G2 protokoller

Håndbog

29.08.2020

SimonsVoss technologies

Indholdsfortegnelse

1 Generelle sikkerhedshenvisninger

Signalord (ANSI Z535.6)	Eventuella omedelbara effekter av bristande efterlevnad
FARE	Död eller allvarlig personskada (troligt)
ADVARSEL	Död eller allvarlig skada (möjligt, men osannolikt)
FORSIGTIG	Liten skada
OPMÆRKSOMHED	Skador på egendom eller fel
BEMÆRK	Låg eller ingen

ADVARSEL

Spærret adgang

Hvis komponenter er fejlagtigt monteret og/eller programmeret, kan adgang til en dør forblive spærret. For følgeskader, der skyldes spærret adgang, fx til personer, der er sårede eller i fare, tingsskader eller andre skader, hæfter SimonsVoss Technologies GmbH ikke!

Blokeret adgang gennem manipulation af produktet

Hvis du selv ændrer produktet, kan der opstå funktionsfejl, og adgang via en dør kan blokeres.

- Modificer kun produktet, når det er nødvendigt, og kun på den måde, der er beskrevet i dokumentationen.

BEMÆRK

Korrekt anvendelse

SimonsVoss-produkter er kun beregnet til åbning og lukning af døre og sammenlignelige genstande.

- Anvend ikke SimonsVoss-produkter til andre formål.

Afvigende tidspunkter ved G2-lukninger

Den interne tidsenhed ved G2-lukninger har en teknisk betinget tolerance på op til ± 15 minutter om året.

Krævede kvalifikationer

Installation og idriftsættelse kræver specialiseret viden.

- Kun uddannet personale må installere og idriftsætte produktet.

Den tyske sprogversion er den originale brugsanvisning. Andre sprog (udkast på kontraktsproget) er oversættelser af de originale instruktioner.

Læs og følg alle installations-, installations- og idriftsættelsesinstruktioner. Overfør disse instruktioner og eventuel vedligeholdelsesinstruktion til brugeren.

2 Generelt

G2-protokoller er en komplet nyudvikling af SimonsVoss-kommunikationen imellem identifikationsmedier og låse. Mange nye funktioner er implementeret, så mulighederne for administration af låseanlægget bliver endnu enklere og bedre.

Baseret på G2-protokollerne er passende hardwareprodukter og en fuldstændig modulær software tilgængelig, så låseanlægget kan tilpasses personlige behov endnu bedre.

3 G2-protokoller

3.1 Generel beskrivelse

G2-protokollerne åbner for nye funktioner i System 3060, når forudsætningerne er opfyldt:

- LSM fra version 3.0
- G2-hardwareprodukter

3.1.1 Låseanlæggets adgangskode

Låseanlæggets adgangskode kræves kun ved oprettelse af låseplanen. Derudover er sikkerheden for låseanlæggets adgangskode øget:

- Minimal længde 64 bit
- Integreret kvalitetsindeks i LSM-softwaren

LSM-softwaren tillader altså ikke længere usikre adgangskoder for låseanlægget og øger låseanlæggets sikkerhed.

3.1.2 Låseanlæggets størrelse

G2-protokollerne definerer grænserne for låseanlægget på ny. Det er nu muligt at administrere

- Op til 64.000 låse pr. låseanlæg
- Op til 64.000 identifikationsmedier pr. lås

Over fire milliarder individuelle rettigheder pr. låseanlæg muliggør en kompromisløs tilpasning af låseanlægget til individuelle behov.

3.1.3 Overlappende låseniveauer

Overlappende låseniveauer kan bruges til at anvende bestemte funktioner i flere låseanlæg. Disse funktioner er sikret af en egen adgangskode, der er uafhængig af låseanlægget (såkaldte tværlåseanlæg). I alt er der tre overordnede låseniveauer:

- Rødt låseniveau
- Grønt låseniveau
- Blåt låseniveau

En transponder kan tilhøre hhv. en af de tre niveauer. I LSM er der for hvert overordnet låseniveau reserveret 1024 transponder-ID'er. Det betyder, at maksimalt 1024 transpondere kan tildeles et overordnet låseniveau. For hver af disse transpondere er det muligt at tildele individuelle rettigheder eller spærre transponderne individuelt.

Transpondere, som du har tildelt det røde låsniveau, kan også åbne deaktiverede låse. Disse forbliver aktiveret eller åben i den indstillede pulsvarighed, men deaktiveres stadig. Hvis en transponder fra det røde låseniveau f.eks. gemmes i et brandmandsnøgledepot, så kan redningsfolk hurtigt rykke ind i bygningen i tilfælde af farer.

3.1.4 Nødfrigivelse

Hvis låseanlægget er sammenkoblet, så kan låsene frigives via netværket (WaveNet). Det gøres ved at sende en kommando fra LSM-softwaren via netværket til de ønskede låse, som vedvarende indkobler låsene. Enhver kan benytte disse låse uafhængigt af identifikationsmedier.

Låse, som er åbnet til nødfrigivelse via kommandoen, forbliver åbne, indtil frigivelsen ophæves af en kommando om nødåbning eller en kommando om fjernåbning.

En brandalarm kan via en kontakt i LSM-softwaren udløse en hændelse, hvis reaktion sender denne kommando. I tilfælde af brand åbnes dermed alle låse, som modtager kommandoen. Indelukkede personer kan forlade bygningen, og redningsfolk kan hurtigt rykke ind i bygningen.

Berettigede identifikationsmedier, som anvendes ved låse med nødfrigivelse, har ingen funktion.

3.1.5 Nødåbning

I LSM-softwaren er det muligt under eksport at tildele en midlertidig adgangskode til LSM Mobile. Denne adgangskode skal mindst have otte tegn, men har ellers ingen begrænsninger.

Med denne adgangskode er det så muligt på stedet at udføre en nødåbning af en lås, uden at låseanlæggets adgangskode kendes.

Af sikkerhedsårsager kan administratoren begrænse denne funktion:

- Antal mulige nødåbninger
- Tidsperiode, hvor nødåbninger er mulige

3.1.6 Impulslængde

For låsecylindere og SmartRelais kan indkoblingstider frit vælges imellem et og 25 sekunder.

Samtidigt er det med LSM-funktionen "Lang åbning" muligt at give enkelte identifikationsmedier en længere indkoblingstid. Denne funktion fordobler indkoblingstiden, hvor den samlede indkoblingstid fortsat er begrænset til 25 sekunder.

Indkoblingstider for alle låse påvirker	Impulslængden i låsens konfiguration

Indkoblingstider for enkelte identifikationsmedier påvirker	"Lang åbning" i identifikationsmediets konfiguration

3.1.7 Akustisk åbningssignal

Låse udsender et akustisk åbningssignal. Dette akustiske åbningssignal kan være forstyrrende, f.eks. i et sygehus. Åbning af døre om natten ville vække patienterne med et akustisk åbningssignal.

Dette akustiske åbningssignal kan deaktiveres for identifikationsmedier. Kobling af låse gøres dermed lydløs for enkelte eller for alle identifikationsmedier.

3.2 Tildeling af rettigheder

3.2.1 Generelt

De nye G2-protokoller reducerer administrationsforbruget efter udlevering af nye identifikationsmedier. Intelligente mekanismer i protokollerne eliminerer i vid udstrækning den hidtil nødvendige omprogrammering af låsene på stedet.

Alternativt til omprogrammering af låsene på stedet kan rettighederne også overføres til låsene på følgende måde:

- G2 uden sammenkobling
  - Direkte overførsel: Via identifikationsmedier og låse
  - Spærringer: Via reserve-identifikationsmedier
- Indirekte overførsel: G2 med virtuel sammenkobling (VN), se *Virtuelt netværk (VN) [▸ 9]*
- Netværksoverførsel: WaveNet

3.2.2 G2 uden sammenkobling

Hvis et G2-låseanlæg anvendes uden sammenkobling, så spares der meget tid ved oprettelse af nye låse eller nye identifikationsmedier. Med G2-protokollerne skal identifikationsmedier og låse ikke længere programmeres:

Ny lås	- Gem rettighederne på identifikationsmediet (programmering af identifikationsmedium) eller - Gem rettighederne i låsen (programmering af lås)
Nyt identifikationsmedium	

Der er ikke flere programmeringsopgaver i låseanlægget. For låseanlæggets administrator står et helt åbent system til rådighed. Ved programmeringen besluttes, om rettighederne gemmes på identifikationsmediet eller i låsen - afhængigt af, hvad der er mest komfortabelt.

Låse

I hver lås kan op til 64.000 identifikationsmedier administreres, dvs. individuelle rettigheder og spærring. Programmeringen er principielt identisk med programmeringen for G1-låse. I hvert G2-låseanlæg kan op til 64.000 låse gemmes og administreres.

Identifikationsmedier

I G2-låseanlæggene er det muligt individuelt i hvert identifikationsmedium at gemme, hvilke låse dette identifikationsmedium har rettigheder til. De nye G2-transpondere kan gemme og administrere op til tre G1-låseanlæg og fire G2-låseanlæg - dermed er det i G2-låseanlæg muligt at gemme hele låseplanen på transponderen.

Reservetranspondere og spærre-ID'er

Med introduktionen af LSM 3.0 SP2 kan andre identifikationsmedier (som f.eks. er blevet stjålet) også spærres med reserve-identifikationsmedier. Hvis reserve-identifikationsmediet programmeres, vælges det identifikationsmedium, som skal spærres, og et spærre-ID overføres til identifikationsmediet. Så snart reserve-identifikationsmediet bruges ved en lås, overfører reserve-identifikationsmediet spærre-ID'et til låsen, og identifikationsmediet, som skal spærres, har ikke længere sine rettigheder til denne lås.

Programmeringsbehovet ved låsene bevares og ophæves først efter en ny programmering af låsene, hvor identifikationsmediet, som skal spærres, hidtil har haft adgangsret.

3.3 Virtuelt netværk (VN)

I et virtuelt netværk modtager låsene kun de grundlæggende informationer ved den første programmering og godkendes i låseanlægget. Rettighederne gemmes udelukkende på identifikationsmedierne.

Hvis rettighederne ændres, skal rettighederne kun opdateres i identifikationsmedierne. I virtuelle netværk fås såkaldte gateways. Brugerne benytter identifikationsmedier ved gatewaysene og starter dermed dataoverførslen. Hvis der foreligger ændringer af rettighederne, opdaterer gatewayen rettighederne i identifikationsmedierne. Det er dermed ikke længere nødvendigt for låseanlæggenes administrator at omprogrammere låse eller identifikationsmedier, når rettigheder skal ændres.

3.3.1 Gateways

Gateways fås som onlinevariant. I et SimonsVoss-netværk overføres data imellem gateway og identifikationsmedium:

- Rettighedsændringer (positiv og negativ) fra gateway til identifikationsmedium
- Spærre-ID'er fra gateway til identifikationsmedium
- Låseanlæggets kvitteringer fra identifikationsmedium til gateway gemt på identifikationsmedierne

Programmering af låsene ved hjælp af programmeringsenhed bortfalder. I stedet for omprogrammeres låseanlægget via gateways eller identifikationsmediernes brugere.

Med LSM SmartRelais kan mulige gateways anvendes til låseanlægget.

3.3.2 Direkte rettigheder

Rettighedsændringer overført til gateways sletter eller tildeler rettigheder direkte i identifikationsmediet på ny og er derfor straks effektive. Hvis identifikationsmedier skal spærres, kan gatewaysene også overføre disse informationer (spærre-id) til identifikationsmedierne. Brugere af identifikationsmedier overfører så disse informationer til låsene i låseanlægget med deres identifikationsmedier.

Låsen gemmer den succesfulde modtagelse af rettighedsændringer udført af et identifikationsmedium som feedback på efterfølgende identifikationsmedier (kvitteringsstyring). Brugere af identifikationsmedier bringer derefter denne feedback med tilbage til gatewayen igen. Gatewayen gemmer den succesfulde overførsel i databasen, og LSM viser ikke længere noget programmeringsbehov ved den pågældende lås.

Låseanlæggets administrator bevarer dermed overblikket over, hvilke låse der allerede har modtaget rettighedsændringen, og hvilke der ikke har. Låseanlæggets tilstand kendes.

3.3.3 Spærre-ID'er (Lock priority)

De tildeler og fjerner rettigheder i LSM eller spærrer og deaktiverer identifikationsmedier og overfører rettighedsændringer med en gateway over identifikationsmedier til låsene.

I et virtuelt netværk anvendes normalt de rettigheder, der er gemt på identifikationsmedierne. Hvis et identifikationsmedium skal spærres og rettighederne på dette identifikationsmedium fortsat anvendes, vil dette identifikationsmedium fortsat kunne åbne låse, sålænge rettighederne på dette identifikationsmedium ikke ændres af en gateway.

Det forhindres af en Lock priority indstillet for identifikationsmediets ID. Hvis et identifikationsmedium ikke længere har adgangsret til en lås, indstilles en såkaldt Lock priority for dets ID. Gatewayen overfører denne Lock priority via andre identifikationsmedier til låsene.

Hvis der i en lås er indstillet en Lock priority for et identifikationsmediums ID, ignoreres den rettighed, som eventuelt stadig forefindes og normalt anvendes på dette identifikationsmedium, for denne lås. I stedet for gælder de rettigheder, som er gemt i låsen, og som i et virtuelt netværk opdateres af identifikationsmedierne (og derfor er mere aktuelle).

Samtidigt gemmes ID'et for identifikationsmediet, som spærres på denne måde, i en blacklist og kan ikke utilsigtet aktiveres igen.

3.3.4 Forfaldsdato (Expiry date)

En effektiv anvendelse af det virtuelle netværk kræver, at gatewayen regelmæssigt kan overføre data til og fra identifikationsmedierne. Låseanlæggets administrator kan med en forfaldsdato "tvinge" brugerne af låseanlægget til regelmæssigt at benytte deres identifikationsmedier ved gatewayen.

En forfaldsdato indskrænker et identifikationsmediums gyldighed. Brugerne skal regelmæssigt opfylde deres tidsbeholdning ved en gateway, ellers kan de ikke længere benytte deres identifikationsmedium ved en lås (heller ikke en offline-lås), før opfyldning af tidsbeholdningen ved en gateway har fundet sted. Der er to muligheder for denne tidsbeholdning:

- Faste timetal imellem en og 255 timer (f.eks. rettighed til otte timer fra opfyldning)
- Fast udløbs-klokkeslæt imellem kl. 1:00 og kl. 24:00 (f.eks. rettighed imellem opfyldningstidspunkt og kl. 20:00)

Denne tidsbeholdning indstilles globalt for alle identifikationsmedier i LSM. For enkelte transpondere er det dog også muligt at fastlægge en individuel tidsbeholdning. Generelle ændringer (f.eks. tidsbeholdningens varighed) programmeres direkte med LSM.

3.3.5 Indstilling af klokkeslæt

Der er indeholdt et tidsmodul i låsene og i transponderne. Hvis en transponder benyttes ved en gateway, indstilles tidsmodulet i transponderen på ny (og evt. forudgående eller efterfølgende tider i transponderen korrigeres). Tiden i transponderen bruges som reference ved anvendelse ved en lås. Hvis tiden i låsen afviger ved anvendelsen, indstilles tidsmodulet i låsen på ny efter tiden i transponderen (og evt. forudgående eller efterfølgende tider i låsen korrigeres).

Tiden i låsene i det virtuelle netværk indstilles automatisk regelmæssigt på ny, uden at låseanlæggets administrator skal programmere låsene igen manuelt.

3.4 Tidsstyring

Med tidszonestyring kan tidsrummet begrænses (tidszone), hvor bestemte identifikationsmedier (og dermed personer eller persongrupper) kan benytte en lås (og dermed f.eks. kan komme ind i bygningen).

3.4.1 Tidszoner

Vilkårlige tidszoneplaner kan oprettes, og hvert område kan individuelt tildeles en tidszoneplan. En tidszoneplan indeholder op til hundrede tidszonegrupper, som frit kan konfigureres med forskellige adgangstider. I de forskellige tidszoneplaner kan tidszonegrupperne vælges eller konfigureres forskelligt.

3.4.2 Helligdage

I tidszoneplanerne er det foruden de syv ugedage (mandag til søndag) også muligt at gå ind på særlige dage eller helligdage.

Her anvendes de helligdagslister (for alle tyske forbundslande), som er gemt i LSM-softwaren i stedet for selv at oprette dem. Alternativt kan egne helligdagslister oprettes uafhængigt af de medfølgende helligdagslister. Enhver vilkårlig dag kan gemmes som helligdag og kan eksempelvis behandles som en søndag (se også *Særlige dage [▸ 12]*).

3.4.3 Særlige dage

En særlig dag fastlægger en tidsprofil for bestemte dage, som er uafhængig af de syv ugedage. Særlige dage har en højere prioritet end helligdage.

Med særlige dage kan f.eks. adgangen for skolepersonale tillades i skoletiden fra mandag til fredag og generelt spærres med særlige dage (med højere prioritet) under ferie.

3.4.4 Gyldighedsdato (Validation date)

Transpondere kan tildeles en vilkårlig gyldighedsdato. Transpondere med en gyldighedsdato kan først anvendes i låseanlægget efter denne gyldighedsdato.

Denne funktion er uafhængig af den virtuelle sammenkobling (se *Forfaldsdato (Expiry date) [▸ 11]*) og kan kun ændres af programmeringsenheden. Brug ikke denne funktion sammen med den virtuelle sammenkobling.

3.4.5 Forfaldsdato (Expiry date)

Transpondere kan tildeles en vilkårlig forfaldsdato. Transpondere med en forfaldsdato kan ikke længere anvendes i låseanlægget efter denne forfaldsdato.

Denne funktion er uafhængig af den virtuelle sammenkobling (se *Forfaldsdato (Expiry date) [▸ 11]*) og kan kun ændres af programmeringsenheden. Brug ikke denne funktion sammen med den virtuelle sammenkobling.

3.5 Lister

3.5.1 Tilgangslister

Låse med ZK-funktion protokollerer adgange i en tilgangsliste:

- Dato
- Klokkeslæt
- Identifikationsmediets ID
- Navn på bruger

Tilgangslisten kan udlæses og vises med LSM-softwaren. Antallet af poster i tilgangslisten afhænger af låsen og konfigurationen.

	Standard	Gateway
Cylinder	Op til 3000	
SmartRelais	Op til 3600	Op til 200

3.5.2 Adgangslister

G2-transpondere protokollerer adgangene uafhængigt af tilgangslisterne i en adgangsliste. I denne adgangsliste er de sidste adgange gemt (op til 1000):

- Dato
- Klokkeslæt
- Låsens ID

Adgangslisten kan udlæses og vises med LSM-softwaren.

3.6 Protokolgenerationer

3.6.1 G1-låseanlæg

I G1-låseanlæg er det kun muligt at anvende G1-produkter og kun G1-funktioner.

Hvis G1-datasæt anvendes i G2-transpondere, understøttes G1-protokollernes Expiry-funktioner ikke (f.eks. med valideringsterminaler).

BEMÆRK

G1-produkter er ophørt

G1-produkter kan ikke længere fås.

3.6.2 G2-låseanlæg

I G2-låseanlæg er det kun muligt at anvende G2-produkter og kun G2-funktioner.

3.6.3 G1- og G2-låseanlæg adskilt

Med denne tilgang deles de forskellige protokolgenerationer op i (mindst) to forskellige låseanlæg. På hvert identifikationsmedium er der gemt (mindst) to datasæt for låseanlæg, som er uafhængige af hinanden (hhv. et fra G1 og et fra G2).

Fordelen ved denne tilgang forhindrer kompatibilitetsproblemer på forhånd.

Disse låseanlæg administreres i samme låseplan og i samme database. Fra LSM 3.0 kan visningen filtreres efter protokolgeneration i matrixen, og afhængigt af filter ses kun låse og identifikationsmedier for G1 eller G2.

3.6.4 G1- og G2-låseanlæg blandet (kompatibilitetstilstand)

Med denne tilgang administreres de to forskellige protokolgenerationer i samme låseanlæg.

- G1-produkter anvender fortsat kun G1-funktioner.
- G2-produkter anvendes i kompatibilitetstilstand.

Kun et eneste låseanlæg skal passes, men på grund af blandingen af G1 og G2 begrænses overskueligheden og forskelligheden.

BEMÆRK

Funktionsbegrænsninger på grund af blandet drift

Anvendelsen af blandede systemer kan medføre funktionsbegrænsninger og kræver erfaring.

1. Undgå blandede låseanlæg.
2. Benyt i stedet for adskilte låseanlæg (se *G1- og G2-låseanlæg adskilt [▸ 14]*).

3.7 Batteriadvarsler

Cylindernes batteriadvarsler med G2-protokol er identiske med cylindere med G1-protokol (undtagelse: Mifare-cylindere, se de pågældende manualer/korte vejledninger).

3.7.1 G2-batteriskifttranspondere

Cylindere med meget svage batterier kan ikke længere bruges med normale identifikationsmedier, så en total afladning undgås (G1: lagertilstand, G2: freeze-tilstand).

Lagertilstanden og batteriadvarslerne ved cylindere med G1-protokoller kan kun ophæves på stedet med programmeringsenheden.

G2-protokollen muliggør såkaldte batteriskifttranspondere fra LSM 3.0. Med batteriskifttransponderen ophæves freeze-tilstanden for G2-låsecylinderen, og låsen betjenes med en normalt berettiget transponder. Programmeringsenheden på stedet ved låsen kræves ikke.

FORSIGTIG

Afladning af batterierne på grund af misbrug

Ved alle åbninger i sammenhæng med en batteriskiftetransponder bliver batteriet yderligere tømt. Ved forkert anvendelse kan det medføre fuldstændig afladning af batterierne! I denne tilstand skal batterierne udskiftes omgående.

4 G2-produkter

Hvis alle G2-protokollernes funktioner skal anvendes, må der kun anvendes G2-produkter. Informationer om G2-produkternes tilgængelighed findes i den aktuelle SimonsVoss-prisliste.

4.1 Programmeringsenheder

Til programmering af G2-komponenter kræves en programmeringsenhed med egnet firmware:

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

Firmwaren er kompatibel nedefter. De hidtidige G1-komponenter kan også programmeres med programmeringsenheder med ny firmware.

4.2 Cylinder

Produkt	G1-kompatibel	G2-kompatibel
Standardcylinder (25 kHz)	Ja	Ja
Mifare/SmartCard-Zylinder	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 SmartRelais

Produkt	G1-kompatibel	G2-kompatibel
SmartRelais	Ja	Ja
SmartRelais 2	Ja	Ja
SmartRelais 3	Ja	Ja

4.5 Transponder

Alle transpondere fås som G2-produkt.

4.6 Netværk (WaveNet)

WaveNet (RouterNodes og LockNodes) kan styre G1- og G2-produkter. Eksterne LockNodes understøttes betinget også i G2-komponenter.

	Dørovervågning	Omprogrammering
Interne LockNodes	Ja	Ja
Eksterne LockNodes	Ja	Nej

5 Signalering

Ved signalering skelnes imellem transpondersignalering (f.eks. OK) og tilstandssignalering (f.eks. batteriadvarsel).

5.1 Transaktion

Funktion	Beskrivelse	Signalering
Transaktion er ok Lås kobler ind	Lås kobler ind	2x kort
Lås kobler ud	Lås kobler ud	1x kort
Flip-flop-tilstand (kobler ind)	Lås kobler ind	1x kort, 1x lang
Flip-flop-tilstand (kobler ud)	Lås kobler ud	1x lang, 1x kort
Proces kan ikke udføres	Lås er deaktiveret	1x kort
	Lås er i freeze-tilstand	1x kort
	Identifikationsmedium er ugyldigt	1x kort

G2-produkter viser brugeren med et afvisningssignal, at identifikationsmediet ikke er berettiget.

5.2 Tilstand

Funktion	Beskrivelse	Signalering
Låsens kritiske batteristatus	Batteriadvarsel 1	8x kort (før indkobling)
Låsens kritiske batteristatus (lås er i flip-flop-tilstand)	Batteriadvarsel 1	Ca. for hver 60 sekunder 4x dobbelt kort
Låsens kritiske batteristatus	Batteriadvarsel 2	8x kort med et sekunds pause i 30 sekunder (før indkobling)
Låsens kritiske batteristatus	Freeze-tilstand	6x lang-kort
Transponderens kritiske batteristatus		8x dobbelt kort (efter udkobling)
Programmering		1x kort (afhængigt af programmeringsdataene)

Funktion	Beskrivelse	Signalering
Genstart (Power-On-Reset)		3x kort

De akustiske batteriadvarsler ved cylinderne kan deaktiveres. Cylinderen signalerer ikke længere brugere om tomme batterier i denne tilstand.

5.3 Konfigurationsmuligheder

5.3.1 Programmering

En programmerings signalering på låsens side kan deaktiveres.

5.3.2 Åbning

En programmerings akustiske signalering på låsens side kan deaktiveres for enkelte identifikationsmedier. Denne deaktivering gælder for dette identifikationsmedium i hele låseanlægget.

6 Udvidelse

6.1 Udvidelse af G1

G1-enheder kan ikke længere fås. Hvis et G1-låseanlæg anvendes og der kræves nye enheder, udvides G1-låseanlægget med et G2-låseanlæg. Låseanlæggene kan bruges adskilt (se *G1- og G2-låseanlæg adskilt [▸ 14]*) eller blandet (se *G1- og G2-låseanlæg blandet (kompatibilitetstilstand) [▸ 14]*).

En eventuel virtuel sammenkobling, delvis sammenkobling eller total sammenkobling øger komforten og kan til enhver tid eftermonteres (se *Forskelle: Sammenkoblinger [▸ 21]*).

6.2 Udvidelse af G2

G2-låseanlægget kan til enhver tid udvides og omprogrammeres til G2-protokollernes grænser.

En eventuel virtuel sammenkobling, delvis sammenkobling eller total sammenkobling øger komforten og kan til enhver tid eftermonteres (se *Forskelle: Sammenkoblinger [▸ 21]*).

7 Forskelle: Sammenkoblinger

	WaveNet (online)	Virtuel sammenkobling (virtuel)	Ingen sammenkobling (offline)
Funktionsprincip	Overførsel af data med sammenkoblede WaveNet-enheder (se Overførselsveje og Enheder).	Overførsel af data med identifikationsmedier (undtagen programmeringsdata).	Overførsel af data med programmeringsenheder.
Udbredelse	WaveNet-er forbundet via forskellige overførselsmedier. Alle former for data overføres ved hjælp af disse overførselsmedier.	I det virtuelle netværk overføres bestemte data ved hjælp af en gateway til identifikationsmedierne (registreringer i blacklist). Når disse identifikationsmedier anvendes ved en virtuelt sammenkoblet lås, overføres dataene til låsen.	Låse, som ikke er sammenkoblet, kan kun udveksle data med programmeringsenheden. Programmeringsenheden skal være ved låsen.
Programmeringsopgaver	Få.	Få.	Opgaver afhænger af låseanlæggets størrelse. ▪ Lille låseanlæg: Få opgaver. ▪ Mellemstort låseanlæg: Mellem opgaver. ▪ Stort låseanlæg: Mange opgaver.
Dataudvekslingens overførselshastighed	Umiddelbar. Dataudveksling med forskellige overførselsmedier.	Hastighed imellem gateway og lås stærkt afhængig af låsenes anvendelsesintensitet. Identifikationsmedier er overførselsmedier - uden identifikation ingen dataoverførsel.	Langsom.
Central aktivering/deaktivering af låse	Mulig.	Ikke mulig.	Ikke mulig.

	WaveNet (online)	Virtuel sammenkobling (virtuel)	Ingen sammenkobling (offline)
Aktivering/deaktivering kan spores centralt	Mulig.	Ikke mulig.	Ikke mulig.
Fjernåbning	Mulig.	Ikke mulig.	Ikke mulig.
Fjernovervågning (DoorMonitoring)	Mulig.	Ikke mulig.	Ikke mulig.
Eventmanagement	Mulig.	Ikke mulig.	Ikke mulig.
Tilgangslister kan hentes centralt	Mulig.	Ikke mulig (undtagen SREL 3).	Ikke mulig.
Software-/serveruafhængigt beskyttelsesfunktioner	Mulig.	Ikke mulig.	Ikke mulig.
Øjeblikkelig reaktion på kritiske situationer i hele anlægget (tilgængelighed af beskyttelsesfunktioner, se I/O-konfiguration og beskyttelsesfunktioner og RingCast)	Mulig.	Ikke mulig.	Ikke mulig.

8 Bilag

8.1 Forskelle G1- og G2-protokoller

	G1	G2	G2 (virtuelt sammenkoblet)
Låsninger	16000	64000	64000
Identifikationsmedier	8000	64000	64000
Tidszonegrupper	5+1	100+1	100+1
Basisinformationer	Identifikationsmedier		Låse
Låseplansinformationer	Låse	Låse eller identifikationsmedier	Identifikationsmedier
Gateways (online)	Nej	Nej	Ja
Netværk	Ja	Ja	Ja (kun gateways)

Hvis G2-protokoller anvendes uden virtuel sammenkobling, er det muligt ved hvert programmeringsbehov at beslutte, om identifikationsmediet eller låsen programmeres. Låsene kan gemme en identifikationsmediumliste og identifikationsmedierne en låseliste.

8.2 Ordliste

Begreb	Forklaring
ASM	Anlægsstatusmonitoring
Område	Sammenfatning af flere låse til lettere administrering af rettigheder
Adgangsliste	Liste over betrådte låse, som gemmes på identifikationsmediet
Database	Lagring af alle informationer i låseplanen eller låseanlægget for System 3060
Direkte sammenkobling (LockNode Inside)	Netværksknude (LockNode) integreret direkte i låsen
Gateway	Det virtuelle netværks tilslutning til LSM-softwaren

Begreb	Forklaring
G1	B-felt-grænsefladens gamle protokolgeneration
G2	B-felt-grænsefladens aktuelle protokolgeneration
LID	Lock-ID: Entydig identifikator for en lås i et SimonsVoss-låseanlæg
LSM	Locking System Management: Databasebeskyttet pc-software til administrering af SimonsVoss-låseanlægget
LockNode	Netværksknude til direkte nærområdekommunikation med en lås
Mekanisk aktiv	(=Indkoblet) Mekanisk tilstand for en lås, som muliggør åbning og lukning for en bruger
Mekanisk inaktiv	(=Udkoblet) Mekanisk tilstand for en lås, som ikke tillader åbning og lukning for en bruger
Netværk	SimonsVoss WaveNet. Låse kan anvendes i onlinetilstand (=sammenkoblet)
Låseanlæg	Sammenhørende og fælles administreret mængde af låse og identifikationsmedier
Låseanlæggets adgangskode	Adgangskode til sikring af låseanlægget
Låseplan	En låseplan kan bestå af flere låseanlæg
SID	Låseanlæg-ID: Entydig identifikator for et låseanlæg i en SimonsVoss-låseplan
Lås	Overbegreb for alle produkter, som kan styres med et identifikationsmedium
SmartCD	Programmeringsenhed: SimonsVoss-produkterne programmeres med en SmartCD

Begreb	Forklaring
TID	Transponder-ID: Entydig identifikator for et identifikationsmedium i et SimonsVoss-låseanlæg
Transponder	Medium, som kan kommunikere med en lås
Transpondergrupper	Sammenfatning af flere identifikationsmedier til en gruppe, så rettigheder kan administreres nemmere
Virtuelt netværk	Teknologi, hvormed rettighedsændringer ved offline-låse kan udbredes via gateways og låses ikke skal opsøges
Tidszonegrupper	Grupper som del af en tidszoneplan
Tidszoneplaner	Tidszoneplan, som kan gemmes i låsen
Tilgangsliste	Liste over adgange, som gemmes i låsen (forudsætning: ZK)
Adgangsprofil (transpondergrupper/områder)	Definerer mængden af låse, som kan styres med et identifikationsmedium, hvorpå denne profil befinder sig

9 Hjælp og flere oplysninger

Infomateriale/dokumenter

Detaljerede oplysninger om drift og konfiguration samt yderligere dokumenter kan findes på SimonsVoss hjemmeside i downloadområdet under Dokumenter (*https://www.simons-voss.com/dk/downloads/dokumenter.html*).

Overensstemmelseserklæringer

Overensstemmelseserklæringer for dette produkt findes på SimonsVoss hjemmeside i certifikatområdet (*https://www.simons-voss.com/dk/certifikater.html*).

Hotline

Ved tekniske spørgsmål hjælper SimonsVoss Service-Hotline gerne på telefon +49 (0) 89 99 228 333 (Opkald på tysk fastnet, prisen varierer af udbyder).

e-mail

Vil du hellere skrive os en e-mail?

support-simonsvoss@allegion.com (System 3060, MobileKey)

FAQ

Information og assistance med SimonsVoss produkter findes på SimonsVoss hjemmeside i FAQ sektionen (*https://faq.simons-voss.com/otrs/public.pl*).

Adresse

SimonsVoss Technologies GmbH
Feringastraße 4
85774 Unterföhring
Tyskland

Det er SimonsVoss

SimonsVoss er teknologiførende inden for digitale låsesystemer.

Pioneren for radiostyret, trådløs låseteknik tilbyder systemløsninger med en bred produktpalet til små og mellemstore virksomheder, store virksomheder samt offentlige områder.

SimonsVoss låsesystemer forbinder intelligent funktionalitet, høj kvalitet og præmieret design Made in Germany. Som innovativ systemudbyder lægger SimonsVoss vægt på skalerbare systemer, høj sikkerhed, pålidelige komponenter, ydedygtig software og nem betjening.

Modet til innovation, bæredygtig tankegang og handling samt høj påskønnelse af medarbejdere og partnere er grundlaget for den økonomiske succes. Virksomheden med hovedsæde i Unterföring ved München og produktion i Osterfeld (Sachsen-Anhalt) beskæftiger ca. 300 medarbejdere i otte lande.

SimonsVoss er en virksomhed i ALLEGION Group – et globalt arbejdende netværk inden for området sikkerhed. Allegion er repræsenteret i ca. 130 lande verden over (www.allegion.com).

ALLEGION

SimonsVoss technologies