G2 protocols

Manual

29.08.2020

SimonsVoss technologies

Contents

1 General safety instructions

Signal word (ANSI Z535.6)	Possible immediate effects of non-compliance
DANGER	Death or serious injury (likely)
WARNING	Death or serious injury (possible, but unlikely)
CAUTION	Minor injury
IMPORTANT	Property damage or malfunction
NOTE	Low or none

WARNING

Blocked access

Access through a door may stay blocked due to incorrectly fitted and/or incorrectly programmed components. SimonsVoss Technologies GmbH is not liable for the consequences of blocked access such as access to injured or endangered persons, material damage or other damage!

Blocked access through manipulation of the product

If you change the product on your own, malfunctions can occur and access through a door can be blocked.

- Modify the product only when needed and only in the manner described in the documentation.

NOTE

Intended use

SimonsVoss-products are designed exclusively for opening and closing doors and similar objects.

- Do not use SimonsVoss products for any other purposes.

Different times for G2 locks

The internal time unit of the G2 locks has a technical tolerance of up to ± 15 minutes per year.

Qualifications required

The installation and commissioning requires specialized knowledge.

- Only trained personnel may install and commission the product.

The German language version is the original instruction manual. Other languages (drafting in the contract language) are translations of the original instructions.

Read and follow all installation, installation, and commissioning instructions. Pass these instructions and any maintenance instructions to the user.

2 General information

The G2 protocols are a completely new development in SimonsVoss communication between identification media and locking devices. Many new functions have been implemented to give you even easier and better options for managing your locking system.

Based on the G2 protocols, suitable hardware products and fully modular software are available to help you adapt your locking system even better to your personal requirements.

3 G2 protocols

3.1 General description

The G2 protocols enable new functions in System 3060 if the prerequisites are fulfilled:

- LSM Version 3.0 or higher
- G2 hardware products

3.1.1 Locking system password

You only need the locking system password when creating the locking plan. The security of the locking system password is also increased:

- Minimum length 64 bit
- Integrated quality index in the LSM software

The LSM software therefore no longer permits unsafe locking system passwords and increases the security of your locking system.

3.1.2 Locking system size

The G2 protocols redefine the limits of your locking system. You can now administer

- up to 64000 locking devices per locking system
- up to 64000 identification media per locking device

. Over four billion possible individual authorisations per locking system enable you to adapt your locking system to your individual requirements without compromise.

3.1.3 Common locking levels

You can use overlapping locking levels to use certain functions in several locking systems. These functions are secured by their own password, independent of the locking system (so-called cross-locking systems). Three superordinate locking levels are available:

- Red locking level
- Green locking level
- Blue locking level

Each transponder can belong to one of the three levels. In the LSM, 1024 transponder IDs are reserved for each higher-level locking level. You can therefore assign a maximum of 1024 transponders to a higher-level locking level. You can assign individual authorisations for each of these transponders or lock the transponders individually.

Transponders that you have assigned to the red lock level can also open deactivated locks. These remain engaged or open for the set pulse duration, but are still deactivated. If you store a transponder at the red locking level in a fire brigade key depot, for example, rescue personnel can advance quickly in the building in the event of danger.

3.1.4 Emergency release

If you have networked your locking system, you can activate your locking devices via your network (WaveNet). To do this, send a command from the LSM software via the network to the desired locking devices that permanently engages the locking devices. Anyone can access these locking devices independently of identification media.

Locking devices that you have opened using the emergency release command remain open until you cancel the emergency release command with an emergency opening command or a remote opening command.

A fire alarm system can trigger an event via a contact in the LSM software, the reaction of which sends this command. In the event of a fire, all locking devices that receive the command are thus opened. Persons that are locked in can leave the building and rescue teams can move forward quickly in the building.

Authorised identification media used on emergency released locking devices have no function.

3.1.5 Emergency opening

You can assign a temporary password in the LSM software during the export to LSM Mobile. This password must be at least eight characters long, but has no further restrictions.

With this password, an emergency opening can then be performed on a locking device on site without the locking system password having to be known.

As an administrator, you can restrict this function for security reasons:

- Number of possible emergency openings
- Period in which emergency openings are possible

3.1.6 Pulse length

You can freely select engage times between one and 25 seconds for locking cylinders and SmartRelays.

At the same time, you can use the LSM function "Long opening" to allow individual identification media a longer engage time. This function doubles the engage time, whereby the total engage time is still limited to 25 seconds.

Influence engage times for all locking devices	Pulse length in the locking device configuration
Influence engage times for individual identification media	"Long opening" in the configuration of the identification medium

3.1.7 Acoustic opening signal

Locking devices emit an audible opening signal. This acoustic opening signal can be disturbing, for example in a hospital. Opening doors at night would wake patients up when using an audible opening signal.

You can deactivate this acoustic opening signal for each identification medium. This enables you to mute locking devices for individual or all identification media.

3.2 Issuing of authorisation

3.2.1 General information

The new G2 protocols reduce your administrative effort after the issue of new identification media. Intelligent mechanisms in the protocols largely avoid the previously necessary reprogramming of your locking devices on site.

As an alternative to reprogramming your locking devices on site, you can also transfer authorisations to your locking devices as follows:

- G2 without networking
  - Direct transmission: Via identification media and locking devices
  - Blockings: Via replacement identification media
- Indirect transmission: G2 with virtual networking (VN), see *Virtual network (VN) [▸ 10]*
- Network transmission: WaveNet

3.2.2 G2 without networking

If you use a G2 locking system without a network, you save a lot of time when creating new locking devices or new identification media. In this case, you no longer need to programme identification media and locking devices with the G2 protocols:

New locking device	■ Save the authorisations on the identification medium (programming the identification medium) or ■ save the authorisations in the locking devcie (programming the locking device).
New identification medium	

There is no further programming effort in your locking system. As a locking system administrator, you have a completely open system at your disposal. When programming, you can decide whether to save the authorisations on the identification medium or in the locking device - depending on which is more convenient for you.

Locking devices

You can manage up to 64000 identification media in each locking device, i.e. individually authorise and block them. The programming procedure is basically identical to the programming procedure for G1 locking devices. Up to 64000 locking devices can be stored and managed in each G2 locking system.

Identification media

In your G2 locking systems, you can store individually in each identification medium for which locking devices this identification medium is authorised. The new G2 transponders can store and manage up to three G1 locking systems and four G2 locking systems - so the entire locking plan can be stored on the transponder in G2 locking systems.

Replacement transponders and locking IDs

With the introduction of LSM 3.0 SP2, you can use replacement identification media to block other identification media (such as those that have been stolen). If you program the substitute identification medium, select the identification medium to be locked and transfer a lock ID to the identification medium. As soon as the replacement identification medium is operated on a locking device, the replacement identification medium transfers the lock ID to the locking device and the identification medium to be locked is no longer authorised for this locking device.

The programming requirement for the locking devices remains and is only cancelled when you re-programme the locking devices for which the identification medium to be locked was previously authorised.

3.3 Virtual network (VN)

In a virtual network, the locking devices are only given basic information when they are first programmed and are permitted in your locking system. Authorisations are stored exclusively on the identification media.

If the authorisations change, the authorisations only need to be updated in the identification media. In virtual networks there are so-called gateways for this purpose. The users operate the identification media on the gateways and thus start data transmission. If authorisation changes have been made, the gateway updates the authorisations in the identification media. As the locking system administrator, you no longer have to reprogram locking devices or identification media if you change authorisations.

3.3.1 Gateways

The gateways are available as an online variant. In a SimonsVoss network, data is transferred between the gateway and the identification medium:

- Authorisation changes (positive and negative) from the gateway to the identification medium
- Locking IDs from the gateway to the identification medium
- Acknowledgements of the locking system stored on the identification media from the identification medium to the gateway

There is no need to program the locking devices using a programming device. Instead, the locking system is reprogrammed via the gateways or the users of the identification media.

You can use the LSM SmartRelay as possible gateways for your locking system.

3.3.2 Direct authorisations

Authorisation changes transferred to the gateways can be deleted or new authorisations assigned directly in the identification medium and are therefore effective immediately. If you want to lock identification media, the gateways can also transfer this information (locking ID) to the identification media. The users of the identification media then use their identification media to transfer this information to the locking devices in your locking system.

The locking device stores the successful receipt of authorisation changes by an identification medium as feedback on subsequent identification media (acknowledgement management). The users of the identification media then return this feedback to the gateway. The gateway saves the successful transmission in the database and LSM no longer displays any programming requirements for the corresponding locking devices.

As the locking system administrator, you thus retain an overview of which locking devices have already received the authorisation change and which have not. You know the status of your locking system.

3.3.3 Locking IDs (Lock priority)

You assign and withdraw authorisations in the LSM or block and deactivate identification media and transfer the authorisation changes to the locking devices with a gateway via identification media.

The authorisations stored on the identification media themselves are normally used in a virtual network. If an identification medium is to be blocked and the authorisations on this identification medium are still used, this identification medium could continue to open locking devices as long as the authorisations on this identification medium are not changed by a gateway.

This is prevented by a lock priority set for the ID of the identification medium. If an identification medium is no longer authorised for a locking device, a lock priority is set for its ID. The gateway transmits the lock priority to the locking devices via other identification media.

If a lock priority is set in a locking device for an ID of an identification medium, the authorisation for this locking device that may still exist on this identification medium and is normally used is ignored. Instead, the authorisations that are stored in the locking device itself and are updated in a virtual network by the identification media apply (and are therefore more up-to-date).

At the same time, the ID of the identification medium blocked in this way is stored in a blacklist and can therefore not be reactivated accidentally.

3.3.4 Expiry date

For an effective use of the virtual network, it is necessary that the gateway can regularly transfer data to and from the identification media. As a locking system administrator, you can use an expiry date to "force" the users of your locking system to regularly operate their identification media at the gateway.

An expiry date limits the validity of an identification medium. Users must regularly top up their time credit at a gateway, otherwise they cannot use any locking devices (including offline locking device) until the time credit at a gateway has been topped up. There are two options for this time credit:

- Fixed number of hours between one and 255 hours (e.g. authorisation for eight hours after recharging)
- Fixed expiration time between 1:00 p.m. and 12:00 a.m. (e.g. authorisation between charging time and 8:00 p.m.)

You set this time credit in LSM globally for all identification media. However, you can also define an individual time credit for individual transponders. General changes (e.g. the duration of the time credit) are programmed directly with LSM.

3.3.5 Setting the time

The locking devices and transponders are equipped with a time module. If a transponder is operated on a gateway, the time block in the transponder is reset (and any previous or subsequent times in the transponder are corrected). The time in the transponder serves as a reference when a lockinf device is actuated. If the time in the locking device differs during actuation, the time module in the locking device is reset after the time in the transponder (and corrected in the locking device, if necessary).

The time in the locking devices in your virtual network is automatically reset on a regular basis without you having to reprogram the locking devices manually as the locking system administrator.

3.4 Time control

You can use time zone control to limit the period (time zone) during which certain identification media (and thus persons or groups of persons) can activate a locking device (and thus enter the building, for instance).

3.4.1 Time zones

You can create any time zone plans and assign a time zone plan to each area individually. A time zone plan contains up to one hundred time zone groups that can be freely configured with different access times. In the different time zone plans, you can select or configure the time zone groups differently.

3.4.2 Public holidays

In addition to the seven weekdays (Monday to Sunday), you can also enter special or public holidays in the time zone plans.

To do this, simply use the holiday lists stored in the LSM software (for all German federal states) instead of creating them yourself. Alternatively, you can create your own holiday lists independently of the holiday lists supplied. Any day can be saved as a holiday and can be treated like a Sunday (also see *Special days [▸ 12]*).

3.4.3 Special days

A special day defines a time profile for certain days that is independent of the seven days of the week. Special days have a higher priority than public holidays.

For example, you can use special days to allow access for school staff during school hours from Monday to Friday, and to generally block access during holidays with special days (with higher priority).

3.4.4 Validation date

You can assign any validation date to transponders. Transponders with a validity date can only be used in the locking system after this validation date.

This function is independent of virtual networking (see *Expiry date [▸ 11]*) and can only be changed by the programming device. Do not use this function in conjunction with virtual networking.

3.4.5 Expiry date

You can assign any expiry date to transponders. Transponders with an expiry date can no longer be used in the locking system after this expiry date.

This function is independent of virtual networking (see *Expiry date [▸ 11]*) and can only be changed by the programming device. Do not use this function in conjunction with virtual networking.

3.5 Lists

3.5.1 Access lists

Locking devices with ZK function log the accesses in an access list:

- Date
- Time
- ID of the identification medium
- Name of the user

You can read and display the access list with the LSM software. The number of entries in the access list depends on the locking device and the configuration.

	Standard	Gateway
Cylinder	Up to 3000	
SmartRelay	Up to 3600	Up to 200

3.5.2 Physical access lists

G2 transponders log the accesses in an access list independently of access lists. The last accesses (up to 1000) are stored in this physical access list:

- Date

- Time
- ID of the locking device

You can read and display the physical access list with the LSM software.

3.6 Protocol generations

3.6.1 G1 locking systems

Only G1 products and only G1 functions can be used in G1 locking systems.

If you use G1 data records in G2 transponders, the expiry functions of the G1 protocols (for example with validation terminals) are not supported.

NOTE

G1 products are being discontinued

G1 products are no longer available.

3.6.2 G2 locking systems

Only G2 products and only G2 functions can be used in G2 locking systems.

3.6.3 G1 and G2 locking systems separately

This approach allows you to separate the different protocol generations into (at least) two different locking systems. Each identification medium then stores (at least) two independent locking system data records (one each from G1 and G2).

The advantage of this approach avoids compatibility problems from the beginning

You manage these locking systems in the same locking plan or database. As of LSM 3.0, you can filter the display in the matrix according to the protocol generation and, depending on the filter, only see the locking devices and identification media for G1 or G2.

3.6.4 G1 and G2 locking systems mixed (compatibility mode)

This approach allows you to manage the two different protocol generations in the same locking system.

- G1 products continue to use only G1 functions.
- G2 products are operated in compatibility mode.

You only need to manage a single locking system, but mixing G1 and G2 restricts clarity and differentiation.

NOTE

Functional limitations due to mixed operation

The use of mixing systems can lead to functional limitations and requires experience.

1. Avoid mixed locking systems.
2. Use separate locking systems instead (see *G1 and G2 locking systems separately [▸ 14]*).

3.7 Battery warnings

The battery warnings for cylinders with G2 protocol are identical to those for cylinders with G1 protocol (exception: Mifare cylinders, see the relevant manuals/quick guides).

3.7.1 G2 battery change transponder

Cylinders with very weak batteries can no longer be operated with normal identification media in order to prevent complete discharge (G1: storage mode, G2: freeze mode).

The storage mode and battery warnings for cylinders with G1 protocols can only be cancelled with the local programming device.

As of LSM 3.0, the G2 protocol enables so-called battery change transponders. You can use a battery change transponder to cancel the freeze mode of G2 locking cylinders and operate the locking device with a normal authorised transponder. You do not have to be on site with the programming device to activate the locking device.

CAUTION

Depleting batteries through misuse

The battery is depleted further each time it opens a locking device in conjunction with a battery replacement transponder. This may lead to the batteries being fully discharged if the transponder is not used for its intended purpose! The batteries must be replaced immediately in such cases.

4 G2 products

If you want to use all functions of the G2 protocols, you may only use G2 products. You can find information on the availability of G2 products in the current SimonsVoss price list.

4.1 Programming devices

To program G2 components, you need a programming device with suitable firmware:

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

The firmware is downward compatible. You can also use programming devices with new firmware to program the previous G1 components.

4.2 Cylinder

Product	G1-compatible	G2-compatible
Standard cylinder (25 kHz)	Yes	Yes
Mifare/SmartCard cylinder	No	Yes

4.3 SmartHandle

Product	G1-compatible	G2-compatible
SmartHandle 3062 Standard (25 kHz)	Yes	Yes
SmartHandle 3062 Mifare/SmartCard	No	Yes
SmartHandle AX Standard (25 kHz)	Yes	Yes
SmartHandle AX Mifare/SmartCard	No	Yes

4.4 SmartRelay

Product	G1-compatible	G2-compatible
SmartRelay	Yes	Yes
SmartRelay 2	Yes	Yes
SmartRelay 3	Yes	Yes

4.5 Transponder

You will receive all transponders as a G2 product.

4.6 Network (WaveNet)

Your WaveNet (RouterNodes and LockNodes) can address G1 and G2 products. External LockNodes are also partially supported in G2 components.

	Door monitoring	Post-programming
Internal LockNodes	Yes	Yes
External LockNodes	Yes	No

5 Signalling

A distinction is made between transponder signalling (e.g. OK) and status signalling (e.g. battery warning).

5.1 Transaction

Position	Description	Signalling
Transaction is ok Locking device engages	Locking device engages	2x short
Locking device disengages	Locking device disengages	1x short
Flip-flop mode (engages)	Locking device engages	1x short, 1x long
Flip-flop mode (disengages)	Locking device disengages	1x long, 1x short
Process cannot be executed	Locking device is deactivated	1x short
	Locking device is in freeze mode	1x short
	Identification medium is invalid	1x short

G2 products use a warning signal to indicate to the user that his identification medium is not authorised.

5.2 Status

Position	Description	Signalling
Critical battery condition of the locking device	Battery Warning Level 1	8x short (before engaging)
Critical battery condition of the locking device (locking device is in flip-flop mode)	Battery Warning Level 1	approx. every 60 seconds 4x double short
Critical battery condition of the locking device	Battery Warning Level 2	8x short with one second pause for 30 seconds (before engaging)

Position	Description	Signalling
Critical battery condition of the locking device	Freeze mode	6x long-short
Critical battery condition of the transponder		8x double short (after disengaging)
Programming procedure		1x short (depending on the programming data)
Restart (Power-On-Reset)		3x short

You can deactivate the acoustic battery warnings for cylinders. The cylinder no longer signals empty batteries to users in this state.

5.3 Configuration options

5.3.1 Programming operations

You can deactivate the locking device-side signalling of a programming.

5.3.2 Opening

You can deactivate the locking device-side acoustic signalling of a programming for individual identification media. This deactivation applies to this identification medium throughout the locking system.

6 Extension

6.1 Extend G1

G1 devices are no longer available. If you have previously used a G1 locking system and need new devices, then extend your G1 locking system with a G2 locking system. You can operate the locking systems separately (see *G1 and G2 locking systems separately [▸ 14]*) or mixed (see *G1 and G2 locking systems mixed (compatibility mode) [▸ 14]*).

Possible virtual networking, partial networking or full networking increases your convenience and can be retrofitted at any time (see *Differences: Networking [▸ 21]*).

6.2 Extend G2

You can extend and re-program your G2 locking system at any time according to your needs up to the limits of the G2 protocols.

Possible virtual networking, partial networking or full networking increases your convenience and can be retrofitted at any time (see *Differences: Networking [▸ 21]*).

7 Differences: Networking

	WaveNet (online)	Virtual networking (virtual)	No networking (offline)
Functional principle	Data transmission with networked WaveNet devices (see Transmission paths and Devices).	Data transmission with identification media (except programming data).	Data transmission with programming devices.
Extension	WaveNet devices are connected via various transmission media. All types of data are transmitted using these transmission media.	In a virtual network, certain data is transferred to the identification media using a gateway (entries in the blacklist). If you operate this identification media on a virtually networked locking device, the data is transferred to the locking device.	Locking devices that are not networked can only exchange data with the programming device. You must go to the locking devices with the programming device.
Programming effort	Low.	Low.	Effort depends on the size of the locking system. ▪ Small locking system: Low effort. ▪ Medium locking system: Medium effort. ▪ Large locking system: Extensive effort.
Transmission speed of the data exchange	Immediately. Data exchange with different transmission media.	Speed between gateway and locking devices highly dependent on the intensity of use of the locking devices. Identification media are transmission media - no data transmission without identification.	Slow.
Central activation/deactivation of locking devices	Possible.	Not possible.	Not possible.

	WaveNet (online)	Virtual networking (virtual)	No networking (offline)
Activation/deactivation centrally traceable	Possible.	Not possible.	Not possible.
Remote opening	Possible.	Not possible.	Not possible.
Remote monitoring (DoorMonitoring)	Possible.	Not possible.	Not possible.
Event management	Possible.	Not possible.	Not possible.
Access lists centrally retrievable	Possible.	Not possible (except SREL 3).	Not possible.
Software/ server independent protective functions	Possible.	Not possible.	Not possible.
Immediate locking device system-wide response to critical situations (availability of protective functions, see I/O configuration and protection functions and RingCast)	Possible.	Not possible.	Not possible.

8 Appendix

8.1 Differences between G1 and G2 protocols

	G1	G2	G2 (virtual network)
Locking devices	16000	64000	64000
Identification media	8000	64000	64000
Time zone groups	5+1	100+1	100+1
Basic information	Identification media		Locking devices
Locking plan information	Locking devices	Locking devices or identification media	Identification media
Gateways (online)	No	No	Yes
Network	Yes	Yes	Yes (only gateways)

If you use the G2 protocols without virtual networking, you can decide for each programming requirement whether you want to program the identification medium or the locking device. The locking devices can store an identification media list and the identification media a locking device list.

8.2 Glossary

Term	Explanation
ASM	Asset status monitoring
Area	Combining several locking devices for easier authorisation management
Physical access list	List of accessed locking devices stored on the identification medium
Database	Storage of all information of the locking plan or locking system of System 3060
Direct networking (LockNode Inside)	Network node (LockNode) directly integrated into the locking device

Term	Explanation
Gateway	Connection of the virtual network to the LSM software
G1	Old protocol generation of the B-field interface
G2	Current protocol generation of the B-field interface
LID	Lock-ID: Unambiguous identifier for a locking device within a Simons-Voss locking system
LSM	Locking System Management: Database-driven PC software used to manage a SimonsVoss locking system
LockNode	Network node for direct near-field communication with a locking device
Mechanically active	(=engaged) Mechanical state of a locking device that allows the user to open and lock it.
Mechanically inactive	(=disengaged) Mechanical state of a locking device that does not allow the user to open and lock it.
Network	SimonsVoss WaveNet. Locking devices can thus be operated in on-line mode (= networked).
Locking system	Related and jointly managed set of locking devices and identification media
Locking system password	Password to secure locking system
locking plan	A locking plan can consist of several locking systems
SID	Locking system ID: Unambiguous identification of a locking system in a SimonsVoss locking plan
Locking device	Generic term for all products that can be addressed with an identifica-tion medium.

Term	Explanation
SmartCD	Programming device: SimonsVoss products are programmed using a SmartCD
TID	Transponder ID: Unambiguous identifier of an identification medium in a SimonsVoss locking system
Transponder	Medium that can communicate with a locking device
Transponder groups	Grouping of several identification media into one group to be able to manage authorisations more easily
Virtual network	Technology with which authorisation changes are distributed via gateways during offline locking and the locking devices do not have to be physically accessed.
Time zone groups	Groups as part of a time zone plan
Time zone plans	Time zone plan that can be saved in the locking device
Access list	List of inspections that are stored in the locking device (prerequisite: ZK)
Access profile (transponder groups / areas)	Defines the number of locking devices that can be addressed with an identification medium on which this profile is located.

9 Help and other information

Information material/documents

You will find detailed information on operation and configuration and other documents under Informative material/Documents in the Download section on the SimonsVoss website (*https://www.simons-voss.com/en/downloads/documents.html*).

Declarations of conformity

You will find declarations of conformity for this product in the Certificate section on the SimonsVoss website (*https://www.simons-voss.com/en/certificates.html*).

Hotline

If you have any questions, the SimonsVoss Service Hotline will be happy to help you on +49 (0)89 99 228 333 (German fixed network; call charges vary depending on the operator).

Email

You may prefer to send us an email.

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

FAQs

You will find information and help for SimonsVoss products in the FAQ section on the SimonsVoss website (*https://faq.simons-voss.com/otrs/public.pl*).

Address

SimonsVoss Technologies GmbH
Feringastrasse 4
85774 Unterföhring
Germany

This is SimonsVoss

SimonsVoss is a technology leader in digital locking systems.

The pioneer in wirelessly controlled, cable-free locking technology delivers system solutions with an extensive product range for SOHOs, SMEs, major companies and public institutions.

SimonsVoss locking systems unite intelligent functions, optimum quality and award-winning German-made design. As an innovative system provider, SimonsVoss attaches great importance to scalable systems, effective security, reliable components, high-performance software and simple operation.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners. With its headquarters in Unterföhring, near Munich, and its production site in Osterfeld, eastern Germany, the company employs around 300 staff in eight countries.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide (www.allegion.com).

ALLEGION

SimonsVoss technologies