G2-Protokolle

Handbuch

29.08.2020

SimonsVoss technologies

Inhaltsverzeichnis

1 Allgemeine Sicherheitshinweise

Signalwort (ANSI Z535.6)	Mögliche unmittelbare Auswirkungen bei Nicht-beachtung
Gefahr	Tod oder schwere Verletzung (wahrscheinlich)
Warnung	Tod oder schwere Verletzung (möglich, aber unwahrscheinlich)
Vorsicht	Leichte Verletzung
Achtung	Sachschäden oder Fehlfunktionen
Hinweis	Geringe oder keine

WARNUNG

Versperrter Zugang

Durch fehlerhaft montierte und/oder programmierte Komponenten kann der Zutritt durch eine Tür versperrt bleiben. Für Folgen eines versperrten Zutritts wie Zugang zu verletzten oder gefährdeten Personen, Sachschäden oder anderen Schäden haftet die SimonsVoss Technologies GmbH nicht!

Versperrter Zugang durch Manipulation des Produkts

Wenn Sie das Produkt eigenmächtig verändern, dann können Fehlfunktionen auftreten und der Zugang durch eine Tür versperrt werden.

- Verändern Sie das Produkt nur bei Bedarf und nur in der Dokumentation beschriebenen Art und Weise.

HINWEIS

Bestimmungsgemäßer Gebrauch

SimonsVoss-Produkte sind ausschließlich für das Öffnen und Schließen von Türen und vergleichbaren Gegenständen bestimmt.

- Verwenden Sie SimonsVoss-Produkte nicht für andere Zwecke.

Abweichende Zeiten bei G2-Schließungen

Die interne Zeiteinheit der G2-Schließungen hat eine technisch bedingte Toleranz von bis zu ± 15 Minuten pro Jahr.

Qualifikationen erforderlich

Die Installation und Inbetriebnahme setzt Fachkenntnisse voraus.

- Nur geschultes Fachpersonal darf das Produkt installieren und in Betrieb nehmen.

Die deutsche Sprachfassung ist die Originalbetriebsanleitung. Andere Sprachen (Abfassung in der Vertragssprache) sind Übersetzungen der Originalbetriebsanleitung.

Lesen Sie alle Anweisungen zur Installation, zum Einbau und zur Inbetriebnahme und befolgen Sie diese. Geben Sie diese Anweisungen und jegliche Anweisungen zur Wartung an den Benutzer weiter.

2 Allgemeines

Die G2-Protokolle sind eine komplette Neuentwicklung der SimonsVoss-Kommunikation zwischen Identifikationsmedien und Schließungen. Viele neue Funktionen wurden implementiert, damit Sie noch einfachere und noch bessere Möglichkeiten zur Verwaltung Ihrer Schließanlage haben.

Basierend auf den G2-Protokollen stehen Ihnen passende Hardwareprodukte und eine vollständig modulare Software zur Verfügung, um Ihre Schließanlage noch besser an Ihre persönlichen Bedürfnisse anzupassen.

3 G2-Protokolle

3.1 Allgemeine Beschreibung

Die G2-Protokolle ermöglichen im System 3060 neue Funktionen, wenn die Voraussetzungen dafür erfüllt sind:

- LSM ab Version 3.0
- G2-Hardwareprodukte

3.1.1 Schließanlagenpasswort

Sie benötigen das Schließanlagenpasswort nur noch bei der Erstellung des Schließplans. Außerdem ist die Sicherheit des Schließanlagenpassworts erhöht:

- Minimale Länge 64 Bit
- Integrierter Qualitätsindex in der LSM-Software

Die LSM-Software lässt unsichere Schließanlagenpasswörter also nicht mehr zu und erhöht die Sicherheit Ihrer Schließanlage.

3.1.2 Schließanlagengröße

Die G2-Protokolle definieren die Grenzen Ihrer Schließanlage neu. Sie können jetzt

- bis zu 64000 Schließungen pro Schließanlage
- Bis zu 64000 Identifikationsmedien pro Schließung

verwalten. Über vier Milliarden mögliche Einzelberechtigungen pro Schließanlage ermöglichen die kompromisslose Anpassung Ihrer Schließanlage an Ihre individuellen Bedürfnisse.

3.1.3 Übergreifende Schließebenen

Sie können übergreifende Schließebenen verwenden, um bestimmte Funktionen in mehreren Schließanlagen zu verwenden. Diese Funktionen sind durch ein eigenes, von der Schließanlage unabhängiges, Passwort gesichert (sogenannte Querschließanlagen). Ihnen stehen drei übergeordnete Schließebenen zur Verfügung:

- Rote Schließebene
- Grüne Schließebene
- Blaue Schließebene

Ein Transponder kann jeweils zu einer der drei Ebenen gehören. In der LSM sind für jede übergeordnete Schließebene 1024 Transponder-IDs reserviert. Das bedeutet, dass Sie einer übergeordneten Schließebene maximal 1024

Transponder zuordnen können. Für jeden dieser Transponder können Sie individuelle Berechtigungen vergeben oder die Transponder individuell sperren.

Transponder, die Sie der roten Schließebene zugeordnet haben, können auch deaktivierte Schließungen öffnen. Diese bleiben für die eingestellte Impulsdauer eingekuppelt bzw. geöffnet, sind aber weiterhin deaktiviert. Wenn Sie einen Transponder der roten Schließebene zum Beispiel in einem Feuerwehrschlüsseldepot hinterlegen, dann können Rettungskräfte im Gefahrenfall im Gebäude schnell vorrücken.

3.1.4 Notfreischaltung

Wenn Sie Ihre Schließanlage vernetzt haben, dann können Sie Ihre Schließungen über Ihr Netzwerk (WaveNet) freischalten. Dazu versenden Sie aus der LSM-Software über das Netzwerk an die gewünschten Schließungen einen Befehl, der die Schließungen dauerhaft einkuppelt. Jeder kann unabhängig von Identifikationsmedien diese Schließungen begehen.

Schließungen, die Sie über den Befehl zur Notfreischaltung geöffnet haben, bleiben solange geöffnet, bis Sie die Notfreischaltung durch einen Befehl zur Notöffnung oder einen Befehl zur Fernöffnung aufheben.

Eine Brandmeldeanlage kann über einen Kontakt in der LSM-Software ein Ereignis auslösen, dessen Reaktion diesen Befehl verschickt. Im Brandfall werden so alle Schließungen, die den Befehl empfangen, geöffnet. Eingeschlossene Personen können das Gebäude verlassen und Rettungskräfte im Gebäude schnell vorrücken.

Berechtigte Identifikationsmedien, die an notfreigeschalteten Schließungen verwendet werden, haben keine Funktion.

3.1.5 Notöffnung

Sie können in der LSM-Software während des Exports auf die LSM Mobile ein temporäres Passwort vergeben. Dieses Passwort muss mindestens acht Zeichen lang sein, hat aber keine weiteren Einschränkungen.

Mit diesem Passwort kann dann vor Ort eine Notöffnung an einer Schließung durchgeführt werden, ohne dass dazu das Schließanlagenpasswort bekannt sein muss.

Aus Sicherheitsgründen können Sie als Administrator diese Funktion einschränken:

- Anzahl möglicher Notöffnungen
- Zeitraum, in dem die Notöffnungen möglich sind

3.1.6 Pulslänge

Sie können für Schließzylinder und SmartRelais Einkuppelzeiten zwischen einer und 25 Sekunden frei wählen.

Gleichzeitig können Sie mit der LSM-Funktion "Langes Öffnen" einzelnen Identifikationsmedien eine längere Einkuppelzeit zugestehen. Diese Funktion verdoppelt die Einkuppelzeit, wobei die Gesamteinkuppelzeit weiterhin auf 25 Sekunden begrenzt ist.

Einkuppelzeiten für alle Schließungen beeinflussen	Pulslänge in der Konfiguration der Schließung
Einkuppelzeiten für einzelne Identifikationsmedien beeinflussen	"Langes Öffnen" in der Konfiguration des Identifikationsmediums

3.1.7 Akustisches Öffnungssignal

Schließungen geben ein akustisches Öffnungssignal ab. Dieses akustische Öffnungssignal kann störend sein, zum Beispiel in einem Krankenhaus. Das nächtliche Öffnen von Türen würde mit einem akustischen Öffnungssignal die Patienten wecken.

Sie können dieses akustische Öffnungssignal identifikationsmediumsbezogen deaktivieren. Damit schalten Sie Schließungen für einzelne oder für alle Identifikationsmedien stumm.

3.2 Berechtigungsvergabe

3.2.1 Allgemeines

Die neuen G2-Protokolle reduzieren Ihren Verwaltungsaufwand nach der Ausgabe neuer Identifikationsmedien. Intelligente Mechanismen in den Protokollen vermeiden das bisher notwendige Umprogrammieren Ihrer Schließungen vor Ort weitgehend.

Alternativ zur Umprogrammierung Ihrer Schließungen vor Ort können Sie die Berechtigungen auch wie folgt an Ihre Schließungen übertragen:

- G2 ohne Vernetzung
  - Direkte Übertragung: Über Identifikationsmedien und Schließungen
  - Sperrungen: Über Ersatz-Identifikationsmedien
- Indirekte Übertragung: G2 mit virtueller Vernetzung (VN), siehe *Virtuelles Netzwerk (VN) [▸ 11]*
- Netzwerkübertragung: WaveNet

3.2.2 G2 ohne Vernetzung

Wenn Sie eine G2-Schließanlage unvernetzt verwenden, dann sparen Sie beim Anlegen neuer Schließungen oder neuer Identifikationsmedien viel Zeit. Sie müssen mit den G2-Protokollen in diesem Fall nicht mehr Identifikationsmedien und Schließungen programmieren:

Neue Schließung	■ Speichern Sie die Berechtigungen auf dem Identifikationsmedium (Programmieren des Identifikationsmediums) oder ■ Speichern Sie die Berechtigungen in der Schließung (Programmieren der Schließung)
Neues Identifikationsmedium	

Es entsteht kein weiterer Programmieraufwand in Ihrer Schließanlage. Ihnen steht als Schließanlagenadministrator ein vollständig offenes System zur Verfügung. Sie können bei der Programmierung entscheiden, ob Sie die Berechtigungen auf dem Identifikationsmedium oder in der Schließung speichern - je nachdem, was für Sie komfortabler ist.

Schließungen

Sie können in jeder Schließung bis zu 64000 Identifikationsmedien verwalten, d.h. individuell berechtigen und sperren. Der Programmiervorgang ist prinzipiell mit dem Programmiervorgang der G1-Schließungen identisch. In jeder G2-Schließanlage können bis zu 64000 Schließungen gespeichert und verwaltet werden.

Identifikationsmedien

Sie können in Ihren G2-Schließanlagen in jedem Identifikationsmedium individuell speichern, für welche Schließungen dieses Identifikationsmedium berechtigt ist. Die neuen G2-Transponder können bis zu drei G1-Schließanlagen und vier G2-Schließanlagen speichern und verwalten - somit kann in G2-Schließanlagen der gesamte Schließplan auf dem Transponder gespeichert werden.

Ersatztransponder und Sperr-IDs

Mit der Einführung der LSM 3.0 SP2 können Sie mit Ersatz-Identifikationsmedien auch gleich andere Identifikationsmedien (die beispielsweise gestohlen wurden) sperren. Wenn Sie das Ersatz-Identifikationsmedium programmieren, dann wählen Sie das zu sperrende Identifikationsmedium aus und übertragen eine Sperr-ID auf das Identifikationsmedium. Sobald das Ersatz-Identifikationsmedium an einer

Schließung betätigt wird, überträgt das Ersatz-Identifikationsmedium die Sperr-ID an die Schließung und das zu sperrende Identifikationsmedium ist an dieser Schließung nicht mehr berechtigt.

Der Programmierbedarf an den Schließungen bleibt bestehen und wird erst aufgehoben, wenn Sie die Schließungen, an denen das zu sperrende Identifikationsmedium bisher berechtigt war, nachprogrammieren.

3.3 Virtuelles Netzwerk (VN)

In einem virtuellen Netzwerk werden den Schließungen bei der Erstprogrammierung nur noch grundsätzliche Informationen mitgeteilt und in Ihrer Schließanlage zugelassen. Die Berechtigungen werden ausschließlich auf den Identifikationsmedien gespeichert.

Wenn sich die Berechtigungen ändern, dann müssen die Berechtigungen nur in den Identifikationsmedien aktualisiert werden. In virtuellen Netzwerken gibt es dafür sogenannte Gateways. Die Benutzer betätigen die Identifikationsmedien an den Gateways und beginnen so die Datenübertragung. Wenn Berechtigungsänderungen vorliegen, dann aktualisiert das Gateway in den Identifikationsmedien die Berechtigungen. Als Schließanalgenadministrator müssen Sie so keine Schließungen oder Identifikationsmedien mehr umprogrammieren, wenn Sie die Berechtigungen ändern.

3.3.1 Gateways

Die Gateways stehen als Online-Variante zur Verfügung. In einem SimonsVoss-Netzwerk werden Daten zwischen Gateway und Identifikationsmedium übertragen:

- Berechtigungsänderungen (positiv und negativ) vom Gateway auf das Identifikationsmedium
- Sperr-IDs vom Gateway auf das Identifikationsmedium
- Auf den Identifikationsmedien gespeicherte Quittungen der Schließanlage vom Identifikationsmedium an das Gateway

Die Programmierung der Schließungen mittels Programmiergerät entfällt. Stattdessen wird die Schließanlage über die Gateways bzw. die Nutzer der Identifikationsmedien umprogrammiert.

Sie können mit der LSM SmartRelais als mögliche Gateways für Ihre Schließanlage einsetzen.

3.3.2 Direkte Berechtigungen

An den Gateways übertragene Berechtigungsänderungen löschen bzw. vergeben Berechtigungen direkt im Identifikationsmedium neu und sind deshalb sofort wirksam. Wenn Sie Identifikationsmedien sperren wollen,

dann können die Gateways diese Information (Sperr-ID) auch auf die Identifikationsmedien übertragen. Die Nutzer der Identifikationsmedien übertragen mit ihren Identifikationsmedien diese Information dann an die Schließungen Ihrer Schließanlage.

Die Schließung speichert den erfolgreichen Empfang von Berechtigungsänderungen durch ein Identifikationsmedium als Feedback auf nachfolgenden Identifikationsmedien (Quittungsmanagement). Die Nutzer der Identifikationsmedien tragen dieses Feedback anschließend wieder zum Gateway zurück. Das Gateway speichert die erfolgreiche Übertragung in der Datenbank und die LSM zeigt an den entsprechenden Schließungen keinen Programmierbedarf mehr an.

Als Schließanlagenadministrator behalten Sie so den Überblick darüber, welche Schließungen die Berechtigungsänderung bereits erhalten haben und welche nicht. Sie kennen den Zustand Ihrer Schließanlage.

3.3.3 Sperr-IDs (Lock priority)

Sie vergeben und entziehen Berechtigungen in der LSM bzw. sperren und deaktivieren Identifikationsmedien und übertragen die Berechtigungsänderungen mit einem Gateway über Identifikationsmedien auf die Schließungen.

Normalerweise werden in einem virtuellen Netzwerk die auf den Identifikationsmedien selbst hinterlegten Berechtigungen verwendet. Wenn ein Identifikationsmedium gesperrt werden soll und weiterhin die Berechtigungen auf diesem Identifikationsmedium verwendet werden, dann könnte dieses Identifikationsmedium weiterhin Schließungen öffnen, solange die Berechtigungen auf diesem Identifikationsmedium nicht durch ein Gateway geändert werden.

Das wird durch eine für die ID des Identifikationsmediums gesetzte Lock priority verhindert. Wenn ein Identifikationsmedium an einer Schließung nicht mehr berechtigt ist, dann wird für dessen ID eine sogenannte Lock priority gesetzt. Das Gateway überträgt die Lock priority über andere Identifikationsmedien an die Schließungen.

Wenn in einer Schließung für eine ID eines Identifikationsmediums eine Lock priority gesetzt ist, dann wird die ggfs. auf diesem Identifikationsmedium noch vorhandene und im Normalfall verwendete Berechtigung für diese Schließung ignoriert. Stattdessen gelten die Berechtigungen, die in der Schließung selbst gespeichert sind und in einem virtuellen Netzwerk durch die Identifikationsmedien aktualisiert werden (und deshalb aktueller sind).

Gleichzeitig wird die ID des auf diese Weise gesperrten Identifikationsmediums in einer Blacklist gespeichert und kann nicht aus Versehen wieder aktiviert werden.

3.3.4 Verfallsdatum (Expiry date)

Für eine effektive Nutzung des virtuellen Netzwerks ist es notwendig, dass das Gateway regelmäßig Daten von und zu den Identifikationsmedien übertragen kann. Sie können als Schließanlagenadministrator mit einem Verfallsdatum die Nutzer Ihrer Schließanlage dazu "zwingen", ihre Identifikationsmedien regelmäßig an dem Gateway zu betätigen.

Ein Verfallsdatum schränkt die Gültigkeit eines Identifikationsmediums zeitlich ein. Die Nutzer müssen ihr Zeitguthaben regelmäßig an einem Gateway aufladen, sonst können Sie bis zur Aufladung des Zeitguthabens an einem Gateway keine Schließung (auch keine Offline-Schließung) mehr benutzen. Für dieses Zeitguthaben gibt es zwei Möglichkeiten:

- Fixe Stundenzahl zwischen einer und 255 Stunden (zum Beispiel Berechtigung für acht Stunden ab Aufladung)
- Fixe Ablauf-Uhrzeit zwischen 1:00 Uhr und 24:00 Uhr (zum Beispiel Berechtigung zwischen Aufladungszeitpunkt und 20:00 Uhr)

Sie stellen dieses Zeitguthaben in der LSM global für alle Identifikationsmedien ein. Für einzelne Transponder können Sie aber auch ein individuelles Zeitguthaben festlegen. Generelle Änderungen (zum Beispiel die Dauer des Zeitguthabens) werden direkt mit der LSM programmiert.

3.3.5 Uhrzeit stellen

In den Schließungen und in den Transpondern ist ein Zeitbaustein enthalten. Wenn ein Transponder an einem Gateway betätigt wird, dann wird der Zeitbaustein im Transponder neu gestellt (und ggfs. vor- oder nachgehende Zeiten im Transponder korrigiert). Die Zeit im Transponder dient bei der Betätigung an einer Schließung als Referenz. Wenn die Zeit in der Schließung bei der Betätigung abweicht, dann wird der Zeitbaustein in der Schließung nach der Zeit im Transponder neu gestellt (und ggfs. vor- oder nachgehende Zeit in der Schließung korrigiert).

Die Zeit in den Schließungen in Ihrem virtuellen Netzwerk wird automatisch regelmäßig neu gestellt, ohne dass Sie als Schließanlagenadministrator die Schließungen manuell nachprogrammieren müssen.

3.4 Zeitsteuerung

Mit der Zeitzonensteuerung können Sie den Zeitraum begrenzen (Zeitzone), in dem bestimmte Identifikationsmedien (und damit Personen bzw. Personengruppen) eine Schließung betätigen können (und so zum Beispiel das Gebäude betreten können).

3.4.1 Zeitzonen

Sie können beliebige Zeitzonenpläne anlegen und jedem Bereich individuell einen Zeitzonenplan zuordnen. Ein Zeitzonenplan enthält bis zu hundert Zeitzonengruppen, die mit unterschiedlichen Zutrittszeiten frei konfiguriert werden können. In den verschiedenen Zeitzonenplänen können Sie die Zeitzonengruppen unterschiedlich wählen bzw. konfigurieren.

3.4.2 Feiertage

In den Zeitzonenplänen können Sie neben den sieben Wochentagen (Montag bis Sonntag) auch auf Sonder- oder Feiertage eingehen.

Dazu verwenden Sie einfach die in der LSM-Software hinterlegten Feiertagslisten (für alle deutschen Bundesländer), statt diese selbst anzulegen. Alternativ legen Sie unabhängig von den mitgelieferten Feiertagslisten eigene Feiertagslisten an. Jeder beliebige Tag kann als Feiertag gespeichert werden und kann beispielsweise wie ein Sonntag behandelt werden (siehe auch *Sondertage [▸ 14]*).

3.4.3 Sondertage

Ein Sondertag legt für bestimmte Tage ein von den sieben Wochentagen unabhängiges Zeitprofil fest. Sondertage haben eine höhere Priorität als Feiertage.

Mit Sondertagen können Sie beispielsweise den Zutritt von Schulpersonal während der Schulzeiten von Montag bis Freitag gestatten und während der Ferien mit (höher priorisierten) Sondertagen generell sperren.

3.4.4 Gültigkeitsdatum (Validation date)

Sie können Transpondern ein beliebiges Gültigkeitsdatum zuweisen. Transponder mit einem Gültigkeitsdatum können erst nach diesem Gültigkeitsdatum in der Schließanlage verwendet werden.

Diese Funktion ist unabhängig von der virtuellen Vernetzung (siehe *Verfallsdatum (Expiry date) [▸ 13]*) und kann nur durch das Programmiergerät geändert werden. Verwenden Sie diese Funktion nicht im Zusammenhang mit der virtuellen Vernetzung.

3.4.5 Verfallsdatum (Expiry date)

Sie können Transpondern ein beliebiges Verfallsdatum zuweisen. Transponder mit einem Verfallsdatum können nach diesem Verfallsdatum nicht mehr in der Schließanlage verwendet werden.

Diese Funktion ist unabhängig von der virtuellen Vernetzung (siehe *Verfallsdatum (Expiry date) [▸ 13]*) und kann nur durch das Programmiergerät geändert werden. Verwenden Sie diese Funktion nicht im Zusammenhang mit der virtuellen Vernetzung.

3.5 Listen

3.5.1 Zutrittslisten

Schließungen mit ZK-Funktion protokollieren die Zutritte in einer Zutrittsliste:

- Datum
- Uhrzeit
- ID des Identifikationsmediums
- Name des Nutzers oder der Nutzerin

Sie können die Zutrittsliste mit der LSM-Software auslesen und anzeigen. Die Anzahl der Einträge in der Zutrittsliste hängt von der Schließung und der Konfiguration ab.

	Standard	Gateway
Zylinder	Bis zu 3000	
SmartRelais	Bis zu 3600	Bis zu 200

3.5.2 Begehungslisten

G2-Transponder protokollieren die Zutritte unabhängig von Zutrittslisten in einer Begehungsliste. In dieser Begehungsliste sind die letzten Begehungen gespeichert (bis zu 1000):

- Datum
- Uhrzeit
- ID der Schließung

Sie können die Begehungsliste mit der LSM-Software auslesen und anzeigen.

3.6 Protokollgenerationen

3.6.1 G1-Schließanlagen

In G1-Schließanlagen können nur G1-Produkte und nur G1-Funktionen verwendet werden.

Wenn Sie G1-Datensätze in G2-Transpondern verwenden, dann werden die Expiry-Funktionen der G1-Protokolle (zum Beispiel mit Validation Terminals) nicht unterstützt.

HINWEIS

G1-Produkte sind abgekündigt

G1-Produkte sind nicht mehr erhältlich.

3.6.2 G2-Schließanlagen

In G2-Schließanlagen können nur G2-Produkte und nur G2-Funktionen verwendet werden.

3.6.3 G1- und G2-Schließanlagen getrennt

Mit diesem Ansatz trennen Sie die unterschiedlichen Protokollgenerationen auf (mindestens) zwei unterschiedliche Schließanlagen auf. Auf jedem Identifikationsmedium sind dann (mindestens) zwei voneinander unabhängige Schließanlagendatensätze gespeichert (je einer aus G1 und einer aus G2).

Der Vorteil dieses Ansatzes vermeidet von vornherein Kompatibilitätsprobleme.

Sie verwalten diese Schließanlagen im selben Schließplan bzw. in derselben Datenbank. Ab der LSM 3.0 können Sie in der Matrix die Anzeige nach der Protokollgeneration filtern und sehen je nach Filter nur noch die Schließungen und Identifikationsmedien für G1 oder G2.

3.6.4 G1- und G2-Schließanlagen gemischt (Kompatibilitätsmodus)

Mit diesem Ansatz verwalten Sie die beiden unterschiedlichen Protokollgenerationen in derselben Schließanlage.

- G1-Produkte verwenden weiterhin nur G1-Funktionen.
- G2-Produkte werden im Kompatibilitätsmodus betrieben.

Sie müssen nur eine einzige Schließanlage betreuen, aber durch die Vermischung von G1 und G2 wird die Übersichtlichkeit und Unterscheidbarkeit eingeschränkt.

HINWEIS

Funktionseinschränkungen durch Mischbetrieb

Die Verwendung von Mischsystemen kann zu Funktionseinschränkungen führen und erfordert Erfahrung.

1. Vermeiden Sie gemische Schließanlagen.
2. Verwenden Sie stattdessen getrennte Schließanlagen (siehe *G1- und G2-Schließanlagen getrennt [▸ 16]*).

3.7 Batteriewarnungen

Die Batteriewarnungen der Zylinder mit G2-Protokoll sind identisch zu den Zylindern mit G1-Protokoll (Ausnahme: Mifare-Zylinder, siehe die jeweiligen Handbücher/Kurzanleitungen).

3.7.1 G2-Batteriewechseltransponder

Zylinder mit sehr schwachen Batterien lassen sich mit normalen Identifikationsmedien nicht mehr betätigen, um ein vollständiges Entladen zu verhindern (G1: Lagermodus, G2: Freeze-Modus).

Der Lagermodus und die Batteriewarnungen bei Zylindern mit G1-Protokollen kann nur mit dem Programmiergerät vor Ort aufgehoben werden.

Das G2-Protokoll ermöglicht ab der LSM 3.0 sogenannte Batteriewechseltransponder. Mit einem Batteriewechseltransponder heben Sie den Freeze-Modus von G2-Schließzylindern aufheben und betätigen die Schließung mit einem normalen berechtigten Transponder. Sie müssen dazu nicht mit dem Programmiergerät vor Ort an der Schließung sein.

VORSICHT

Entleerung der Batterien durch Missbrauch

Bei jeder Öffnung im Zusammenhang mit einem Batteriewechsel-Transponder wird die Batterie weiter entleert. Das kann bei nicht zweckmäßiger Verwendung zu einer völligen Entleerung der Batterien führen! Die Batterien müssen in diesem Zustand sofort erneuert werden.

4 G2-Produkte

Wenn Sie alle Funktionen der G2-Protokolle verwenden wollen, dann dürfen Sie ausschließlich G2-Produkte verwenden. Informationen zur Verfügbarkeit der G2-Produkte finden Sie in der aktuellen SimonsVoss-Preisliste.

4.1 Programmiergeräte

Für die Programmierung von G2-Komponenten benötigen Sie ein Programmiergerät mit geeigneter Firmware:

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

Die Firmware ist abwärtskompatibel. Sie können mit Programmiergeräten mit neuer Firmware auch die bisherigen G1-Komponenten programmieren.

4.2 Zylinder

Produkt	G1-kompatibel	G2-kompatibel
Standard-Zylinder (25 kHz)	ja	ja
Mifare/SmartCard-Zylinder	nein	ja

4.3 SmartHandle

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

4.4 SmartRelais

Produkt	G1-kompatibel	G2-kompatibel
SmartRelais	ja	ja
SmartRelais 2	ja	ja

Produkt	G1-kompatibel	G2-kompatibel
SmartRelais 3	ja	ja

4.5 Transponder

Sie erhalten alle Transponder als G2-Produkt.

4.6 Netzwerk (WaveNet)

Ihr WaveNet (RouterNodes und LockNodes) kann G1- und G2-Produkte ansprechen. Externe LockNodes werden bedingt auch in G2-Komponenten unterstützt.

	Türüberwachung	Nachprogrammierung
Interne LockNodes	ja	ja
Externe LockNodes	ja	nein

5 Signalisierung

Bei der Signalisierung wird zwischen Transpondersignalisierung (z.B. OK) und Zustandssignalisierung (z.B. Batteriewarnung) unterschieden.

5.1 Transaktion

Funktion	Beschreibung	Signalisierung
Transaktion ist ok Schließung kuppelt ein	Schließung kuppelt ein	2x kurz
Schließung kuppelt aus	Schließung kuppelt aus	1x kurz
Flip-Flop-Modus (kuppelt ein)	Schließung kuppelt ein	1x kurz, 1x lang
Flip-Flop-Modus (kuppel aus)	Schließung kuppelt aus	1x lang, 1x kurz
Vorgang kann nicht ausgeführt werden	Schließung ist deaktiviert	1x kurz
	Schließung ist im Freeze-Modus	1x kurz
	Identifikationsmedium ist ungültig	1x kurz

G2-Produkte zeigen dem Nutzer durch ein Abwehrsignal an, dass sein Identifikationsmedium nicht berechtigt ist.

5.2 Zustand

Funktion	Beschreibung	Signalisierung
Kritischer Batteriezustand der Schließung	Batteriewarnstufe 1	8x kurz (vor dem Einkuppeln)
Kritischer Batteriezustand der Schließung (Schließung ist im Flip-Flop-Modus)	Batteriewarnstufe 1	ca. alle 60 Sekunden 4x doppelt kurz
Kritischer Batteriezustand der Schließung	Batteriewarnstufe 2	8x kurz mit einer Sekunde Pause für 30 Sekunden (vor dem Einkuppeln)
Kritischer Batteriezustand der Schließung	Freeze-Modus	6x lang-kurz

Funktion	Beschreibung	Signalisierung
Kritischer Batteriezustand des Transponders		8x doppelt kurz (nach dem Auskuppeln)
Programmiervorgang		1x kurz (abhängig von den Programmierdaten)
Neustart (Power-On-Reset)		3x kurz

Sie können die akustischen Batteriewarnungen bei Zylindern deaktivieren. Der Zylinder signalisiert den Nutzern leere Batterien in diesem Zustand nicht mehr.

5.3 Konfigurationsmöglichkeiten

5.3.1 Programmiervorgänge

Sie können die schließungsseitige Signalisierung einer Programmierung deaktivieren.

5.3.2 Öffnung

Sie können die schließungsseitige akustische Signalisierung einer Programmierung für einzelne Identifikationsmedien deaktivieren. Diese Deaktivierung gilt für dieses Identifikationsmedium schließungsanlagenweit.

6 Erweiterung

6.1 G1 erweitern

G1-Geräte sind nicht mehr erhältlich. Wenn Sie bisher eine G1-Schließanlage verwendet haben und neue Geräte brauchen, dann erweitern Sie Ihre G1-Schließanlage mit einer G2-Schließanlage. Sie können die Schließanlagen getrennt betreiben (siehe *G1- und G2-Schließanlagen getrennt [▸ 16]*) oder gemischt betreiben (siehe *G1- und G2-Schließanlagen gemischt (Kompatibilitätsmodus) [▸ 16]*).

Eine mögliche virtuelle Vernetzung, Teilvernetzung oder Vollvernetzung steigert Ihren Komfort und kann jederzeit nachgerüstet werden (siehe *Unterschiede: Vernetzungen [▸ 23]*).

6.2 G2 erweitern

Sie können Ihre G2-Schließanlage nach Ihren Wünschen jederzeit bis zu den Grenzen der G2-Protokolle erweitern und nachprogrammieren.

Eine mögliche virtuelle Vernetzung, Teilvernetzung oder Vollvernetzung steigert Ihren Komfort und kann jederzeit nachgerüstet werden (siehe *Unterschiede: Vernetzungen [▸ 23]*).

7 Unterschiede: Vernetzungen

	WaveNet (online)	Virtuelle Vernetzung (virtuell)	Keine Vernetzung (offline)
Funktionsprinzip	Übertragung der Daten mit vernetzten WaveNet-Geräten (siehe Übertragungswege und Geräte).	Übertragung der Daten mit Identifikationsmedien (außer Programmierdaten).	Übertragung der Daten mit Programmiergeräten.
Ausbreitung	WaveNet-Geräte sind über verschiedene Übertragungsmedien verbunden. Daten aller Art werden mithilfe dieser Übertragungsmedien übermittelt.	Im virtuellen Netzwerk werden bestimmte Daten mithilfe eines Gateways auf die Identifikationsmedien übertragen (Einträge in die Blacklist). Wenn Sie diese Identifikationsmedien an einer virtuell vernetzten Schließung betätigen, dann werden die Daten auf die Schließung übertragen.	Schließungen, die nicht vernetzt sind, können nur mit dem Programmiergerät Daten austauschen. Sie müssen mit dem Programmiergerät zu den Schließungen gehen.
Programmieraufwand	Gering.	Gering.	Aufwand hängt von Größe der Schließanlage ab. ▪ Kleine Schließanlage: Geringer Aufwand. ▪ Mittlere Schließanlage: Mittlerer Aufwand. ▪ Große Schließanlage: Großer Aufwand.
Übertragungsgeschwindigkeit des Datenaustauschs	Unmittelbar. Datenaustausch mit verschiedenen Übertragungsmedien.	Geschwindigkeit zwischen Gateway und Schließungen stark abhängig von Nutzungsintensität der Schließungen. Identifikationsmedien sind Übertragungsmedium - ohne Identifikation keine Datenübertragung.	Langsam.

	WaveNet (online)	Virtuelle Vernetzung (virtuell)	Keine Vernetzung (offline)
Zentrale Aktivierung/Deaktivierung von Schließungen	Möglich.	Nicht möglich.	Nicht möglich.
Aktivierung/ Deaktivierung zentral nachverfolgbar	Möglich.	Nicht möglich.	Nicht möglich.
Fernöffnung	Möglich.	Nicht möglich.	Nicht möglich.
Fernüberwachung (Door-Monitoring)	Möglich.	Nicht möglich.	Nicht möglich.
Eventmanagement	Möglich.	Nicht möglich.	Nicht möglich.
Zutrittslisten zentral abrufbar	Möglich.	Nicht möglich (außer SREL 3).	Nicht möglich.
Software-/ serverunabhängige Schutzfunktionen	Möglich.	Nicht möglich.	Nicht möglich.
Sofortige schließanlagenweite Reaktion auf kritische Situationen (Verfügbarkeit von Schutzfunktionen, siehe I/O-Konfiguration und Schutzfunktionen und RingCast)	Möglich.	Nicht möglich.	Nicht möglich.

8 Anhang

8.1 Unterschiede G1- und G2-Protokolle

	G1	G2	G2 (virtuell vernetzt)
Schließungen	16000	64000	64000
Identifikationsmedien	8000	64000	64000
Zeitzonengruppen	5+1	100+1	100+1
Basisinformationen	Identifikationsmedien		Schließungen
Schließplaninformationen	Schließungen	Schließungen oder Identifikationsmedien	Identifikationsmedien
Gateways (online)	Nein	Nein	Ja
Netzwerk	Ja	Ja	Ja (nur Gateways)

Wenn Sie die G2-Protokolle ohne virtuelle Vernetzung verwenden, dann können Sie bei jedem Programmierbedarf entscheiden, ob Sie das Identifikationsmedium oder die Schließung programmieren. Die Schließungen können eine Identifikationsmedienliste speichern und die Identifikationsmedien eine Schließungsliste.

8.2 Glossar

Begriff	Erklärung
ASM	Anlagenstatusmonitoring
Bereich	Zusammenfassung mehrerer Schließungen zur leichteren Berechtigungsverwaltung
Begehungsliste	Liste von begangenen Schließungen, welche auf dem Identifikationsmedium gespeichert wird
Datenbank	Speicherung aller Informationen des Schließplans bzw. der Schließanlage des Systems 3060

Begriff	Erklärung
Direktvernetzung (LockNode Inside)	Netzwerkknoten (LockNode) direkt in die Schließung integriert
Gateway	Anbindung des virtuellen Netzwerks an die LSM-Software
G1	Alte Protokollgeneration der B-Feld-Schnittstelle
G2	Aktuelle Protokollgeneration der B-Feld-Schnittstelle
LID	Lock-ID: Eindeutige Kennung einer Schließung innerhalb einer Simons-Voss-Schließanlage
LSM	Locking System Management: Datenbankgestützte PC-Software zur Verwaltung der SimonsVoss-Schließanlage
LockNode	Netzwerkknoten zur direkten Nahfeldkommunikation mit einer Schließung
Mechanisch aktiv	(=Eingekuppelt) Mechanischer Zustand einer Schließung, der dem Anwender das Öffnen und Schließen erlaubt
Mechanisch inaktiv	(=Ausgekuppelt) Mechanischer Zustand einer Schließung, der dem Anwender das Öffnen und Schließen nicht erlaubt
Netzwerk	SimonsVoss WaveNet. Schließungen können damit im Online-Modus (=vernetzt) betrieben werden
Schließanlage	Zusammengehörige und gemeinsam verwaltete Menge von Schließungen und Identifikationsmedien
Schließanlagenpasswort	Passwort zur Absicherung der Schließanlage
Schließplan	Ein Schließplan kann aus mehreren Schließanlagen bestehen

Begriff	Erklärung
SID	Schließanlagen-ID: Eindeutige Kennung einer Schließanlage in einem SimonsVoss-Schließplan
Schließung	Oberbegriff für alle Produkte, die mit einem Identifikationsmedium angesprochen werden können
SmartCD	Programmiergerät: Mit einem SmartCD werden die SimonsVoss-Produkte programmiert
TID	Transponder-ID: Eindeutige Kennung eines Identifikationsmediums in einer SimonsVoss-Schließanlage
Transponder	Medium, das mit einer Schließung kommunizieren kann
Transpondergruppen	Zusammenfassung mehrer Identifikationsmedien zur einer Gruppe, um die Berechtigungen einfacher verwalten zu können
Virtuelles Netzwerk	Technologie, mit der bei Offline-Schließungen Berechtigungsänderungen über Gateways verbreitet werden und die Schließungen nicht aufgesucht werden müssen
Zeitzonengruppen	Gruppen als Bestandteil eines Zeitzonenplans
Zeitzonenpläne	Zeitzonenplan, der in der Schließung gespeichert werden kann
Zutrittsliste	Liste von Begehungen, die in der Schließung gespeichert wird (Voraussetzung: ZK)
Zutrittsprofil (Transpondergruppen / Bereiche)	Definiert die Menge von Schließungen, die mit einem Identifikationsmedium, auf dem sich dieses Profil befindet, angesprochen werden können

9 Hilfe und weitere Informationen

Infomaterial/Dokumente

Detaillierte Informationen zum Betrieb und zur Konfiguration sowie weitere Dokumente finden Sie auf der SimonsVoss-Homepage im Downloadbereich unter Dokumente (*https://www.simons-voss.com/de/downloads/dokumente.html*).

Konformitätserklärungen und Zertifikate

Konformitätserklärungen und Zertifikate zu diesem Produkt finden Sie auf der SimonsVoss-Homepage im Zertifikatsbereich (*https://www.simons-voss.com/de/zertifikate.html*).

Hotline

Bei technischen Fragen hilft Ihnen die SimonsVoss Service-Hotline unter +49 (0) 89 99 228 333 (Anruf in das deutsche Festnetz, Kosten variieren je nach Anbieter).

E-Mail

Sie möchten uns lieber eine E-Mail schreiben?

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

FAQ

Informationen und Hilfestellungen zu SimonsVoss-Produkten finden Sie auf der SimonsVoss-Homepage im FAQ-Bereich (*https://faq.simons-voss.com/otrs/public.pl*).

Adresse

SimonsVoss Technologies GmbH
Feringastraße 4
85774 Unterföhring
Deutschland

Das ist SimonsVoss

SimonsVoss ist Technologieführer bei digitalen Schließsystemen.

Der Pionier funkgesteuerter, kabelloser Schließtechnik bietet Systemlösungen mit breiter Produktpalette für die Bereiche SOHO, mittlere und Großunternehmen sowie öffentliche Einrichtungen.

SimonsVoss-Schließsysteme verbinden intelligente Funktionalität, hohe Qualität und preisgekröntes Design made in Germany. Als innovativer Systemanbieter legt SimonsVoss Wert auf skalierbare Systeme, hohe Sicherheit, zuverlässige Komponenten, leistungsstarke Software und einfache Bedienung.

Mut zur Innovation, nachhaltiges Denken und Handeln sowie hohe Wertschätzung der Mitarbeiter und Partner sind Grundlage des wirtschaftlichen Erfolgs. Das Unternehmen mit Hauptsitz in Unterföhring bei München und Produktionsstätte in Osterfeld (Sachsen-Anhalt) beschäftigt rund 300 Mitarbeiter in acht Ländern.

SimonsVoss ist ein Unternehmen der ALLEGION Group - ein global agierendes Netzwerk im Bereich Sicherheit. Allegion ist in rund 130 Ländern weltweit vertreten (www.allegion.com)

ALLEGION

SimonsVoss technologies