Protocolli G2

Manuale

12.12.2023

SimonsVoss technologies

Sommario

1. Avvisi di sicurezza generali

Parola segnale: Possibili effetti immediati di non conformità
AVVERTENZA: Morte o lesioni gravi (possibili, ma improbabili)
ATTENZIONE: Lesione minori
NOTA: Basso o no

AVVERTENZA

Accesso bloccato

Con componenti montati e/o programmati in modo difettoso, l'accesso attraverso una porta può restare bloccato. La SimonsVoss Technologies GmbH non risponde delle conseguenze di un accesso bloccato, per esempio nel caso si debba accedere a persone ferite o in pericolo, di danni a cose o altri danni!

Accesso bloccato tramite manipolazione del prodotto

Se si modifica il prodotto da solo, possono verificarsi malfunzionamenti e l'accesso attraverso una porta può essere bloccato.

- Modificare il prodotto solo quando necessario e solo nel modo descritto nella documentazione.

NOTA

Uso conforme

I prodotti SimonsVoss sono concepiti esclusivamente per l'apertura e la chiusura di porte e oggetti simili.

- Non utilizzare i prodotti SimonsVoss per altri scopi.

Tempi diversi per chiusure G2

L'unità temporale interna delle chiusure G2 è tecnicamente vincolata a una tolleranza fino a ± 15 minuti all'anno.

Qualifiche richieste

L'installazione e la messa in servizio richiedono conoscenze specialistiche.

- Solo personale qualificato può installare e mettere in servizio il prodotto.

Non si escludono modifiche o perfezionamenti tecnici, anche senza preavviso.

La versione in lingua tedesca è il manuale di istruzioni originale. Altre lingue (redazione nella lingua del contratto) sono traduzioni delle istruzioni originali.

Leggere e seguire tutte le istruzioni di installazione, installazione e messa in servizio. Passare queste istruzioni e tutte le istruzioni di manutenzione all'utente.

2. Dati generali

I protocolli G2 sono uno sviluppo completamente nuovo nella comunicazione SimonsVoss tra i supporti di identificazione e le chiusure. Numerose nuove funzioni sono state implementate in modo da avere opzioni ancora più semplici e migliori per la gestione del vostro impianto di chiusura.

Basati sui protocolli G2, sono disponibili i giusti prodotti hardware e un software completamente modulare per adattare meglio l'impianto di chiusura alle vostre esigenze personali.

3. Protocolli G2

3.1 Descrizione generale

I protocolli G2 abilitano nuove funzionalità nel Sistema 3060 se vengono soddisfatti requisiti specifici:

- LSM a partire dalla versione 3.0
- Prodotti hardware G2

3.1.1 Password del sistema di chiusura

La password dell'impianto di chiusura è necessaria solo durante la creazione del piano di chiusura. Inoltre aumenta la sicurezza della password dell'impianto di chiusura:

- Lunghezza minima 64 bit
- Indice di qualità integrato nel software LSM

Pertanto, il software LSM non consente più password non sicure e aumenta la sicurezza dell'impianto di chiusura.

3.1.2 Dimensioni dell'impianto di chiusura

I protocolli G2 ridefiniscono i limiti del vostro impianto di chiusura. Ora sono in grado di gestire

- fino a 64000 chiusure per impianto
- fino a 64000 supporti di identificazione per

impianto. Più di quattro miliardi di possibili autorizzazioni individuali per impianto di chiusura consentono l'adattamento senza compromessi dell'impianto di chiusura alle vostre esigenze individuali.

3.1.3 Livelli di chiusura sovrapposti

Con i livelli di chiusura sovrapposti è possibile utilizzare determinate funzioni in più impianti di chiusura. Queste funzioni sono protette da una password propria, indipendentemente dall'impianto di chiusura (i cosiddetti impianti di chiusura incrociata). Sono disponibili tre livelli di chiusura sovraordinati:

- Livello di chiusura rosso
- Livello di chiusura verde
- Livello di chiusura blu

Ogni transponder può appartenere ad uno dei tre livelli. Nell'LSM, 1024 ID transponder sono riservati per ogni livello di chiusura superiore. Ciò significa che è possibile assegnare un massimo di 1024 transponder ad un livello di chiusura superiore. Per ognuno di questi transponder è possibile assegnare autorizzazioni individuali o bloccare i transponder singolarmente.

I transponder assegnati al livello di blocco rosso possono anche aprire blocchi disattivati. Questi rimangono impegnati o aperti per la durata dell'impulso impostata, ma sono ancora disattivati. Se, ad esempio, si posiziona un transponder del livello di chiusura rosso in un deposito di chiavi dei vigili del fuoco, il personale di soccorso può avanzare rapidamente all'interno dell'edificio in caso di pericolo.

3.1.4 Sblocco di emergenza

Se avete collegato in rete il vostro impianto di chiusura, potete attivare le vostre serrature tramite la vostra rete (WaveNet). A tale scopo, si invia un comando dal software LSM attraverso la rete ai sistemi di chiusura desiderati. Tale comando accoppia permanentemente i sistemi di chiusura. Chiunque può accedere a queste chiusure indipendentemente dai supporti di identificazione.

Le chiusure che sono state aperte utilizzando il comando di sblocco di emergenza rimangono aperte fino a quando non si annulla il comando di sblocco di emergenza con un comando di apertura di emergenza o un comando di apertura remota.

Un sistema di allarme antincendio può innescare un evento tramite un contatto nel software LSM, la cui reazione invia questo comando. In caso di incendio, tutte le chiusure che ricevono il comando vengono aperte. Le persone intrappolate possono lasciare l'edificio e i soccorritori possono muoversi rapidamente all'interno dell'edificio.

I supporti di identificazione autorizzati che vengono utilizzati sulle chiusure di emergenza sbloccate non hanno alcuna funzione.

3.1.5 Apertura di emergenza

È possibile assegnare una password temporanea nel software LSM durante l'esportazione in LSM Mobile. Questa password deve essere lunga almeno otto caratteri, ma non ha ulteriori restrizioni.

Con questa password è possibile effettuare in loco un'apertura di emergenza su una chiusura senza dover conoscere la password dell'impianto di chiusura.

Per motivi di sicurezza, come amministratore è possibile limitare questa funzione:

- Numero di possibili aperture d’emergenza

- Periodo in cui sono possibili aperture di emergenza

3.1.6 Lunghezza dell'impulso

Per i cilindri di chiusura e gli Smart Relè è possibile selezionare liberamente tempi di accoppiamento da uno a 25 secondi.

Allo stesso tempo, è possibile utilizzare la funzione LSM "Apertura lunga" per consentire ai singoli supporti di identificazione un tempo di accoppiamento più lungo. Questa funzione raddoppia il tempo di accoppiamento, ma il tempo totale di accoppiamento è ancora limitato a 25 secondi.

Influenzare i tempi di accoppiamento per tutte le chiusure	Lunghezza dell'impulso nella configurazione della chiusura
Influenzare i tempi di accoppiamento per singoli supporti di identificazione	"Apertura lunga" nella configurazione del supporto di identificazione.

3.1.7 Segnale acustico di apertura

Le chiusure emettono un segnale acustico di apertura. Questo segnale acustico di apertura può disturbare, ad esempio in un ospedale. L'apertura delle porte di notte sveglierebbe i pazienti con un segnale acustico di apertura.

Questo segnale acustico di apertura può essere disattivato per ogni mezzo di identificazione. In questo modo è possibile disattivare le chiusure per i singoli o per tutti i supporti di identificazione.

3.2 Assegnazione dell'autorizzazione

3.2.1 Dati generali

I nuovi protocolli G2 riducono il vostro impegno di gestione dopo l'emissione di nuovi supporti di identificazione. Meccanismi intelligenti nei protocolli evitano in larga misura la riprogrammazione in loco, fino ad ora necessaria, delle vostre chiusure.

In alternativa alla riprogrammazione delle chiusure in loco, è anche possibile trasmettere le autorizzazioni alle chiusure come segue:

- G2 senza collegamento in rete
  - Trasmissione diretta: tramite supporti di identificazione e chiusure
  - Blocchi: Tramite supporti di identificazione sostitutivi
- Trasmissione indiretta: G2 con collegamento in rete virtuale (VN), vedere *Rete virtuale (VN) [▸ 10]*

- Trasmissione in rete: WaveNet

3.2.2 G2 senza collegamento in rete

Se si utilizza un impianto di chiusura G2 senza rete, si risparmia tempo nella creazione di nuove chiusure o di nuovi supporti di identificazione. In questo caso, non è più necessario programmare i supporti di identificazione e le chiusure con i protocolli G2:

Nuova chiusura	- Salvate le autorizzazioni sul supporto di identificazione (programmando il supporto di identificazione) oppure - salvate le autorizzazioni nella chiusura (programmazione della chiusura)
Nuovo supporto di identificazione	

La programmazione del vostro impianto di chiusura non richiede ulteriori operazioni di programmazione. In qualità di amministratore di un impianto di chiusura avete a disposizione un impianto completamente aperto. Durante la programmazione potete decidere se salvare le autorizzazioni sul supporto di identificazione o nella chiusura - a seconda di quale sia più conveniente per voi.

Chiusure

È possibile gestire fino a 64000 supporti di identificazione in ogni chiusura, ovvero autorizzarli e bloccarli singolarmente. La procedura di programmazione è sostanzialmente identica a quella delle chiusure G1. In ogni impianto di chiusura G2 è possibile memorizzare e gestire fino a 64000 chiusure.

Supporti di identificazione

Nei vostri impianti di chiusura G2 potete memorizzare individualmente in ogni supporto di identificazione per quali chiusure questo supporto di identificazione è autorizzato. I nuovi transponder G2 possono memorizzare e gestire fino a tre impianti di chiusura G1 e quattro impianti di chiusura G2 - in questo modo l'intero piano di chiusura può essere memorizzato sul transponder negli impianti di chiusura G2.

Transponder di ricambio e ID di blocco

Con l'introduzione di LSM 3.0 SP2, è possibile utilizzare supporti di identificazione sostitutivi per bloccare altri supporti di identificazione (come quelli che sono stati rubati). Quando si programma il supporto di identificazione sostitutivo, selezionare il supporto di identificazione da bloccare e trasmettere un ID di blocco al supporto di identificazione. Non

appena viene azionato su una chiusura, il supporto di identificazione sostitutivo trasferisce l'ID di blocco alla chiusura e il supporto di identificazione da bloccare non è più autorizzato su questa chiusura.

La necessità di programmazione dei sistemi di chiusura rimane e viene annullata solo quando si riprogramma i sistemi di chiusura per i quali il supporto di identificazione da bloccare era stato precedentemente autorizzato.

3.3 Rete virtuale (VN)

In una rete virtuale, i sistemi di chiusura ricevono le informazioni di base e sono ammessi nel vostro impianto di chiusura solo al momento della prima programmazione. Le autorizzazioni sono conservate esclusivamente sul supporto di identificazione.

Se cambiano, le autorizzazioni devono essere aggiornate solo nei supporti di identificazione. Nelle reti virtuali sono previsti per questo scopo i cosiddetti gateway. Gli utenti utilizzano i supporti di identificazione sui gateway iniziando così la trasmissione dei dati. In caso di modifiche dell'autorizzazione, il gateway aggiorna le autorizzazioni nel supporto di identificazione. In qualità di amministratore dell'impianto di chiusura non è più necessario riprogrammare le chiusure o i supporti di identificazione quando si modificano le autorizzazioni.

3.3.1 Gateway

I gateway sono disponibili come varianti online. In una rete SimonsVoss lo scambio dei dati avviene tra il gateway e il supporto di identificazione:

- Modifiche alle autorizzazioni (positive e negative) da gateway a supporto di identificazione
- ID di blocco da gateway a supporto di identificazione
- Conferme dell'impianto di chiusura memorizzate sui supporti di identificazione dal supporto di identificazione al gateway

Non è necessario programmare le chiusure con un dispositivo di programmazione. L'impianto di chiusura viene invece riprogrammato attraverso i gateway o gli utenti dei supporti di identificazione.

È possibile utilizzare lo Smart Relè LSM come possibile gateway per il proprio impianto di chiusura.

3.3.2 Autorizzazioni dirette

Le modifiche alle autorizzazioni trasferite ai gateway possono essere cancellate o le nuove autorizzazioni assegnate direttamente nel supporto di identificazione e sono quindi immediatamente valide. Se si desidera bloccare il supporto di identificazione, i gateway possono anche trasferire

queste informazioni (ID di blocco) al supporto di identificazione. Gli utenti dei supporti di identificazione utilizzano quindi i loro supporti di identificazione per trasferire queste informazioni alle serrature del vostro impianto di chiusura.

La chiusura memorizza la corretta ricezione delle modifiche dell'autorizzazione da parte di un supporto di identificazione come feedback sui supporti di identificazione successivi (gestione della conferma). Gli utenti dei supporti di identificazione riportano poi questo feedback al gateway. Il gateway memorizza la trasmissione riuscita nella banca dati e LSM non visualizza più alcuna necessità di programmazione per le chiusure corrispondenti.

In qualità di amministratore di un impianto di chiusura, avete così una panoramica dei sistemi di chiusura che hanno già ricevuto la modifica dell'autorizzazione e di quelli che non l'hanno ricevuta, che vi permette di conoscere le condizioni del vostro impianto di chiusura.

3.3.3 ID di blocco (Lock priority)

Assegnate e revocate le autorizzazioni nell'LSM o bloccate e disattivate i supporti di identificazione e trasferite le modifiche delle autorizzazione ai sistemi di chiusura con un gateway tramite supporti di identificazione.

Normalmente, in una rete virtuale, vengono utilizzate le autorizzazioni memorizzate sui supporti di identificazione stessi. Se un supporto di identificazione deve essere bloccato e le autorizzazioni su questo supporto di identificazione continuano ad essere utilizzate, esso potrebbe continuare ad aprire i sistemi di chiusura finché le autorizzazioni su di esso non vengono modificate da un gateway.

Ciò è impedito da una Lock Priority impostata per l'ID del supporto di identificazione. Se un supporto di identificazione non è più autorizzato per una serratura, viene impostata una Lock Priority per il suo ID. Il gateway trasmette la Lock Priority alle chiusure tramite altri supporti di identificazione.

Se in un sistema di chiusura viene impostata una Lock Priority per un ID di un supporto di identificazione, l'autorizzazione che può ancora esistere su questo supporto di identificazione, e che viene normalmente utilizzata, viene ignorata. Si applicano invece le autorizzazioni memorizzate nella chiusura stessa e aggiornate in una rete virtuale dal supporto di identificazione (e quindi più attuali).

Allo stesso tempo, l'ID del supporto di identificazione così bloccato viene memorizzato in una blacklist e non può essere riattivato accidentalmente.

3.3.4 Data di scadenza (Expiry date)

Per un uso efficace della rete virtuale, è necessario che il gateway possa regolarmente trasferire dati da e verso il supporto di identificazione. In qualità di amministratore di un impianto di chiusura, potete “forzare" gli utenti del vostro impianto di chiusura ad attivare regolarmente i loro supporti di identificazione sul gateway con una data di scadenza.

Una data di scadenza limita la validità di un supporto di identificazione. Gli utenti devono ricaricare regolarmente il loro credito di tempo su un gateway, altrimenti non possono utilizzare alcuna chiusura (comprese le chiusure offline) fino a quando non ricaricano il loro credito di tempo presso un gateway. Ci sono due opzioni per questo credito di tempo:

- Numero fisso di ore tra una e 255 ore (ad es. autorizzazione per otto ore dopo la ricarica)
- Orario di scadenza fisso tra 1:00 e 24:00 (es. autorizzazione tra l'orario di ricarica e le 20:00)

Questo credito di tempo viene impostato in LSM a livello globale per tutti i supporti di identificazione. Tuttavia, è anche possibile definire un credito di tempo individuale per i singoli transponder. Modifiche generali (ad esempio, la durata del credito di tempo) vengono programmate direttamente con l'LSM.

3.3.5 Impostazione dell'ora

Le chiusure e i transponder contengono un modulo orario. Se un transponder viene utilizzato su un gateway, il modulo orario nel transponder viene resettato (e vengono corretti eventuali tempi precedenti o successivi nel transponder). Il tempo nel transponder funge da riferimento per l'azionamento di una chiusura. Se l'orario della chiusura è diverso durante l’azionamento, il modulo orario della chiusura viene resettato in base all'orario del transponder (e corretto nella chiusura, se necessario, con l'orario precedente o successivo).

L'orario delle chiusure nella vostra rete virtuale viene automaticamente ripristinato regolarmente senza che voi, in qualità di amministratore dell'impianto di chiusura, dobbiate riprogrammare manualmente i sistemi di chiusura.

3.4 Controllo delle fasce orarie

Con la regolazione delle fasce orarie, è possibile limitare il periodo (fascia oraria) in cui determinati supporti di identificazione (e quindi persone o gruppi di persone) possono attivare una chiusura (e quindi, ad esempio, entrare nell'edificio).

3.4.1 Fasce orarie

È possibile creare qualsiasi piano di fasce orarie e assegnare un piano di fasce orarie ad ogni area individualmente. Un piano di fasce orarie contiene fino a cento gruppi di fasce orarie che possono essere liberamente configurati con diversi orari di accesso. È possibile selezionare o configurare i gruppi di fasce orarie in modo diverso nei vari piani.

3.4.2 Festività

Oltre ai sette giorni feriali (dal lunedì alla domenica), è possibile inserire nei piani delle fasce orarie anche giorni festivi o speciali.

Per fare questo, è sufficiente utilizzare le liste delle festività memorizzate nel software LSM (per tutti gli stati federali tedeschi) invece di crearle da soli. In alternativa, è possibile creare le proprie liste di festività indipendentemente dalle liste fornite. Ogni giorno può essere salvato come giorno festivo e può essere trattato come una domenica (vedere anche *Giorni speciali [▸ 13]*).

3.4.3 Giorni speciali

Un giorno speciale definisce un profilo temporale per determinati giorni che è indipendente dai sette giorni della settimana. I giorni speciali hanno una priorità maggiore rispetto ai giorni festivi.

Con i giorni speciali, ad esempio, è possibile consentire l'accesso al personale scolastico durante l'orario scolastico dal lunedì al venerdì e generalmente bloccare l'accesso durante le vacanze con giorni speciali (a priorità più elevata).

3.4.4 Data di validità (Validation date)

È possibile assegnare qualsiasi data di validità ai transponder. I transponder con data di validità possono essere utilizzati nell'impianto di chiusura solo a decorrere da questa data.

Questa funzione è indipendente dalla rete virtuale (vedere *Data di scadenza (Expiry date) [▸ 12]*) e può essere modificata esclusivamente mediante un dispositivo di programmazione. Non utilizzare questa funzione in connessione con la rete virtuale.

3.4.5 Data di scadenza (Expiry date)

È possibile assegnare una data di scadenza a scelta ai transponder. I transponder con data di scadenza non possono più essere utilizzati nell'impianto di chiusura a decorrere da tale data.

Questa funzione è indipendente dalla rete virtuale (vedere *Data di scadenza (Expiry date) [▸ 12]*) e può essere modificata esclusivamente mediante un dispositivo di programmazione. Non utilizzare questa funzione in connessione con la rete virtuale.

3.5 Elenchi

3.5.1 Elenchi degli accessi

Le chiusure con funzione ZK registrano gli accessi in una lista degli accessi:

- Data
- Ora
- ID del supporto di identificazione
- Nome dell'utente

È possibile leggere e visualizzare l'elenco degli accessi con il software LSM. Il numero di voci nell'elenco degli accessi dipende dalla chiusura e dalla configurazione.

	Standard	Gateway
Cilindro	Fino a 3000	
SmartHandle	Fino a 3000	
Smart Relè	Fino a 3600	Fino a 200

In un sistema di chiusura in rete, è possibile anche automatizzare il processo di lettura (vedere Lettura della chiusura).

3.5.2 elenchi di transiti

I transponder G2 registrano gli accessi indipendentemente dall'elenco di transiti. In questo elenco di transiti sono memorizzati gli ultimi transiti (fino a 1000):

- Data
- Ora
- ID della chiusura

È possibile leggere e visualizzare l'elenco di transiti con il software LSM.

3.6 Generazioni di protocolli

3.6.1 Impianti di chiusura G1

Negli impianti di chiusura G1 possono essere utilizzati solo i prodotti G1 e solo le funzioni G1.

Se si utilizzano record di dati G1 nei transponder G2, le funzioni Expiry dei protocolli G1 (ad esempio, con terminali di validazione) non sono supportate.

NOTA

I prodotti G1 sono fuori produzione

I prodotti G1 non sono più disponibili.

3.6.2 Impianti di chiusura G2

Negli impianti di chiusura G2 possono essere utilizzati solo i prodotti G2 e solo le funzioni G2.

3.6.3 Impianti di chiusura G1 e G2 separati

Questo approccio consente di separare le diverse generazioni di protocolli in (almeno) due diversi impianti di chiusura. Ogni supporto di identificazione memorizza (minimo) due record di dati indipendenti dell'impianto di chiusura (uno per G1 e uno per G2).

Il vantaggio di questo approccio evita fin dall'inizio problemi di compatibilità.

Questi impianti di chiusura vengono gestiti nello stesso piano di chiusura o nella stessa banca dati. A partire da LSM 3.0 è possibile filtrare la visualizzazione nella matrice in base alla generazione del protocollo e, a seconda del filtro, vedere solo le chiusure e i supporti di identificazione per G1 o G2.

3.6.4 Sistemi di chiusura G1 e G2 misti (modo compatibilità)

Questo approccio consente di gestire le due diverse generazioni di protocolli nello stesso impianto di chiusura.

- I prodotti G1 continuano ad utilizzare solo le funzioni G1.
- I prodotti G2 funzionano in modalità di compatibilità.

È sufficiente gestire un unico impianto di chiusura, ma la mescolanza di G1 e G2 limita la chiarezza e la differenziazione.

NOTA

Limitazioni funzionali dovute al funzionamento misto

L'uso di sistemi misti può portare a limitazioni funzionali e richiede esperienza.

1. Evitare impianti di chiusura misti.
2. Utilizzare invece impianti di chiusura separati (vedere *Impianti di chiusura G1 e G2 separati [▸ 15]*).

3.7 Avvisi batteria

Gli avvisi batteria dei cilindri con protocollo G2 sono identici a quelli dei cilindri con protocollo G1 (eccezione: cilindro Mifare, vedere i rispettivi manuali / brevi istruzioni).

3.7.1 Transponder per cambio batteria G2

I cilindri con batterie molto scariche non possono più essere utilizzati con i normali supporti di identificazione per evitare una scarica completa (G1: modo conservazione, G2: modalità Freeze).

La modalità di conservazione e gli avvisi batteria per i cilindri con protocollo G1 possono essere cancellati solo con il dispositivo di programmazione locale.

A partire da LSM 3.0, il protocollo G2 abilita i cosiddetti transponder per cambio batteria. Con un transponder per il cambio batteria è possibile disattivare la modalità di blocco dei cilindri di chiusura G2 e azionare la serratura con un normale transponder autorizzato. Per fare questo non è necessario essere sul posto presso la chiusura con il dispositivo di programmazione.

ATTENZIONE

Scaricamento delle batterie per uso scorretto

Ad ogni apertura con un transponder per sostituzione batteria, la batteria si scarica ulteriormente. In caso di utilizzo non appropriato, ciò può causare lo scaricamento completo delle batterie! Sostituire immediatamente le batterie che si trovano in tali condizioni.

4. Prodotti G2

Se si desidera utilizzare tutte le funzioni dei protocolli G2, è possibile utilizzare solo prodotti G2. Informazioni sulla disponibilità dei prodotti G2 sono disponibili nel listino prezzi attuale di SimonsVoss.

4.1 Dispositivi di programmazione

Per programmare i componenti G2 è necessario un dispositivo di programmazione con un firmware adeguato:

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

Il firmware è retrocompatibile. È inoltre possibile utilizzare dispositivi di programmazione con un nuovo firmware per programmare i precedenti componenti G1.

4.2 Cilindro

Prodotto	G1 compatibile	G2 compatibile
Cilindro standard (25 kHz)	Sì	Sì
Cilindro Mifare/Smart-Card	No	Sì

4.3 SmartHandle

Prodotto	G1 compatibile	G2 compatibile
SmartHandle 3062 Standard (25 kHz)	Sì	Sì
SmartHandle 3062 Mifare/SmartCard	No	Sì
SmartHandle AX Standard (25 kHz)	Sì	Sì
SmartHandle AX Mifare/SmartCard	No	Sì

4.4 Smart Relè

Prodotto	G1 compatibile	G2 compatibile
Smart Relè	Sì	Sì
Smart Relè 2	Sì	Sì

Prodotto	G1 compatibile	G2 compatibile
Smart Relè 3	Sì	Sì

4.5 Transponder

Tutti i transponder sono disponibili come prodotto G2.

4.6 Rete (WaveNet)

La vostra WaveNet (RouterNodes e LockNodes) può interloquire con i prodotti G1 e G2. I LockNode esterni sono parzialmente supportati anche nei componenti G2.

	Sorveglianza porta	Riprogrammazione
LockNodes interni	Sì	Sì
LockNodes esterni	Sì	No

5. Segnalazione

Si distingue tra segnalazione transponder (ad es. OK) e segnalazione di stato (ad es. avviso batteria).

5.1 Transazione

Funzione	Descrizione	Segnalazione
La transazione è ok La chiusura si accoppia	La chiusura si accoppia	2x breve
La chiusura si disaccoppia	La chiusura si disaccoppia	1x breve
Modalità Flip-Flop (si accoppia)	La chiusura si accoppia	1x breve, 1x lungo
Modalità Flip-Flop (si disaccoppia)	La chiusura si disaccoppia	1x lungo, 1x breve
L'operazione non può essere eseguita	La chiusura è disattivata	1x breve
	La chiusura è in modalità Freeze	1x breve
	Il supporto di identificazione non è valido	1x breve

I prodotti G2 utilizzano un segnale difensivo per indicare all'utente che il suo supporto di identificazione non è autorizzato.

5.2 Stato

Funzione	Descrizione	Segnalazione
Stato critico della batteria della chiusura	Livello di avviso batteria 1	8x breve (prima di accoppiarsi)
Stato critico della batteria della chiusura (la chiusura è nella modalità Flip-Flop)	Livello di avviso batteria 1	Ogni 60 secondi circa 4x doppio e breve
Stato critico della batteria della chiusura	Livello di avviso batteria 2	8x breve con un secondo di pausa per 30 secondi (prima di accoppiarsi)
Stato critico della batteria della chiusura	Modalità Freeze	6x lunga-breve

Funzione	Descrizione	Segnalazione
Stato critico della batteria del transponder		8x doppio e breve (dopo il disaccoppiamento)
Procedura di programmazione		1x breve (in funzione dei dati di programmazione)
Riavvio (Power-On-Reset)		3x breve

È possibile disattivare gli avvisi batteria acustici per i cilindri. In questo stato, il cilindro non segnala più le batterie scariche agli utenti.

5.3 Possibilità di configurazione

5.3.1 Procedure di programmazione

È possibile disattivare la segnalazione lato chiusura di una programmazione.

5.3.2 Apertura

È possibile disattivare la segnalazione acustica lato chiusura di una programmazione per i singoli supporti di identificazione. Questa disattivazione vale per questo supporto di identificazione in tutto l'impianto di chiusura.

6. Ampliamento

6.1 Ampliamento G1

I dispositivi G1 non sono più disponibili. Se fino ad ora avete utilizzato un impianto di chiusura G1 e avete bisogno di nuovi dispositivi, ampliate il vostro impianto di chiusura G1 con un impianto di chiusura G2. Gli impianti di chiusura possono essere gestiti separatamente (vedere *Impianti di chiusura G1 e G2 separati [▸ 15]*) oppure combinati (vedere *Sistemi di chiusura G1 e G2 misti (modo compatibilità) [▸ 15]*).

Una possibile rete virtuale, una rete parziale o una rete completa aumenta il comfort e può essere adattata in qualsiasi momento (vedi *Differenze: collegamenti in rete [▸ 22]*).

6.2 Ampliamento G2

Potete estendere e riprogrammare in qualsiasi momento il vostro impianto di chiusura G2 secondo i vostri desideri fino ai limiti dei protocolli G2.

Una possibile rete virtuale, una rete parziale o una rete completa aumenta il comfort e può essere adattata in qualsiasi momento (vedi *Differenze: collegamenti in rete [▸ 22]*).

7. Differenze: collegamenti in rete

	WaveNet (online)	Rete virtuale (virtuale)	Nessun collegamento (offline)
Principio di funzionamento	Trasmissione dati con dispositivi WaveNet collegati in rete (vedere Linee di trasmissione e Dispositivi).	Trasmissione dei dati con supporti di identificazione (ad eccezione dei dati di programmazione).	Trasmissione dei dati con dispositivi di programmazione.
Diffusione	I dispositivi WaveNet sono collegati tramite diversi supporti di trasmissione. Tutti i tipi di dati sono trasmessi utilizzando questi supporti di trasmissione.	Nella rete virtuale, alcuni dati vengono trasferiti ai supporti di identificazione tramite un gateway (voci nella blacklist). Se si utilizzano questi supporti di identificazione su una chiusura virtualmente collegata in rete, i dati vengono trasferiti alla chiusura.	Le serrature non collegate in rete possono scambiare dati solo con l'apparecchio di programmazione. È necessario recarsi alle chiusure con il dispositivo di programmazione.
Sforzo di programmazione	Ridotto.	Ridotto.	Lo sforzo dipende dalle dimensioni dell'impianto di chiusura. - Impianto di chiusura di piccole dimensioni: sforzo ridotto. - Impianto di chiusura di medie dimensioni: sforzo medio. - Impianto di chiusura di grandi dimensioni: grande sforzo.
Velocità di trasmissione nello scambio dei dati	Immediato. Scambio di dati con diversi supporti di trasmissione.	La velocità tra il gateway e le chiusure dipende in larga misura dall'intensità di utilizzo delle chiusure. I supporti di identificazione sono supporti di trasmissione - nessuna trasmissione di dati senza identificazione.	Lenta.

	WaveNet (online)	Rete virtuale (virtuale)	Nessun collegamento (offline)
Attivazione/disattivazione centralizzata delle chiusure	Possibile.	Non possibile.	Non possibile.
Attivazione/disattivazione tracciabile a livello centrale	Possibile.	Non possibile.	Non possibile.
Apertura a distanza	Possibile.	Non possibile.	Non possibile.
Monitoraggio a distanza (DoorMonitoring)	Possibile.	Non possibile.	Non possibile.
Gestione eventi	Possibile.	Non possibile.	Non possibile.
Elenchi di accesso richiamabili a livello centrale	Possibile.	Non possibile (ad eccezione di SREL 3).	Non possibile.
Funzioni di protezione indipendenti da software/server	Possibile.	Non possibile.	Non possibile.
Reazione immediata dell'intero impianto di chiusura in situazioni critiche (disponibilità di funzioni di protezione, vedere Configurazione I/O e funzioni di protezione e RingCast)	Possibile.	Non possibile.	Non possibile.

8. Allegato

8.1 Differenze tra i protocolli G1 e G2

	G1	G2	G2 (collegato in una rete virtuale)
Chiusure	16000	64000	64000
Supporti di identificazione	8000	64000	64000
Gruppi fasce temporali	5+1	100+1	100+1
Informazioni di base	Supporti di identificazione		Chiusure
Informazioni sul piano di chiusura	Chiusure	Chiusure o supporti di identificazione	Supporti di identificazione
Gateway (online)	No	No	Sì
Rete	Sì	Sì	Sì (solo gateway)

Se si utilizzano i protocolli G2 senza rete virtuale, si può decidere per ogni esigenza di programmazione se si desidera programmare il supporto di identificazione o la chiusura. Le chiusure possono memorizzare un elenco di supporti di identificazione e i supporti di identificazione un elenco di chiusure.

8.2 Glossario

Termine	Spiegazione
ASM	Monitoraggio dello stato dell'impianto
Area	Raggruppamento di più chiusure per una più facile gestione delle autorizzazioni
Elenco di transiti	Elenco delle chiusure percorse, memorizzate sul supporto di identificazione
Banca dati	Memorizzazione di tutte le informazioni del piano di chiusura o dell'impianto di chiusura del sistema 3060

Termine	Spiegazione
Collegamento diretto in rete (LockNode Inside)	Nodo di rete (LockNode) direttamente integrato nella chiusura
Gateway	Collegamento della rete virtuale al software LSM
G1	Vecchia generazione del protocollo dell'interfaccia del campo B
G2	Generazione corrente del protocollo dell'interfaccia del campo B
LID	Lock-ID: Identificatore unico di una chiusura in un impianto di chiusura SimonsVoss
LSM	Locking System Management: Software per PC supportato da database per la gestione dell'impianto di chiusura SimonsVoss
LockNode	Nodo di rete per la Near Field Communication diretta con una chiusura
Meccanico attivo	(=accoppiato) Stato meccanico di una chiusura che permette all'utente di aprirla e chiuderla.
Meccanico inattivo	(=disaccoppiato) Stato meccanico di una chiusura che non permette all'utente di aprirla e chiuderla.
Rete	SimonsVoss WaveNet. Le chiusure possono essere azionate in modalità online (= in rete).
Impianto di chiusura	Set di serrature e supporti di identificazione correlati e gestiti congiuntamente
Password del sistema di chiusura	Password per la protezione dell'impianto di chiusura
Piano di chiusura	Un piano di chiusura può essere composto da più impianti di chiusura
SID	ID impianto di chiusura: Identificatore unico di un impianto di chiusura in un piano di chiusura SimonsVoss

Termine	Spiegazione
Chiusura	Termine generico per tutti i prodotti che possono interloquire con un supporto di identificazione.
SmartCD	Dispositivo di programmazione: I prodotti SimonsVoss sono programmati utilizzando uno SmartCD
TID	ID transponder: Identificatore unico di un supporto di identificazione in un impianto di chiusura SimonsVoss
Transponder	Mezzo in grado di comunicare con una chiusura
Gruppi di transponder	Raggruppamento di diversi supporti di identificazione in un unico gruppo per poter gestire più facilmente le autorizzazioni
Rete virtuale	La tecnologia con la quale le modifiche di autorizzazione vengono distribuite attraverso i gateway in caso di chiusure offline e le chiusure non devono essere cercate.
Gruppi fasce temporali	Gruppi come parte di un piano di fasce orarie
Piani di fasce orarie	Piano di fasce orarie che può essere salvato nella chiusura
Elenchi degli accessi	Elenco dei transiti memorizzati nella chiusura (prerequisito: ZK)
Profilo di accesso (gruppi di transponder / aree)	Definisce il numero di chiusure che possono interloquire con un supporto di identificazione su cui si trova questo profilo.

9. Supporto e ulteriori informazioni

Materiale informativo/Documenti

Maggiori informazioni sul funzionamento e sulla configurazione nonché ulteriori documenti sono riportati nella homepage:

https://www.simons-voss.com/it/documenti.html

Dichiarazioni di conformità

Le dichiarazioni di conformità e altri certificati sono riportate nella homepage:

https://www.simons-voss.com/it/certificati.html

Supporto tecnico

Il nostro supporto tecnico sarà lieto di aiutarvi (linea fissa, i costi dipendono dal provider):

+49 (0) 89 / 99 228 333

E-mail

Se si preferisce contattarci via e-mail, scrivere all'indirizzo:

support-simonsvoss@allegion.com

FAQ

Per informazioni e consigli utili, consultare l'area FAQ:

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

Indirizzo

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Germania

Ecco a voi SimonsVoss

SimonsVoss, pioniere della tecnologia di chiusura radiocomandata senza fili, offre soluzioni di sistema con un'ampia gamma di prodotti per il settore SOHO, per le piccole e grandi imprese e le istituzioni pubbliche. Gli apparati SimonsVoss racchiudono funzionalità intelligenti, alta qualità e design pluripremiato Made in Germany.

Come fornitore di prodotti innovativi, SimonsVoss punta su scalabilità, alta sicurezza, affidabilità, software potenti e facilità d'uso. Questo rende SimonsVoss un leader tecnologico riconosciuto nell'ambito dei sistemi di chiusura digitali wireless.

Coraggio di innovare, mentalità e agire sostenibile e grande attenzione verso collaboratori e clienti: questa è la chiave del nostro successo.

SimonsVoss fa parte di ALLEGION, un gruppo internazionale operante nel settore della sicurezza. Allegion vanta sedi in circa 130 paesi (www.allegion.com).

Qualità "made in Germany"

Per SimonsVoss, il "Made in Germany" è un impegno serio: Tutti i prodotti sono sviluppati e realizzati esclusivamente in Germania.

SimonsVoss technologies

Made in Germany

A BRAND OF ALLEGION