbaka till gateway-resursen. Gateway-resursen sparar överföringen i databasen och i LSM visas att det inte längre föreligger något programmeringsbehov av låsen i fråga.

Som administratör av låssystemet har du alltså översikt över vilka lås som har registrerat den ändrade behörigheten och vilka som ännu inte har gjort det. Du känner till låssystemets status.

3.3.3 Spärr-ID:n (Lock priority)

Du delar ut och återkallar behörigheter i LSM samt spärrar och avaktiverar identifikationsmedier och överför de ändrade behörigheterna med en gateway via identifikationsmedierna till låsen.

I ett virtuellt nätverk används normalt de behörigheter som är sparade på identifikationsmedierna. Om ett identifikationsmedium ska spärras och behörigheterna på detta identifikationsmedium fortfarande används skulle detta identifikationsmedium fortfarande kunna öppna lås så länge som behörigheterna på identifikationsmediet inte har ändrats via en gateway.

Detta förhindras genom att ett spärr-ID ställs in för identifikationsmediets ID: När ett identifikationsmedium inte längre har behörighet till ett lås ställs ett så kallat Lock priority (spärr-ID) in för mediets ID. Gateway-resursen överför detta spärr-ID till låsen via andra identifikationsmedier.

Om det finns ett spärr-ID för ett identifikationsmediums ID i ett lås ignoreras den behörighet som eventuellt fortfarande finns på identifikationsmediet och som i normalfallet används för detta lås. Istället gäller de behörigheter som är sparade i själva låset och som i ett virtuellt nätverk uppdateras via identifikationsmedierna (och därför är mer aktuella).

Samtidigt sparas det spärrade identifikationsmediets ID i en svart lista och kan inte aktiveras igen av misstag.

3.3.4 Förfallodatum (Expiry date)

För en effektiv användning av det virtuella nätverket är det nödvändigt att gateway-resursen regelbundet kan överföra data till och från identifikationsmedierna. Som administratör av låssystemet kan du lägga till ett förfallodatum som tvingar låssystemets användare att regelbundet använda sina identifikationsmedier med gateway-resursen.

Ett förfallodatum begränsar identifikationsmediets giltighet tidsmässigt. Användarna måste regelbundet fylla på sitt tidstillgodohavande via en gateway. De kan inte manövrera låsen (inte heller offlinelås) förrän de har fyllt på tidstillgodohavandet via gateway-resursen. Det finns två möjligheter att ställa in detta tidstillgodohavande:

- Ett fast antal timmar mellan 1 och 255 (till exempel behörighet under åtta timmar från och med påfyllning)
- Fast förfallotidpunkt mellan kl. 01.00 och 24.00 (till exempel behörighet mellan påfyllningstid och kl. 20.00)

Du ställer in detta tidstillgodohavande i LSM globalt för alla identifikationsmedier. Du kan även fastställa ett individuellt tidstillgodohavande för enskilda transpondrar. Generella ändringar (till exempel tidstillgodohavandets varaktighet) programmeras direkt i LSM.

3.3.5 Ställa in tid

Låsen och transpondrarna innehåller en tidskomponent. När en transponder används med en gateway ställs tidskomponenten i transpondern in på nytt (och eventuella tidsavvikelser i transpondern korrigeras). Tiden i transpondern används som referens vid manövrering av ett lås. Om tiden i låset avviker vid manövrering ställs tidskomponenten i låset in på nytt efter tiden i transpondern (och eventuella tidsavvikelser i låset korrigeras).

Tiden i låsen i det virtuella nätverket ställs in automatiskt med regelbundna intervall utan att du som administratör av låssystemet behöver programmera detta manuellt.

3.4 Tidsstyrning

Med tidszonsstyrningen kan du begränsa den tidsrymd (tidszon) då bestämda identifikationsmedier (och därmed personer eller grupper av personer) kan manövrera ett lås (och på så sätt exempelvis komma in i en byggnad).

3.4.1 Tidszoner

Du kan skapa valfria tidszonsplaner och tilldela varje område en individuell tidzonsplan. En tidszonsplan innehåller upp till 100 tidszonsgrupper som kan konfigureras med olika tillträdestider. I de olika tidszonsplanerna kan du välja och konfigurera tidszonsgrupperna på olika sätt.

3.4.2 Helgdagar

I tidszonsplanerna kan du utöver de sju veckodagarna (måndag till söndag) även ange andra särskilda dagar och helgdagar.

Du kan till exempel använda de listor med helgdagar som finns i LSM-programmet (för de tyska delstaterna). Alternativt kan du skapa egna listor oberoende av de medföljande helgdagslistorna. Du kan spara vilken dag som helst som helgdag så att den exempelvis behandlas som en söndag (se även *Särskilda dagar [▸ 12]*).

3.4.3 Särskilda dagar

En särskild dag har en tidsprofil som är oberoende av de sju veckodagarna. Särskilda dagar har högre prioritet än helgdagar.

Med särskilda dagar kan du exempelvis ge skolpersonal tillträde under skoltider från måndag till fredag och spärra tillträde under ferier med (högre prioriterade) särskilda dagar.

3.4.4 Giltighetsdatum (Validation date)

Du kan tilldela valfria giltighetsdatum till transpondrar. Transpondrar med ett giltighetsdatum kan användas i låssystemet först från och med detta datum.

Den här funktionen är oberoende av den virtuella nätverksanslutningen (se *Förfallodatum (Expiry date) [▸ 11]*) och kan bara ändras med programmeringsenheten. Använd inte den här funktionen tillsammans med virtuell nätverksanslutning.

3.4.5 Förfallodatum (Expiry date)

Du kan tilldela ett valfritt förfallodatum till transpondrar. Transpondrar med ett förfallodatum kan inte längre användas i låssystemet efter detta datum.

Den här funktionen är oberoende av den virtuella nätverksanslutningen (se *Förfallodatum (Expiry date) [▸ 11]*) och kan bara ändras med programmeringsenheten. Använd inte den här funktionen tillsammans med virtuell nätverksanslutning.

3.5 Listor

3.5.1 Passerlistor

Lås med passerkontrollfunktion loggar alla passeringar i en passerlista:

- Datum
- Tid
- Identifikationsmediets ID
- Användarens namn

Du kan läsa av och visa passerlistan i LSM-programmet. Antalet poster i passerlistan beror på låset och konfigurationen.

	Standard	Gateway
Cylinder	Upp till 3 000	
Smartrelä	Upp till 3 600	Upp till 200

3.5.2 Beträdelselistor

G2-transpondrar loggar passeringar i en beträdelselista oberoende av passerlistorna. I denna beträdelselista sparas de senaste beträdelserna (upp till1 000):

- Datum
- Tid
- Låsets ID

Du kan avläsa och visa beträdelselistan med LSM-programmet.

3.6 Protokollgenerationer

3.6.1 G1-låssystem

I G1-låssystem kan bara G1-produkter och G1-funktioner användas.

Om du använder G1-dataposter i G2-transpondrar stöds inte Expiry-funktionerna i G1-protokollen (till exempel med Validation Terminals).

INFO

G1-produkter tillverkas inte längre.

G1-produkter är inte längre tillgängliga.

3.6.2 G2-låssystem

I G2-låssystem kan bara G2-produkter och G2-funktioner användas.

3.6.3 G1- och G2-låssystem åtskilda

Med detta tillvägagångssätt delar du upp olika protokollgenerationer i (minst) två olika låssystem. På varje identifikationsmedium finns då (minst) två av varandra oberoende dataposter till låssystemen sparade (en för G1 och en för G2).

Fördelen med det här tillvägagångssättet är att man kan undvika kompatibilitetsproblem.

Du administrerar låssystemen i samma låsplan och i samma databas. Från och med LSM 3.0 kan du filtrera vyn i översikten efter protokollgeneration och beroende på filter visa lås och identifikationsmedier för antingen G1 eller G2.

3.6.4 G1- och G2-låssystem blandade (kompatibilitetsläge)

Med det här tillvägagångssättet administrerar du de båda olika protokollgenerationerna i samma låssystem.

- G1-produkter använder bara G1-funktioner.
- G2-produkter används i kompatibilitetsläge.

Du behöver bara administrera ett enda låssystem men på grund av att G1 och G2 är blandade begränsas överskådligheten och möjligheten att visa skillnader.

INFO

Funktionsbegränsningar i blandad användning

Användningen av blandsystem kan leda till funktionsbegränsningar och kräver erfarenhet.

1. Undvik blandade låssystem.
2. Använd i stället åtskilda låssystem (se *G1- och G2-låssystem åtskilda [▸ 14]*).

3.7 Batterivarningar

Batterivarningar i cylindrar med G2-protokoll är identiska med cylindrar med G1-protokoll (undantag: Mifare-cylindrar, se respektive handbok/ snabbguide).

3.7.1 G2-batteribytestranspondrar

Cylindrar med mycket svaga batterier går inte att manövrera med vanliga identifikationsmedier för att fullständig urladdning ska förhindras (G1: lagringsläge, G2: freeze-läge).

Lagringsläge och batterivarningar hos cylindrar med G1-protokoll kan bara åtgärdas på plats med hjälp av programmeringsenheten.

G2-protokollet möjliggör så kallade batteribytestranspondrar från och med LSM 3.0. Med en batteribytestransponder kan du häva freeze-läget hos G2-låscylindrar och manövrera låset med en vanlig, behörig transponder. Du måste inte befinna dig på plats vid låset med programmeringsenheten.

OBSERVERA

Urladdning av batterierna till följd av missbruk

Varje öppning som sker med en batteribytestransponder leder till att batterierna töms. Vid felaktig användning kan det leda till att batterierna töms helt. Batterierna måste i så fall omedelbart bytas ut.

4 G2-produkter

Om du vill använda alla funktioner i G2-protokollen måste du använda uteslutande G2-produkter. Information om tillgängliga G2-produkter finns i den aktuella SimonsVoss-prislistan.

4.1 Programmeringsenheter

För programmering av G2-komponenter behöver du en programmeringsenhet med lämplig fast programvara:

Standard (25 kHz)	≥ 9.10.4.XX
Mifare/SmartCard	≥ 9.10.4.34

Den fasta programvaran är bakåtkompatibel. Du kan även programmera befintliga G1-komponenter med programmeringsenheter som har uppdaterad fast programvara.

4.2 Cylindrar

Produkt	G1-kompatibel	G2-kompatibel
Standardcylinder (25 kHz)	ja	ja
Mifare/SmartCard-cylinder	nej	ja

4.3 SmartHandle

Produkt	G1-kompatibel	G2-kompatibel
SmartHandle 3062 Standard (25 kHz)	ja	ja
SmartHandle 3062 Mifare/SmartCard	nej	ja
SmartHandle AX Standard (25 kHz)	ja	ja
SmartHandle AX Mifare/SmartCard	nej	ja

4.4 Smartrelä

Produkt	G1-kompatibel	G2-kompatibel
Smartrelä	ja	ja
Smartrelä 2	ja	ja

Produkt	G1-kompatibel	G2-kompatibel
Smartrelä 3	ja	ja

4.5 Transponder

Du erhåller alla transpondrar som G2-produkter.

4.6 Nätverk (WaveNet)

WaveNet (RouterNodes och LockNodes) kan kommunicera med G1- och G2-produkter. Externa LockNodes stöds under vissa förutsättningar även i G2-komponenter.

	Dörrövervakning	Efterprogrammering
Interna LockNodes	ja	ja
Externa LockNodes	ja	nej

5 Signalering

När det gäller signalering skiljer man mellan transpondersignalering (t.ex. OK) och statussignalering (t.ex. batterivarning).

5.1 Transaktion

Funktion	Beskrivning	Signalering
Transaktion är OK Lås kopplas in	Lås kopplas in	2x kort
Lås kopplas ur	Lås kopplas ur	1x kort
Flipflop-läge (kopplas in)	Lås kopplas in	1x kort, 1x lång
Flipflop-läge (kopplas ur)	Lås kopplas ur	1x lång, 1x kort
Åtgärden kan inte utföras	Låset är avaktiverat	1x kort
	Låset är i freeze-läge	1x kort
	Identifikationsmediet är ogiltigt	1x kort

G2-produkter informerar användare med en signal att identifikationsmediet saknar behörighet.

5.2 Tillstånd

Funktion	Beskrivning	Signalering
Kritisk batteristatus i låset	Batterivarningsnivå 1	8x kort (för inkoppling)
Kritisk batteristatus i låset (låset är i flipflop-läge)	Batterivarningsnivå 1	Ungefär var 60:e sekund 4x dubbelt kort
Kritisk batteristatus i låset	Batterivarningsnivå 2	8x kort med en sekunds paus under 30 sekunder (före inkoppling)
Kritisk batteristatus i låset	Freeze-läge	6x lång-kort
Kritisk batteristatus i transpondern		8x dubbelt kort (efter urkoppling)
Programmeringsförlopp		1x kort (oberoende av programmeringsdata)

Funktion	Beskrivning	Signalering
Omstart (Power-On-Reset)		3x kort

Du kan avaktivera de akustiska batterivarningarna hos cylindrar. Användarna får dock ingen batterivarningsinformation från cylindrarna i detta läge.

5.3 Konfigurationsmöjligheter

5.3.1 Programmeringsförlopp

Du kan avaktivera låssignalering i en programmering.

5.3.2 Öppning

Du kan avaktivera den akustiska låssignaleringen i en programmering för individuella identifikationsmedier. Denna avaktivering gäller i hela låssystemet för detta identifikationsmedium.

6 Utbyggnad

6.1 Bygga ut G1

G1-enheter är inte längre tillgängliga. Bygg ut låssystemet med ett G2-låssystem om du använder ett G1-låssystem och behöver nya enheter. Du kan använda låssystemen åtskilda (se *G1- och G2-låssystem åtskilda [▸ 14]*) eller blandade (se *G1- och G2-låssystem blandade (kompatibilitetsläge) [▸ 14]*).

En virtuell nätverksanslutning, delvis anslutning eller fullständig anslutning till trådlöst nätverk ökar komforten och kan när som helst installeras i efterhand (se *Skillnader: Nätverksanslutningar [▸ 21]*).

6.2 Bygga ut G2

Du kan när som helst bygga ut och efterprogrammera G2-låssystemet som du önskar till gränserna för G2-protokollen.

En virtuell nätverksanslutning, delvis anslutning eller fullständig anslutning till trådlöst nätverk ökar komforten och kan när som helst installeras i efterhand (se *Skillnader: Nätverksanslutningar [▸ 21]*).

7 Skillnader: Nätverksanslutningar

	WaveNet (online)	Virtuell nätverksanslutning (virtuell)	Ingen nätverksanslutning (offline)
Funktionsprincip	Överföring av data med nätverksanslutna WaveNet-enheter (se Överföringsvägar och Enheter).	Överföring av data med identifikationsmedier (utom programmeringsdata).	Överföring av data med identifikationsmedier (utom programmeringsdata).
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.
Central aktivering/ avaktivering av lås	Möjlig.	Inte möjlig.	Inte möjlig.

	WaveNet (online)	Virtuell nätverksanslutning (virtuell)	Ingen nätverksanslutning (offline)
Aktivering/ avaktivering kan spåras centralt	Möjlig.	Inte möjlig.	Inte möjlig.
Fjärröppning	Möjlig.	Inte möjlig.	Inte möjlig.
Fjärrövervakning (DoorMonitoring)	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 på kritiska situationer i hela låssystemet (tillgänglighet för skyddsfunktioner, se I/O-konfiguration och skyddsfunktioner och RingCast)	Möjlig.	Inte möjlig.	Inte möjlig.

8 Bilaga

8.1 Skillnader G1- och G2-protokoll

	G1	G2	G2 (virtuell nätverksanslutning)
Lås	16 000	64 000	64 000
Identifikationsmedier	8 000	64 000	64 000
Tidszonsgrupper	5+1	100+1	100+1
Basinformationen	Identifikationsmedier		Lås
Låsplansinformation	Lås	Lås eller identifikationsmedier	Identifikationsmedier
Gateways (online)	Nej	Nej	Ja
Nätverk	Ja	Ja	Ja (endast Gateways)

Om du använder G2-protokoll utan virtuell nätverksanslutning kan du vid varje programmeringsbehov bestämma om du vill programmera identifikationsmediet eller låset. En identifikationsmedielista kan sparas i låsen och en låslista kan sparas i identifikationsmedierna.

8.2 Ordlista

Begrepp	Förklaring
ASM	Systemstatusövervakning
Område	Gruppering av flera lås för enklare administration av behörigheter
Beträdelselista	Lista som sparas på identifikationsmediet över beträdda lås.
Databas	Lagringsplats för all information om låsplan och låssystem i system 3060
Direkt nätverksanslutning (LockNode Inside)	Nätverksnod (LockNode) integrerad direkt i låset

Begrepp	Förklaring
Gateway	Anslutning av det virtuella nätverket till LSM-programmet
G1	Gammal protokollgeneration till B-fält-gränssnittet
G2	Aktuell protokollgeneration till B-fält-gränssnittet
LID	Lock-ID: Unik identifiering av ett lås i ett SimonsVoss-låssystem.
LSM	Locking System Management: Dataprogram med databasstöd för administration av SimonsVoss-låssystemet
LockNode	Nätverksnod för direkt närfältskommunikation med ett lås
Mekaniskt aktiv	(=inkopplad) Mekaniskt läge för ett lås som gör det möjligt för användaren att öppna och stänga.
Mekaniskt inaktiv	(=urkopplad) Mekaniskt läge för ett lås som gör att det inte är möjligt för användaren att öppna och stänga.
Nätverk	SimonsVoss WaveNet. Lås kan användas i onlineläge (=nätverksanslutet)
Låssystem	Sammanhörande mängd lås och identifikationsmedier som administreras tillsammans
Låssystemets lösenord	Lösenord för säkring av låssystemet
Låsplan	En låsplan kan bestå av flera låssystem
SID	Låssystem-ID: Unik identifiering av ett låssystem i en SimonsVoss-låsplan
Lås	Överordnat begrepp för alla produkter som ett identifikationsmedium kan kommunicera med

Begrepp	Förklaring
SmartCD	Programmeringsenhet: SimonsVoss-produkterna programmeras med en SmartCD
TID	Transponder-ID: Unik identifiering av ett identifikationsmedium i ett SimonsVoss-låssystem
Transponder	Medium som kan kommunicera med ett lås
Transpondergrupper	Gruppering av flera identifikationsmedier för att förenkla administration av behörigheter
Virtuellt nätverk	Teknik som används för att överföra ändrade behörigheter via gateways till offlinelås så att låsen inte behöver uppsökas lokalt
Tidszonsgrupper	Grupper som ingår i en tidszonsplan
Tidszonsplaner	Tidszonsplan som kan spara i ett lås
Passerlista	Lista över passeringar som sparas i låset (förutsättning: passerkontroll)
Tillträdesprofil (transpondergrupper/områden)	Definierar antalet lås som ett identifikationsmedium med denna profil kan kommunicera med.

9 Hjälp och ytterligare information

Infomaterial/dokument

Detaljerad information om drift och konfiguration samt andra dokument finns på SimonsVoss webbplats under rubriken Dokument (*ttps://www.simons-voss.com/se/nerladdningar/dokument.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-simonsvoss@allegion.com (System 3060, MobileKey)

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*).

Adress

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).

ALLEGION

SimonsVoss technologies