

HANDBUCH – G2 Protokolle

Stand: Oktober 2015

HANDBUCH – G2 Protokolle

Inhaltsverzeichnis

1.0	ALLGEMEINES.	5
1.1	Sicherheitshinweise	5
2.0	G2 PROTOKOLLE.	6
2.1	Allgemeine Beschreibung	6
2.1.1	Schließanlagenpasswort	6
2.1.2	Schließanlagengröße	6
2.1.3	Übergreifende Schließebenen	6
2.1.4	Notfreischaltung	7
2.1.5	Notöffnung	7
2.1.6	Pulslänge	7
2.1.7	Kein akustisches Öffnungssignal	8
2.2	Berechtigungsvergabe	8
2.2.1	Allgemeines	8
2.2.2	G2pur	8
2.2.3	Virtuelles Netzwerk	9
2.3	Virtuelles Netzwerk	9
2.3.1	Gateways	10
2.3.2	Direkte Berechtigungen	10
2.3.3	Sperr-IDs (Lock Priority)	10
2.3.4	Verfallsdatum (Expiry Date)	10
2.3.5	Uhrzeit stellen	11
2.4	Zeitsteuerung	11
2.4.1	Zeitzonen	11
2.4.2	Feiertage	11
2.4.3	Sondertage	12
2.4.4	Gültigkeitsdatum (Validation-Date)	12
2.4.5	Verfallsdatum (Expiry-Date)	12
2.5	Listen	12
2.5.1	Zutrittslisten	12
2.5.2	Begehungslisten	13
2.6	Protokollgenerationen	13

HANDBUCH – G2 Protokolle

Inhaltsverzeichnis

2.6.1	G1 Schließanlagen	13
2.6.2	G2 Schließanlagen	13
2.6.3	G1 und G2 Schließanlagen getrennt	13
2.6.4	G1 und G2 Schließanlagen gemischt (Kompatibilitätsmodus)	14
2.7	Batteriewarnungen	14
2.7.1	G2 Batteriewechsel-Transponder	14
3.0	G2 PRODUKTE.	15
3.1	Programmiergeräte	15
3.2	Zylinder	15
3.3	Zylinder - SC	15
3.4	SmartHandle	15
3.5	SmartHandle - SC	15
3.6	Smart Relais	15
3.7	Transponder	15
3.8	Netzwerk	15
4.0	SIGNALISIERUNG.	16
4.1	Beschreibung Transaktionssignalisierung	16
4.2	Beschreibung Zustandssignalisierung (aktive Komponenten)	16
4.3	Konfigurationsmöglichkeiten	17
4.3.1	Programmiervorgänge	17
4.3.2	Transponderöffnung	17
5.0	NUTZUNGSSZENARIOEN.	17
5.1	Neue Schließanlage	17
5.1.1	Anlagengröße: Weniger als 100 Türen, Offline-Betrieb	17
5.1.2	Anlagengröße: Weniger als 100 Türen, Mischbetrieb: Offline/Online	17
5.1.3	Anlagengröße: Weniger als 100 Türen, Online-Betrieb	18
5.1.4	Anlagengröße zwischen 100-500 Türen	18
5.1.5	Anlagengröße: Mehr als 500 Türen	18
5.2	Schließanlagenerweiterung	19
5.2.1	Anlagengröße: Deutlich mehr als 100 Türen	19

HANDBUCH – G2 Protokolle

Inhaltsverzeichnis

5.2.2	Anlagengröße: Systemgrenzen G1 erreicht _____	19
6.0	Anhang. _____	20
6.1	Übersicht Unterschiede G1 und G2 Protokolle _____	20
6.2	Begriffserklärung _____	20

1.0 ALLGEMEINES.

Die G2-Protokolle stellen eine komplette Neuentwicklung der SimonsVoss Kommunikation zwischen Transpondern und Schließungen dar. Hier sind viele neue Funktionalitäten eingeflossen, um die Möglichkeiten Schließanlagen besser und einfacher zu verwalten zur Verfügung zu stellen.

Basierend auf den neuen G2 Protokollen stehen nun neue Hardwareprodukte als auch eine komplett modular aufgebaute Software zur Verfügung, um die Schließanlagen noch besser an die eigenen Bedürfnisse anzupassen.

1.1 Sicherheitshinweise

- Die Handhabung der G2 Protokolle setzt Kenntnisse im Umgang mit der SimonsVoss-Software (möglich ab LSM 3.0 und höher) voraus. Deshalb sollte die Programmierung nur durch geschultes Fachpersonal erfolgen.
- Für Schäden durch fehlerhafte Programmierung übernimmt die SimonsVoss Technologies GmbH keine Haftung.
- Durch fehlerhaft programmierte Produkte kann der Zugang durch eine Tür versperrt werden. Für Folgen, wie versperrter Zugang zu verletzten oder gefährdeten Personen, Sachschäden oder anderen Schäden haftet die SimonsVoss AG nicht. Für Schäden durch fehlerhafte Montage oder Installation übernimmt die SimonsVoss Technologies GmbH keine Haftung.
- Die SimonsVoss Technologies GmbH behält sich das Recht vor, Produktänderungen bzw. technische Weiterentwicklungen ohne Vorankündigung durchzuführen.
- Die Dokumentation wurde nach bestem Wissen erstellt, evtl. Fehler können aber nicht ausgeschlossen werden. Hierfür kann keine Haftung übernommen werden.
- Sollten Abweichungen von Inhalten in Fremdsprachenversionen der Dokumentation bestehen, gilt im Zweifelsfalle das deutsche Original.

2.0 G2 PROTOKOLLE.

2.1 Allgemeine Beschreibung

Durch die Einführung der G2 Protokolle werden neue Funktionalitäten im Simons-Voss Schließsystem 3060 unterstützt. Für die Verwendung der neuen G2 Protokolle ist die LSM ab der Version 3.0 oder höher zwingend erforderlich, und es werden die entsprechenden G2 Komponenten benötigt, welche die neuen Funktionalitäten unterstützen.

2.1.1 Schließanlagenpasswort

Das Schließanlagenpasswort wird nur noch bei der Erstellung des Schließplans benötigt. Dieses Passwort muss mindestens eine Länge von 64 Bit besitzen. Um bei der Erstellung des Passwortes unterstützend helfen zu können, ist ein Qualitätsindex für das Schließanlagenpasswort in die Software integriert. Somit werden unsichere Passwörter nicht mehr zugelassen und die komplette Systemsicherheit weiter erhöht.

2.1.2 Schließanlagengröße

Die Schließanlagengröße wächst durch die Verwendung der neuen Protokolle. Somit können je Schließanlage

- Bis zu 64.000 Schließungen pro Schließanlage verwaltet werden.
- Bis zu 64.000 Transponder individuell zugelassen bzw. gesperrt werden.

Insgesamt können somit über 4 Milliarden Einzelberechtigungen in der LSM je Schließanlage vergeben werden.

2.1.3 Übergreifende Schließebenen

Übergreifende Schließebenen können genutzt werden, um schließanlagenübergreifende Funktionen mit einem eigenen Passwort zu ermöglichen (sog. Querschließanlagen).

Für diese Funktion stehen 3 höhere Ebenen zur Verfügung:

- Rot
- Grün
- Blau

Ein Transponder kann jeweils zu einer der drei Ebenen gehören, wobei für jede Ebene 1.024 TIDs (Transponder-IDs) in der LSM (ab Version 3.0) reserviert sind. Somit können auch in den einzelnen Ebenen unterschiedliche Berechtigungen vergeben bzw. auch diese Transponder individuell gesperrt werden.

Bei Verwendung der Ebene Rot (z.B. zur Hinterlegung in Feuerwehrschlüsseldepots) wird auch eine deaktivierte Schließung (bei Nutzung der SimonsVoss Block Schloss Komponenten) aktiviert und kann innerhalb von 5 Sekunden (bzw. je nach eingestellter Impulsdauer) geöffnet werden.

2.1.4 Notfreischaltung

Bei einer vernetzten Schließanlage können Schließungen über Netzwerk notfreigeschaltet werden. Das heißt, durch einen konfigurierbaren Netzwerktask können Schließungen in einen dauerhaft mechanisch aktiven Zustand versetzt werden. Somit sind diese ohne Transponder frei begehbar. Diese Funktion kann z.B. mit der Brandmeldeanlage gekoppelt werden, somit ist es im Brandfall für die Feuerwehr möglich die Türen frei zu begehen.

In diesem Zustand hat der Einsatz eines Transponders der Schließanlage keine Auswirkung auf die notfreigeschalteten Schließungen.

Die Notfreischaltung kann jederzeit durch eine Notöffnung/Fernöffnung aufgehoben werden.

2.1.5 Notöffnung

Es ist möglich, in der LSM (beim Export auf die LSM Mobile) ein temporäres vom Schließanlagenadministrator frei zu wählendes Passwort zu vergeben, welches eine Mindestlänge von 8 Zeichen aufweisen muss. Mit diesem Passwort kann vor Ort eine Notöffnung an der Schließung durchgeführt werden, ohne dass das Schließanlagenpasswort bekannt ist.

Diese Funktion ist sowohl von der Anzahl als auch vom Durchführungszeitraum seitens des Administrators einschränkbar.

2.1.6 Pulslänge

Die Einkuppelzeiten sowohl für die Schließzylinder, als auch für die Smart Relais sind von 1 bis 25 Sekunden frei wählbar.

In Kombination mit der Transponderfunktion „Langes Öffnen“, welche individuell konfiguriert werden kann, verdoppelt sich die Einkuppelzeit (wobei die max. Pulslänge weiterhin 25 Sekunden beträgt).

Die Einkuppelzeit kann schließungsspezifisch gewählt werden, die Funktion „Langes Öffnen“ wird im Transponder konfiguriert. Somit ist es möglich transponderindividuell die Einkuppelzeit zu konfigurieren.

2.1.7 Kein akustisches Öffnungssignal

Bei beliebigen Transpondern kann das akustische Öffnungssignal an der Schließung abgeschaltet werden. Somit kann z.B. im Krankenhaus vermieden werden, Patienten zu wecken, wenn nachts Türen geöffnet werden müssen.

2.2 Berechtigungsvergabe

2.2.1 Allgemeines

Durch den Einsatz der neuen Protokolle wird durch die Verwendung intelligenter Mechanismen die Umprogrammierung von Schließungen vor Ort bei Ausgabe von neuen Transpondern weitgehend vermieden.

Es besteht nun die Möglichkeit sowohl auf

- G2pur:
 - Transponder und Schließungen (direkt)
 - Sperrungen über Ersatztransponder
- G2 VN: Virtuelle Vernetzung (indirekt)

Berechtigungen an Komponenten der Schließanlage zu vergeben.

2.2.2 G2pur

Im G2pur Modus kann bei jedem Programmiervorgang gewählt werden, ob die Berechtigungen auf den Transpondern oder Schließungen geändert werden sollen. Z.B. bei neuen Nutzern werden die Berechtigungen ausschließlich auf den Transpondern hinterlegt, bei einer neuen Tür wird nur die entsprechende Schließung programmiert. Weiterer Programmieraufwand in der Schließanlage entfällt somit, welches eine große Zeitersparnis darstellt.

Somit steht dem Schließanlagenadministrator ein komplett offenes System zur Verfügung und bei der Programmierung entscheidet man sich für die Möglichkeit mit dem geringsten Aufwand.

2.2.2.1 Schließungen

2.2.2.2 Pro Schließung können bis zu 64.000 Transponder-IDs verwaltet und somit individuell frei geschaltet bzw. gesperrt werden.

Die Programmierung erfolgt prinzipiell wie bei den bisherigen Schließungen der Generation 1.

2.2.2.3 Transponder

In den G2 Schließanlagen ist es möglich, auf einem Transponder anzugeben, für welche Schließungen dieser berechtigt sein soll. Auf den neuen G2 Transpondern können bis zu:

- 3 G1 Schließanlagen
- 4 G2 Schließanlagen

gespeichert und verwaltet werden. Für die G2 Schließanlagen können bis zu 64.000 Schließungen je Schließanlage verwaltet werden.

Somit kann in G2 Schließanlagen der komplette Schließplan auf dem Transponder hinterlegt werden.

2.2.2.4 Ersatztransponder

Ab der LSM 3.0 SP2 ist es möglich durch Anlegung eines Ersatztransponders diesem automatisch die Sperr-ID des verlorenen Transponders bei der Programmierung mitzugeben. Durch die Nutzung dieses Transponders an der Schließung wird der verlorene Transponder bzw. die verlorene TID gesperrt.

Der Programmierbedarf an den Schließungen bleibt bestehen, und kann erst durch eine Nachprogrammierung der entsprechenden Schließungen aufgehoben werden.

2.2.3 Virtuelles Netzwerk

Siehe hierzu Kapitel 2.3

2.3 Virtuelles Netzwerk

Durch die Verwendung von sogenannten Gateways entfällt die Notwendigkeit der direkten Umprogrammierung der Komponenten seitens des Schließanlagenadministrators (Schließungen und Transponder) vor Ort. Die Schließungen bekommen nur noch Basisinformationen bei der Erstprogrammierung mitgeteilt, d.h. diese werden anlagenspezifisch zugelassen. Die Berechtigungsmatrix der Schließanlage wird ausschließlich auf den Transpondern gespeichert.

2.3.1 Gateways

Die Gateways stehen als Online Variante zur Verfügung. Durch das Einbinden der Online-Gateways in ein SimonsVoss Netzwerk, werden zum Einen Änderungen der Berechtigungen (positive als auch negative) und Sperr-IDs auf den Transponder verteilt, als auch Quittungen aus der Anlage an die Gateways zurückgemeldet. Somit entfällt der Programmieraufwand mittels Programmiergerät an den Schließungen, die Schließanlage wird über die Gateways bzw. Transponder der Nutzer umprogrammiert.

SmartRelais können als Gateways eingesetzt werden. Es wird mittels der LSM Software als Gateway konfiguriert.

2.3.2 Direkte Berechtigungen

An den Gateways werden Berechtigungen direkt in der Berechtigungsmatrix der Transponder geändert, und stehen unmittelbar zur Verfügung. Zusätzlich können TIDs als Sperr-IDs an die Transponder verteilt werden, welche dann in der Schließanlage an die entsprechenden Schließungen weitergegeben werden.

Durch Quittungsmanagement (Umprogrammierungen vor Ort durch die Transponder werden als Feedback auf nachfolgende Transponder verteilt) werden durch Rückfluss über die Gateways die Vorgänge in der Schließplanmatrix angezeigt. Programmierbedarf im Schließplan verschwindet automatisch, und der Administrator hat eine aktuelle Übersicht über den Zustand seiner Schließanlage.

2.3.3 Sperr-IDs (Lock Priority)

Ein verlorener Transponder wird in der LSM gesperrt bzw. deaktiviert. Bei Erhalt einer Sperr-ID an einer Schließung, wird für diese Transponder-ID ein sog. Lock Priority gesetzt. D.h. hier wird die Berechtigung an den Gateways entzogen und für diese TID nur noch die Berechtigungsmatrix der Schließung beachtet. Durch die Speicherung dieser TID in einer „Blacklist“ wird verhindert, dass diese TID aus Versehen wieder aktiviert werden kann.

2.3.4 Verfallsdatum (Expiry Date)

Um eine effektive Nutzung der Virtuellen Vernetzung sicherstellen zu können, wird empfohlen ein Verfallsdatum in den Transpondern zu hinterlegen. Somit wird die Gültigkeitsdauer eines Transponders zeitlich eingeschränkt, und es ist gesichert, dass alle Nutzer regelmäßig an den Gateways Berechtigungen bzw. Sperr-IDs auf Ihre Transponder „laden“. Hierbei gibt es zwei unterschiedliche Möglichkeiten:

- Fixe Stundenzahl (z.B. 8 Stunden)
- Fixe Uhrzeit (z.B. 20.00 Uhr)

Sowohl Stundenanzahl (1 Stunde bis 255 Stunden) als auch Uhrzeiten (1:00 Uhr bis 24:00 Uhr) können in der LSM global eingestellt als auch bei den einzelnen Transpondern individuell frei gewählt werden. Nach Ablauf des Verfallsdatums funktionieren die Transponder auch an den Offline-Schließungen nicht mehr, und müssen erst wieder an den Gateways aktiviert werden.

Eine generelle Änderung z.B. die Dauer des Verfallsdatums wird direkt mit der LSM programmiert.

2.3.5 Uhrzeit stellen

Zusätzlich zu den oben genannten Funktionen ist es möglich, über die Transponder die Uhrzeiten in den Schließungen zu aktualisieren. Bei Buchung an einem Gateway wird die Zeitbasis des Transponders aktualisiert, und der Transponder stellt in den Offline-Schließungen die Uhrzeiten nach. Somit werden die Uhrzeiten in den Schließungen über die Virtuelle Vernetzung bei Begehung regelmäßig aktualisiert, eine Nachprogrammierung der Uhrzeit der Schließungen durch den Anlagenadministrator entfällt somit komplett.

2.4 Zeitsteuerung

Mit Hilfe der Zeitzonensteuerung ist es möglich, bestimmten Personen bzw. Personengruppen nur zu bestimmten Zeiten Zutritt zum Gebäude gewähren zu können.

2.4.1 Zeitzonen

Es können beliebige Zeitzonenpläne angelegt werden, wobei jedem Bereich ein individueller Zeitzonenplan zugeordnet werden kann. Jeder Zeitzonenplan kann bis zu 100 Zeitzonengruppen unterscheiden, welche mit unterschiedlichen Zutrittszeiten frei konfiguriert werden können. Die Zeitzonengruppen können in den verschiedenen Zeitzonenplänen unterschiedlich gewählt bzw. konfiguriert werden.

2.4.2 Feiertage

Neben den 7 Wochentagen (Montag bis Sonntag) stehen noch Sonder- bzw. Feiertage zur Verfügung.

Feiertagslisten für alle deutschen Bundesländer sind in der SimonsVoss Software hinterlegt und müssen nicht angelegt werden. Die Zusammenstellung eigener Feiertagslisten ist jederzeit möglich und wird von den vorhandenen Feiertagslisten nicht berührt. Feiertage können beliebigen Tagen zugeordnet werden, sodass diese dann z.B. wie Sonntage behandelt werden. Siehe hierzu auch „Sondertage“.

2.4.3 Sondertage

Ein Sondertag wird benötigt, um einem Feiertag unabhängig von den sieben Wochentagen ein eigenes Zeitprofil zuweisen zu können. So ist es z.B. möglich, das Reinigungspersonal von Montag bis Sonntag (in bestimmten Zeitfenstern) zu berechtigen, während der Schulferien (=Sondertage) jedoch generell nicht. Sondertage haben eine höhere Priorität als Feiertage.

2.4.4 Gültigkeitsdatum (Validation-Date)

Transponder können mit einer frei konfigurierbaren „Gültigkeit ab“ Datum versehen werden. Erst ab diesem Zeitpunkt wird der Transponder aktiviert und kann in der Schließanlage genutzt werden.

Diese Funktion ist unabhängig bzw. nicht in Verbindung von der Virtuellen Vernetzung zu verwenden, da diese nur durch das Programmiergerät geändert bzw. aktualisiert werden kann.

2.4.5 Verfallsdatum (Expiry-Date)

Transponder können mit einer frei konfigurierbaren „Gültigkeitsdauer“ eingeschränkt werden (Verfallsdatum). Nach Ablauf dieser Zeit kann der Transponder in der Schließanlage nicht mehr verwendet werden.

Diese Funktion ist unabhängig bzw. nicht in Verbindung von der Virtuellen Vernetzung zu verwenden, da diese nur durch das Programmiergerät geändert bzw. aktualisiert werden kann.

2.5 Listen

2.5.1 Zutrittslisten

In den Schließungen werden in den Produkten mit ZK-Funktionalität Zutritte in der Zutrittsliste der Schließung abgespeichert. Folgende Informationen können mittels der SimonsVoss Software aus der Zutrittsliste entnommen werden:

- Datum
- Uhrzeit
- TID
- Name des/der Nutzer(in)

Anbei die Auflistung der Größen der Zutrittslisten in den entsprechenden Schließungen je nach Konfiguration mittels der Programmiersoftware:

	Standard	Gateway
Zylinder	Bis zu 3.000	/
Smart Relais	Bis zu 3.600	Bis zu 200

2.5.2 Begehungslisten

Zusätzlich zu den Zutrittslisten in den ZK-Schließungen, ist eine Begehungsliste in den G2 Transpondern integriert.

Hierbei werden die letzten bis zu 1.000 Begehungen (je G2 Schließanlage) mit Datum, Uhrzeit und Lock-ID (LID) im Transponder gespeichert.

2.6 Protokollgenerationen

2.6.1 G1 Schließanlagen

Vom System wird nur die Protokollgeneration 1 unterstützt. Hierbei können alle bisherigen angebotenen G1 Produkte eingebunden und es können alle bisherigen Funktionen konfiguriert und verwendet werden. Bei Nutzung der G1 Datensätze auf den neuen G2 Transpondern werden die Expiry-Funktionen der G1 Protokolle (z.B. in Verbindung mit den Validation-Terminals) nicht unterstützt.

2.6.2 G2 Schließanlagen

Vom System wird nur die Protokollgeneration 2 unterstützt. Für diese stehen neue Produkte zur Verfügung, die alten G1 Protokolle werden dann in den Komponenten komplett deaktiviert.

2.6.3 G1 und G2 Schließanlagen getrennt

Hierbei können sowohl G1 als auch G2 Produkte verwendet werden, allerdings in komplett unterschiedlichen Schließanlagen. D.h. der Nutzer hat jeweils einen Datensatz bzw. eine Schließanlage der Generation 1 und der Generation 2 auf dem Transponder gespeichert.

Vorteil: Klare Trennung der unterschiedlichen Versionen

Beide Schließanlagen werden in einem Schließplan bzw. einer Datenbank verwaltet, und in der LSM 3.0 oder höher kann zwischen beiden in der gleichen Matrix gewechselt werden. D.h. es ist nur der entsprechende Schließplan für G1 bzw. G2 zu erkennen (Übersichtlichkeit!).

2.6.4 G1 und G2 Schließanlagen gemischt (Kompatibilitätsmodus)

Es werden G1 und G2 Komponenten in einer Schließanlage gemeinsam verwaltet. G1 Komponenten arbeiten weiterhin nur mit G1 Funktionalitäten, können aber auch vermischt betrieben werden. Somit sind auch Produkte der Protokollgeneration 2 kompatibel zur Protokollgeneration 1.

Vorteil: Nur eine Schließanlage zu betreuen

Nachteil: Unterschiedliche Protokollgenerationen werden in einer Schließanlage betreut (eingeschränkte Unterscheidbarkeit und Übersichtlichkeit). Hierbei kann es zu funktionalen Einschränkungen kommen. Nur für sehr erfahrene Benutzer, deshalb empfehlen wir wenn immer möglich getrennte Schließanlagen anzulegen!

2.7 Batteriewarnungen

Die Batteriewarnung ist identisch aufgebaut wie bei den Zylindern mit den Protokollen der G1 Generation. Hiervon ausgenommen sind die neuen SmartCard-Produkte, siehe hierzu die aktuellen Beipackzettel und Handbücher.

2.7.1 G2 Batteriewechsel-Transponder

Bei Nichtbeachtung der Batteriewarnungsmeldungen der Zylinder wechselt dieser nach der Batteriewarnstufe 2 in den Freeze-Modus. Bei den Protokollen der Generation 1, musste nun mit dem Programmiergerät überprogrammiert werden, um den Lagermodus und die Batteriewarnungen zu entfernen und diesen wieder einkuppeln zu können.

In der LSM (ab Version 3.0) kann in G2 Schließanlagen ein G2 Batteriewechsel-Transponder erstellt werden. Mit diesem kann der Freezemode durch Betätigen am Zylinder aufgehoben werden, die Öffnung erfolgt dann mit einem berechtigten Transponder. Somit entfällt der Aufwand mit dem Programmiergerät zur Schließung zu gehen.

Achtung: Hierbei werden bei jeder Öffnung die Batterien bei bestehender Batteriewarnung weiter entleert. Das kann bei nicht zweckmäßiger Verwendung zu einer völligen Entleerung der Batterien führen! Die Batterien müssen in diesem Zustand sofort erneuert werden.

3.0 G2 PRODUKTE.

Um die G2 Protokolle mit vollem Funktionsumfang nutzen zu können sind alle Produkte mit Unterstützung der neuesten Protokollgeneration notwendig. Zur Verfügbarkeit von einzelnen Produkten siehe die jeweils aktuelle SimonsVoss Preisliste.

3.1 Programmiergeräte

Für die Programmierung von G2 Komponenten ist ein Programmiergerät ab Firmware 9.10.4.XX, für die neuen SmartCard-Produkte ab 9.10.4.34, oder höher notwendig. Eine Abwärtskompatibilität zur Protokollgeneration1 ist vorhanden, d.h. mit dem Programmiergerät können sowohl G1 als auch G2 Komponenten programmiert werden.

3.2 Zylinder

Alle Zylindervarianten können mit der Protokollgeneration 2 bestellt werden.

3.3 Zylinder - SC

Die Zylindervarianten SmartCard (SC) sind ausschließlich mit der Protokollgeneration 2 verfügbar.

3.4 SmartHandle

Alle SmartHandle Versionen können mit der Protokollgeneration 2 bestellt werden.

3.5 SmartHandle - SC

Alle SmartHandle Versionen SmartCard (SC) sind ausschließlich mit der Protokollgeneration 2 verfügbar.

3.6 Smart Relais

Die SmartRelais (Standard, ZK) können mit der Protokollgeneration 2 bestellt werden.

3.7 Transponder

Für die Verwendung mit den neuen Protokollen kommt eine neue Transpondergeneration zur Anwendung, welche speziell für den Einsatz mit den neuen Protokollen entwickelt wurde.

3.8 Netzwerk

Bestehende WaveNet-Netzwerke (Router) bzw. integrierte LockNodes (LockNode Inside) betreffen die Umstellung nicht. Diese können ohne Änderungen zur Nachprogrammierung von G2 Funktionen genutzt werden. Externe LockNode können weiterhin zu Türüberwachung genutzt werden, stehen allerdings nicht mehr zur Umprogrammierung zur Verfügung. Hier können integrierte LockNodes verwendet werden.

4.0 SIGNALISIERUNG.

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

4.1 Beschreibung Transaktionssignalisierung

Funktion	Beschreibung	Signalisierung
Transaktion ok, Schließung wird mechanisch aktiv	Zylinder kuppelt ein	2x kurz
Schließung wird mechanisch inaktiv	Zylinder kuppelt aus	1x kurz
Flip-Flop Modus (ein)	Zylinder kuppelt ein	1x kurz, 1x lang
Flip-Flop Modus (aus)	Zylinder kuppelt aus	1x lang, 1x kurz
Vorgang kann nicht ausgeführt werden	Zylinder befindet sich im deaktivierten Zustand	1x kurz
	Zylinder befindet sich im Freeze-Modus	1x kurz
	Transponder ist ungültig	1x kurz

Im Gegensatz zu den G1 Protokollen wird dem Nutzer eine Nichtberechtigung durch ein Abwehrsignal angezeigt.

4.2 Beschreibung Zustandssignalisierung (aktive Komponenten)

Funktion	Beschreibung	Signalisierung
Kritischer Batteriezustand der Schließung	Batteriewarnstufe 1	8-fach 2x kurz (vor dem Einkuppeln)
Kritischer Batteriezustand der Schließung Flip-Flop-Modus	Batteriewarnstufe 1	Ca. alle 60 Sekunden 4-fach 2x kurz
Kritischer Batteriezustand der Schließung	Batteriewarnstufe 2	8-fach 2x kurz über 30 Sekunden (vor dem Einkuppeln)
Kritischer Batteriezustand des Transponders		8-fach 2x kurz (nach dem Auskuppeln)
Programmiervorgang		Je Packet 1x kurz
Neustart (Power-on-Reset)		3x kurz

Die akustischen Batteriewarnungen können bei Zylindern deaktiviert werden. Diese werden den Nutzern dann nicht mehr angezeigt. Ein Feedback seitens der Nutzer aufgrund entleerter Batterien entfällt in diesem Zustand.

4.3 Konfigurationsmöglichkeiten

4.3.1 Programmiervorgänge

Signalisierung der an die Schließungen gesendete Programmierpakete kann abgeschaltet werden. Bei der Programmierung über das Netzwerk werden die akustischen Programmierquittungen generell nicht angezeigt, da das akustische Feedback im Regelfall nicht wahrgenommen werden kann.

4.3.2 Transponderöffnung

Die im Rahmen eines Öffnungsprotokolles stattfindende Signalisierung der Schließung kann bei frei wählbaren Transpondern abgeschaltet werden.

5.0 NUTZUNGSSZENARIEN.

5.1 Neue Schließanlage

5.1.1 Anlagengröße: Weniger als 100 Türen, Offline-Betrieb

Die Türen sind unmittelbar erreichbar, und eine Begehung von Türen im Falle eines Transponderverlustes, oder einer Änderung ist unproblematisch (kleinere bis mittlere Schließanlage mit weniger als 100 Türen)?

Dann kommt als kostengünstigste Variante, eine **SimonsVoss G1** Anlage, in Frage. Hierfür stehen ein breites Spektrum an Zubehör (Möbelschlösser, Schaltschrankgriffe, Pincodes Tastaturen etc.) zur Verfügung und einzelne oder alle Türen können jederzeit, auch nachträglich, vernetzt werden.

5.1.2 Anlagengröße: Weniger als 100 Türen, Mischbetrieb: Offline/Online

Alle Türen sind unmittelbar erreichbar, eine Begehung von Türen im Falle eines Transponderverlustes, oder einer Änderung ist unproblematisch (kleinere bis mittlere Schließanlage mit weniger als 100 Türen), jedoch sollen einige Türen überwacht werden oder im Falle eines Transponderverlustes zeitnah reagieren zu können (z.B. einige sicherheitskritische, oder weit entfernte Türen)?

Dann kommt als kostengünstigste Variante, eine **SimonsVoss G1 Anlage**, in Frage. Die kritischen Türen können direkt als **Online Variante** umgesetzt werden. Es steht ein breites Spektrum an Zubehör (Möbelschlösser, Schaltschrankgriffe, Pincodes Tastaturen) zur Verfügung und weitere Türen können jederzeit, auch nachträglich, vernetzen.

5.1.3 Anlagengröße: Weniger als 100 Türen, Online-Betrieb

Die Schließanlage besteht fast ausschließlich aus sicherheitskritischen Türen, an denen im Falle eines Transponderverlustes sofort reagiert werden muss. Außerdem müssen viele Türen überwacht werden um z.B. Alarme auszulösen, oder permanent Zutrittsprotokolle einsehen zu können? Eigentlich hatten Sie über eine Online Zutrittskontrolle nachgedacht.

Dann kommt die Onlinevariante, eine **voll vernetzte SimonsVoss G1 Anlage**, in Frage. Es steht ein breites Spektrum an Zubehör (Möbelschlösser, Schaltschrankgriffe, Pincode Tastaturen) zur Verfügung.

5.1.4 Anlagengröße zwischen 100-500 Türen

Betrieben wird eine normale Schließanlage (100 bis 500 Türen), ein Begehen von Türen im Falle eines Transponderverlustes ist denkbar, aber bei der normale Berechtigungsvergabe oder bei Änderungen soll bedarfsorientiert entschieden werden, ob besser betroffene Transponder oder betroffene Türen programmiert werden sollen.

Dann kommt eine **SimonsVoss G2 Anlage** in Frage. Alle Standardkomponenten (Transponder, Zylinder, SmartRelais) sind mit den neuen G2 Protokollen ausgerüstet, die es ermöglichen immer wahlweise Türen oder Transponder zu programmieren. Einzelne oder alle Türen können jederzeit, auch nachträglich, vernetzt werden.

5.1.5 Anlagengröße: Mehr als 500 Türen

Die Schließanlage ist sehr groß oder sehr unübersichtlich. Sie besteht aus sehr vielen, teilweise auch sehr entfernt liegenden Türen. Eine Begehung im Falle eines Transponderverlustes, ist sehr schwierig umzusetzen. Viele Türen werden darüber hinaus als sicherheitskritisch betrachtet und müssen überwacht werden.

Dann kommt eine **virtuell vernetzte SimonsVoss G2 Anlage** in Frage. Alle Standardkomponenten (Transponder, Zylinder, SmartRelais) sind mit der G2 Firmware ausgerüstet. Alle Änderungen werden von einem zentralen Rechner zu Gateways übertragen und dort täglich auf die Transponder geschrieben. Die Transponder besitzen eine eingeschränkte Gültigkeit (typischer Weise maximal 12 Stunden), so dass bei einer Deaktivierung eines verlorenen Transponders dieser spätestens nach Ablauf dieser Gültigkeit nicht mehr funktioniert. Die Gateways stehen als Onlinevariante zur Verfügung und einzelne oder alle Türen können jederzeit, auch nachträglich, vernetzt werden.

5.2 Schließanlagenerweiterung

5.2.1 Anlagengröße: Deutlich mehr als 100 Türen

Es existiert eine mittlere bis große (deutlich mehr als 100 Türen) SimonsVoss G1 Schließanlage welche bislang noch nicht an die Systemgrenze gestoßen ist (8.000 verschiedene Transponder oder 16.000 verschiedene Türen)? Bei Erweiterung sollen die Türen nicht mehr begangen werden um dort Änderungen zu programmieren?

Erweiterung um wenige Türen:

In diesem Fall kann die Anlage mit **SimonsVoss G1 online Komponenten** erweitert werden.

Erweiterung um viele Türen:

In diesem Fall wird für Erweiterungen des Systems eine **SimonsVoss G2 Schließanlage** verwendet. Diese Schließanlage kann parallel zu ihrer G1 Anlage aufgebaut werden, und wird in einem Schließplan verwaltet. Die neuen G2 Transponder können auch in der G1 Anlage verwendet werden. Falls Personen mit G1 Transpondern (aus dem alten System) auch in der neuen Anlage schließen sollen, bitte die vorhandenen G1 Transponder gegen G2 Transponder austauschen.

Die neue G2 Anlage kann **wahlweise mit virtueller Vernetzung** ausgestattet werden. Alle Änderungen werden von einem zentralen Rechner zu Gateways übertragen und dort täglich auf die Transponder geschrieben. Die G2 Transponder besitzen dann eine eingeschränkte Gültigkeit (typischer Weise maximal 12 Stunden auf G2 Schließkomponenten), so dass bei einer Deaktivierung eines verlorenen Transponders dieser spätestens nach Ablauf dieser Gültigkeit nicht mehr funktioniert. Die Gateways stehen als Onlinevariante zur Verfügung, und einzelne oder alle Türen können jederzeit, auch nachträglich, vernetzt werden.

5.2.2 Anlagengröße: Systemgrenzen G1 erreicht

Die existierende SimonsVoss G1 Anlage stößt langsam an die Systemgrenzen (mehr als 8.000 verschiedene Transponder, oder mehr als 16.000 verschiedene Türen)?

In diesem Fall wird für die Erweiterung des Systems eine **SimonsVoss G2 Schließanlage** verwendet. Diese Anlage wird parallel zur G1 Anlage aufgebaut, und die G2 Transponder können auch in der G1 Anlage verwendet werden. Falls Personen mit G1 Transpondern (aus dem alten System) auch in der neuen Anlage schließen sollen, bitte die vorhandenen G1 Transponder gegen G2 Transponder austauschen.

Die neue G2 Anlage kann **wahlweise mit virtueller Vernetzung** ausgestattet werden. Alle Änderungen werden von einem zentralen Rechner zu Gateways übertragen und dort täglich auf die Transponder geschrieben. Die G2 Transponder besitzen dann eine eingeschränkte Gültigkeit (typischer Weise maximal 12 Stunden auf G2 Schließkomponenten), so dass bei einer Deaktivierung eines verlorenen Transponders dieser spätestens nach Ablauf dieser Gültigkeit nicht mehr funktioniert. Die Gateways stehen als Onlinevariante zur Verfügung, und einzelne oder alle Türen können jederzeit, auch nachträglich, vernetzt werden.

6.0 ANHANG.

6.1 Übersicht Unterschiede G1 und G2 Protokolle

	G1	G2	G2 + VN
Schließungen	16.000	64.000	64.000
Transponder	8.000	64.000	64.000
Zeitzonengruppen	5 + 1	100 + 1	100 + 1
Basis Informationen	Transponder		Schließungen
Schließplaninformationen	Schließungen	Transponder oder Schließungen	Transponder
Gateways (Online)	Nein	Nein	Ja
Netzwerk	Ja	Ja	Ja (nur Gateways)

Bei Nutzung der G2 Protokolle ohne Virtuelle Vernetzung kann bei jedem Programmiervorgang wahlweise festgelegt werden was umprogrammiert wird. D.h. es können jeweils sowohl die Transponder als auch die Schließungen umprogrammiert werden, da die Schließungen eine Transponderliste und die Transponder eine Schließungsliste speichern bzw. verwalten können.

6.2 Begriffserklärung

Begriff	Erläuterung
ASM	Anlagenstatusmonitoring
Bereich	Zusammenfassung mehrerer Schließungen zur leichteren Berechtigungsverwaltung
Begehungsliste	Liste von begangenen Schließungen, welche auf dem Transponder gespeichert wird
Datenbank	Speicherung aller Informationen des Schließplans bzw. der Schließanlage des SimonsVoss Systems 3060
Direktvernetzung (Netzwerk Inside)	Netzwerkknoten (LockNode) direkt in den Schließzylinder integriert
Gateway	Anbindung des virtuellen Netzwerkes an die Verwaltungssoftware.
Protokollgeneration 1 (G1)	Aktuelle Protokollgeneration der B-Feld Schnittstelle
Protokollgeneration 2 (G2)	Neue Protokollgeneration der B-Feld Schnittstelle
LID	Lock-ID: Eindeutige Kennung einer Schließung innerhalb einer SimonsVoss Schließanlage
LSM	Locking-System-Management: Datenbankgestützte PC-Software zur Verwaltung der SimonsVoss Schließanlage
LockNode	Netzwerkknoten zur direkten Nahfeldkommunikation mit einer Schließung
Mechanisch aktiv	Mechanischer Zustand einer Schließung, der es dem

	Anwender ermöglicht einen Öffnungs- bzw. Schließvorgang durchzuführen.
Mechanisch inaktiv	Mechanischer Zustand einer Schließung, in dem es nicht möglich ist einen Öffnungs- bzw. Schließvorgang durchzuführen.
Netzwerk	SimonsVoss WaveNet Netzwerk. Hiermit können Schließungen im Onlinemodus betrieben werden
Schließanlage	Zusammengehörige, gemeinsam verwaltete Menge von Schließungen und Transpondern
Schließanlagenpasswort	Passwort zur Absicherung der Schließanlage
Schließplan	In einem Schließplan ist es möglich mehrere Schließanlagen zu verwalten.
SID	Schließanlagen-ID: Nummer einer Schließanlage
Schließung	Oberbegriff für alle Produkte, welche mit einem Transponder angesprochen werden können
SmartCD	Programmiergerät: Gerät zur Programmierung von SimonsVoss Komponenten.
TID	Transponder-ID: eindeutige Kennnummer eines Transponders
Transponder	Medium um mit einer Schließung kommunizieren zu können
Transpondergruppen	Zusammenfassung mehrerer Transponder zu einer Gruppe zur leichteren Berechtigungsverwaltung
Virtuelles Netzwerk	Technologie um bei Offline-Schließanlagen Berechtigungsänderungen über Gateways durchzuführen ohne die Schließungen aufsuchen zu müssen.
Zeitzonengruppen	Gruppen als Bestandteil eines Zeitzonenplans
Zeitzonepläne	Zeitzoneplan, welcher in einer Schließung hinterlegt werden kann
Zutrittsliste	Liste von Begehungen, welche in der Schließung gespeichert wird
Zutrittsprofil (Transpondergruppen/ Bereiche)	Definiert die Menge von Schließungen, welche mit einem Transponder, auf dem sich dieses Profil befindet, angesprochen werden können