BIOMETRIC READER Q3008

Correct in: August 2007

SimonsVoss
technologies

1.0   General information

Please take 15 minutes to read this manual and familiarise yourself with the function of your Q3008 biometric reader.

To assemble the housing you will need a Torx key of size TX6.

1.1   Safety information

Caution! – The battery used in this product may present a risk of fire or burns if misused. Do not charge or open the battery. Do not heat it to over 100°C or burn it. Do not short-circuit.

Only use batteries which have been approved by SimonsVoss.

Dispose of old and used batteries in the correct way. Keep out of the reach of children.

Reversing the polarities may cause damage to the Q3008 biometric reader.

Do not allow the Q3008 biometric reader to become dirty or scratched. Do not drop it or subject it to any other sudden impact.

It is essential to ensure that the device does not come into direct contact with moisture and is not exposed to temperatures below +5°C.

The biometric reader is for indoor use only.

Master finger mode should only be used when the device is installed in a secure indoor location and with a very small number of doors.

Program the reader as soon as it is commissioned to prevent any risk of misuse.

If the reader fails to recognise a finger, or does not recognise it correctly, this does not necessarily mean there is a defect. SimonsVoss Technologies AG accepts no liability for poor recognition caused by skin dryness or the physical structure of the finger.

In order to configure a SimonsVoss biometric reader Q3008 you must be familiar with the product and SimonsVoss software. The Q3008 biometric reader should therefore only be programmed by trained specialists.

SimonsVoss Technologies AG shall assume no liability for damage caused by incorrect programming.

Access through a door may be denied if a Q3008 biometric reader is incorrectly programmed or is defective. SimonsVoss AG shall assume no liability for consequences such as denied access to injured persons or persons at risk, damage to property or any other form of damage.

SimonsVoss Technologies AG reserves the right to make enhancements and modifications to the product without notice. Consequently, descriptions and

representations in this documentation may vary from the most recent product and software versions.

Should there be any variations in the content of other language versions of the documentation, the German original shall apply in the event of any doubt.

This documentation has been produced to the best of our knowledge, but we cannot guarantee that it is free of errors. We therefore offer no guarantee and accept no legal responsibility for the consequences of any errors in this manual.

1.2 Description of product

The Q3008 biometric reader is a digital 'key' (transponder), designed to be mounted on a wall, which opens SimonsVoss locks by radio when it recognises an authorised fingerprint. The difference between this reader and, for instance, a PIN code keypad, is that it features a highly sensitive Atmel fingerprint strip sensor. A high-performance processor integrated in the reader compares learned fingerprints with the fingerprints read by the sensor. If the fingerprint is recognised, the reader addresses the lock, which can then be opened. This system offers maximum security against unauthorised use by third parties. This makes the Q3008 biometric reader particularly suitable for applications where only a few doors need to be accessed by just a few members of staff, or for additional security for doors or access to high-security areas.

For the system to be configured, the biometric reader must be programmed with the SimonsVoss programming software and it must learn a finger. Then, when the authorised finger is recognised, the appropriate lock is released.

The Q3008 biometric reader may only be used in indoor areas (IP41). The product has its own power supply and can therefore operate self-sufficiently. Assembly is very simple as there is no need for wiring.

Because of its modular nature, this component can be easily integrated into the SimonsVoss System 3060 and like all SimonsVoss components can be programmed with the locking plan software.

2.0   Overview of function

2.1   Functional overview

The Q3008 biometric reader consists of the following components:

- Biometric analysis unit
- Integrated digital transponder which opens the appropriate lock when triggered by a successful biometric analysis.

The Q3008 biometric reader enables you to address all SimonsVoss locks (e.g. cylinders, smart relays or even arming units, etc.) using biometry.

The reader can learn up to 50 different fingerprints. Each finger is assigned its own transponder ID (TID). In SimonsVoss locks (with time control function, i.e. access control and time zone control) it is also possible to grant an individual time-limited access to a building and to keep a log of who accessed an area and when they did so.

2.2   Basic operation

The Q3008 biometric reader scans fingerprints using a strip sensor. The finger is not placed on the sensor (the small grey rectangle inside the black finger guide) but drawn across it.

Please note:

The learned finger image must be of good quality in order for the reader to recognise your fingerprint quickly and easily later on.

So whether you want the reader to learn or recognise your fingerprint, you must always draw your finger across the sensor in the same way.

Place your finger (the finger to be learned or which has already been learned) in the finger guide, above the sensor. At a constant speed and with gentle pressure, draw your finger down the strip sensor from top to bottom as shown in the pictures (moving towards the LED). Because of the design of the housing, you will find that your finger is guided clearly by the higher side walls. This makes it very difficult to operate the reader wrongly.

The strip sensor reads the fingerprint line by line and reassembles these lines in the integrated processor to form a complete image. If the assembled image corresponds to a stored image, the transponder is triggered.

Figure 1

Activate the biometric reader by placing your finger on the finger guide (see chapter 2.4), and then place your finger at the top of the sensor.

Figure 2

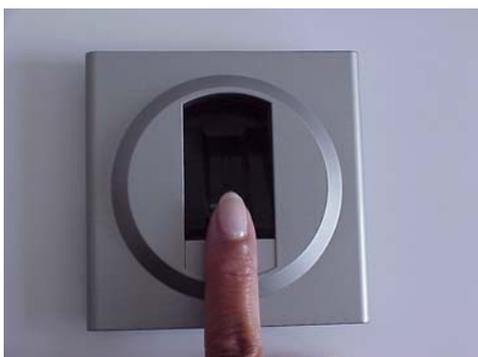Draw your finger across the sensor at an even speed and applying gentle pressure.

Figure 3

Keep your finger straight and extended, i.e. do not bend or curl it.

When scanning your finger please ensure that your finger remains in contact with the sensor at all times. In other words, you should maintain gentle pressure on the sensor during the scanning process.

2.3 Operating statuses

The Q3008 biometric reader distinguishes between 5 different operating statuses:

Status:	Explanation:
Standby	The biometric reader is in idle mode and consumes very little power.
Recognize	Recognize mode is the status used before an attempt is made to open a door. Once an authorised fingerprint is recognised, the lock is addressed by radio and can then be opened.
Learn	In this mode, the relevant integrated transponders (up to 50) can be programmed or reset with the SimonsVoss software. The reader can store up to 50 different fingerprints.
Delete	In delete mode, learned fingerprints can be deleted. You can delete individual fingerprints or all fingerprints.
Battery warning	A battery warning system gives you adequate warning when a battery needs replacing.

2.4 Operation

Once the Q3008 biometric reader has been commissioned and configured, it forms a 'wireless circuit' with a SimonsVoss lock within the System 3060. The following chapters describe in detail how to program individual fingerprints and the relevant transponder data records and how to use the Q3008 biometric reader.

Finger guide

Sensor

LED
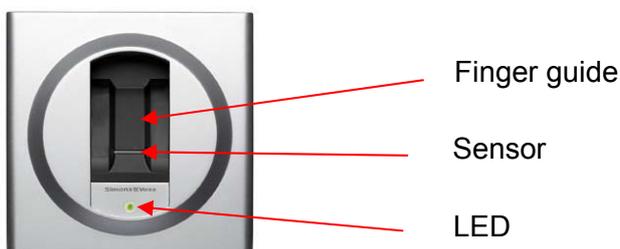
3.0   Programming

The following chapters describe the programming process in detail. If you are using the biometric reader in a small-scale locking system, please refer to chapter 11.0 Master finger mode.

Do not undertake any programming after a battery warning. Replace the battery before proceeding. Refer to chapter 15.0 Replacing the battery.

3.1   Commissioning

Please note: The 3008 biometric reader must be created in the locking plan as a *lock (biometric reader)* and users as transponder type *biometric reader users*. Users (transponder IDs) and fingerprints can only be learned in situ with the SmartLSM and the SmartCD.

Please proceed as follows:

1.   Create a locking plan in the SimonsVoss software.
2.   Create 'biometric reader' as a *lock→biometric reader*.
3.   Create lock (e.g. locking cylinder).
4.   Create transponder using the option *Biometric reader user*.
5.   Issue authorisation for the 'biometric reader' and the corresponding lock.
6.   Connect the SmartCD to the PC and bring within communication range of the 'biometric reader'.
7.   Highlight the biometric reader and launch '**Programming → Lock**' in the programming software. This is where you undertake basic configuration of the biometric reader.
8.   Once the reader has been successfully programmed, this is indicated by a pop-up window. This time, the yellow programming lightning symbol remains displayed in the locking plan.
9.   Bring the SmartCD into the communication range of the lock to be addressed.
10.   Highlight the lock to be addressed by the biometric reader and launch '**Programming → Lock**' in the programming software. This is where you undertake basic configuration of the lock.
11.   Once the lock has been successfully programmed, this is indicated by a pop-up window.

      The following programming steps are performed in situ with a PDA and SmartLSM:

12.   Export the complete locking plan (pocket PC).
13.   Bring the SmartCD into the communication range of the biometric reader.

14. In SmartLSM, launch the '**Read**' locks function. The biometric reader is recognised and read.

15. Select '**Modify transponder**' and start the function by selecting '**Execute**'.

16. Select the appropriate transponder (biometric reader user) and launch the '**Programming**' function.

17. While the transponder is being programmed, the biometric reader automatically switches to Learn mode (LED flashes yellow), and you will be asked to draw your finger over the finger guide.

18. Draw the finger you want the reader to learn over the sensor.

19. If the fingerprint is recognised, the LED on the biometric reader gives two long flashes in green.

20. If programming was successful, the message "Programming successful" appears in the SmartLSM. The fingerprint has been successfully stored.

21. After you re-import the locking plan the programming lightning symbols disappear, both from the transponder and the biometric reader (if all transponders have been programmed).

3.2   Programming additional fingerprints (users)

To learn additional users, proceed as follows:

1. Create transponder using the option *Biometric reader user*.

2. Issue authorisation for the 'biometric reader' and the corresponding lock (e.g. locking cylinder).

3. Fully export the locking plan (pocket PC).

4. Bring the SmartCD into the communication range of the biometric reader in situ.

5. In SmartLSM, launch the '**Read**' locks function.

6. Select '**Modify transponder**' and start the function by selecting '**Execute**'.

7. Select the appropriate transponder (biometric reader user) and launch the '**Programming**' function.

8. While the transponder is being programmed, the biometric reader automatically switches to Learn mode (LED flashes yellow), and you will be asked to draw your finger over the finger guide.

9. Draw your finger over the sensor.

10. If the fingerprint is recognised, the LED on the biometric reader gives two long flashes in green.

11. If programming was successful, the message "Programming successful" appears in the SmartLSM. The fingerprint has been successfully stored in the biometric reader.

12. If you want the reader to learn other fingerprints, repeat from step 4. You must first create additional transponders in the software using the biometric reader user option (see step 1) and assign authorisations to them.

13. Bring the SmartCD into the communication range of the lock to be addressed in situ.

14. In SmartLSM, launch the '**Execute**' function.

15. If programming was successful, the message "Programming successful" appears in the SmartLSM. The new biometric reader users have been successfully stored in the lock.

16. After you import the locking plan the programming lightning symbols disappear, both from the biometric reader user and the biometric reader (if all transponders (biometric reader users) and the corresponding lock have been programmed).

4.0 'Recognize' process

'Recognize' mode is the normal operation for the Q3008 biometric reader, where a person whose fingerprint has been learned wants to open a door using a digital locking cylinder.

Please proceed as follows:

1. When the finger is placed on the finger guide, an integrated proximity sensor activates the biometric reader. After about 0.5 seconds, the LED flashes green.
2. You can now draw your finger (the one learned by the reader) across the sensor, with gentle pressure, making sure that the whole of the top finger joint passes over the sensor (refer to photos in chapter 2.2). Make sure that your finger is in roughly the same position as when the fingerprint was learned.
3. If the fingerprint is recognised and the integrated transponder has been successfully programmed, the LED flashes green twice and the biometric reader is triggered.

If the LED lights up red, fingerprint recognition was not successful. If this happens, you must start again from step 1.
If you moved your finger too quickly over the sensor, the LED gives one rapid flash in red and then turns green again. Draw your finger across the sensor again, this time slightly slower.
If the fingerprint is recognised, the LED will light up green. However, if the lock could not be contacted the LED will light up red again. If this happens, start again from step 1.

Please note:

- The Q3008 may occasionally fail to recognise a fingerprint even though it was correctly learned.

- If a fingerprint is rejected and the LED lights up red, the quality of the scan was not sufficient. This may be because the finger was not moved correctly across the sensor (not straight or not evenly, for example), or because the surface of the sensor is dirty. If the finger is too dry, it may 'judder' across the sensor. Please try again. You may wish to dampen your finger slightly first, for example by breathing on it.
- If the features of your finger could not be assigned to any learned fingerprint, the diode will light up red. You may have inadvertently used the wrong finger. Alternatively, you may have moved your finger differently over the sensor when the reader was learning your fingerprint (for example by turning the finger or with more or less fingertip).

Tip:
A person's fingerprint will not be recognised first time, every time. If you find that a fingerprint is frequently not being recognised, please have the reader learn a different finger.

Dry fingers can make fingerprint recognition more difficult. This can be remedied by moistening your finger or breathing on it, for example.

5.0   Assigning fingerprints to transponder IDs

The maximum of 50 different fingerprints are assigned 50 different transponder IDs. In order to use and differentiate between these 50 different fingerprints, they must be individually programmed.

Each fingerprint is assigned a unique transponder ID (TID). If the locks in a system feature a time control function (i.e. access control), the TIDs are stored in the locks whenever access takes place. This allows you to track which user was given access when.

It is therefore essential to ensure that you keep the same allocations during programming. Otherwise access to the lock may not be guaranteed.

6.0   Replacing fingerprints

You can replace existing fingerprints with new ones at any point, for example if an employee has left the company or no longer requires access through a certain door.

Do not undertake any programming after a battery warning. Replace the battery before proceeding. Refer to chapter 15.0 Replacing the battery.

Please proceed as follows:

1.   Open the locking plan with the SimonsVoss software.

2.   Export the locking plan (pocket PC).

3.   Bring the SmartCD into the communication range of the biometric reader.

4.   In SmartLSM, launch the '**Read**' locks function.

5.   Select '**Modify transponder**' and start the function by selecting '**Execute**'.

6.   Select the appropriate transponder (biometric reader user) and launch the '**Programming**' function.

7.   While the transponder is being programmed, the biometric reader automatically switches to Learn mode (LED flashes yellow), and you will be asked to draw your finger over the finger guide.

8.   Draw the new finger over the sensor.

9.   If the fingerprint is recognised, the LED gives two long flashes in green.

10.   If programming was successful, the message "Programming successful" appears in the SmartLSM. The fingerprint has been successfully stored.

11.   After you import the locking plan the programming lightning symbols disappear, both from the programmed transponder (biometric reader user) and the biometric reader (if all transponders (biometric reader users) have been programmed).

To replace additional fingerprints, repeat from step 3.

7.0   Querying the number of learned fingerprints

You can query the number of learned fingerprints / transponder IDs at any time. Please proceed as follows:

1.   Open the locking plan with the SimonsVoss software.
2.   Export the locking plan (pocket PC).
3.   Bring the SmartCD into the communication range of the biometric reader.
4.   Select the '**Read**' function.
5.   Select the '**Modify trans.**' function.
6.   Select the '**Execute**' function.
7.   You will see a list of all users. Approved biometric reader users are indicated by a thick black cross.

8.0   Deleting an individual fingerprint

Do not undertake any programming after a battery warning. Replace the battery before proceeding. Refer to chapter 15.0 Replacing the battery.

To delete an individual fingerprint, proceed as follows:

1.   Open the locking plan with the SimonsVoss software.
2.   Remove the cross indicating authorisation from the locking plan by clicking on it.
3.   Export the locking plan (pocket PC).
4.   Bring the SmartCD into the communication range of the biometric reader.
5.   Select the '**Read**' function.
6.   Select the '**Modify trans.**' task.
7.   Select the '**Execute**' function.
8.   Select the relevant transponder.
9.   Select the '**Program.**' function.
10.   Following successful programming, the SmartLSM will display the message "Programming successful" and a green dot.
11.   Re-import the locking plan.

The fingerprint and transponder ID have now been deleted from the biometric reader.

9.0   Deleting all fingerprints

Do not undertake any programming after a battery warning. Replace the battery before proceeding. Refer to chapter 15.0 Replacing the battery.

To delete all stored fingerprints from the Q3008 biometric reader at the same time, you need to completely reset the device. Please proceed as follows:

1.   Open the locking plan with the SimonsVoss software.
2.   Export the locking plan (pocket PC).
3.   Bring the SmartCD into the communication range of the biometric reader.
4.   Click on the '**Select**' function.
5.   Select 'Biometric reader'.
6.   Select the '**Read**' function.
7.   Select '**Reset**' and confirm by selecting '**Execute**'.
8.   Enter the password for the locking system or take 'From the database' and click on '**Start**'.
9.   Re-import the locking plan.

10.0   Reading the biometric reader

It is possible at any time to read the biometric reader and identify programmed transponders using the SimonsVoss locking plan software.

Please proceed as follows:

1.   Open the locking plan with the SimonsVoss software.
2.   Export the locking plan (pocket PC).
3.   Bring the SmartCD into the communication range of the biometric reader.
4.   Click on the '**Select**' box.
5.   Select the biometric reader.
6.   Start the '**Read lock**' function in the SimonsVoss SmartLSM.

11.0 Master finger mode

Master finger mode was developed specially for small locking systems. The biometric reader is programmed once and fingerprints can then be learned simply on the biometric reader itself. No distinctions can be made using different transponder IDs (TIDs), because no TIDs are learned in master finger mode.
Generally, we recommend using SimonsVoss programming software for programming purposes.

You can exit master finger mode at any time. To do this, all learned fingerprints (including the master fingers) must be deleted.

Do not undertake any programming after a battery warning. Replace the battery before proceeding. Refer to chapter 15.0 Replacing the battery**Fehler! Es wurde kein Textmarkenname vergeben.Fehler! Es wurde kein Textmarkenname vergeben.**.

11.1 Commissioning – Programming master fingers

The following chapters describe in detail the programming process for master finger mode.

Please note: The first two fingerprints learned are automatically stored as the master fingers. A master finger cannot also be programmed as a user finger (it will be rejected during the learning process, indicated by 4 red flashes). Unlike normal mode, individual fingerprints cannot be allocated a transponder ID (TID), i.e. the lock does not make a distinction between individual users. In master finger mode it is possible to use the biometric reader to produce an access log for all locks in the same system.

Please proceed as follows:

1. Create a locking plan in the SimonsVoss software.

2. Create 'biometric reader' as a *lock→biometric reader*.

3. Create lock (e.g. locking cylinder).

4. Connect the SmartCD to the PC and bring within communication range of the 'biometric reader'.

5. Highlight the biometric reader and launch '**Programming → Lock**' in the programming software. This is where you undertake basic configuration of the biometric reader.

6. If programming was successful, the programming lightning symbol disappears from the locking plan for the relevant biometric reader.

7. Bring the SmartCD into the communication range of the lock.

8. Highlight the lock to be addressed by the biometric reader and launch '**Programming → Lock**' in the programming software. This is where you undertake basic configuration of the lock.

   Please perform the next steps on the biometric reader itself. The first two fingerprints are automatically stored as the master fingers!

9. Place your finger on the sensor to activate the biometric reader.

10. The biometric reader automatically switches to Learn mode (LED flashes slowly in yellow).

11. Draw the finger to be learned as the master finger across the sensor, for as long as the LED keeps flashing slowly in yellow. (If the LED starts flashing quickly in yellow (indicating time-out), wait until the LED goes out and start again.)

12. If the fingerprint is recognised, the LED gives one long flash in green (fingerprint recognised). The LED gives one more long flash in green. The first master finger has now been stored.

13. To learn the second master finger (which must be different from the first one), please repeat from step 7.

Only once both master fingers have been successfully stored can the reader start learning user fingers. The persons chosen as the master fingers should be the locking system administrator or other persons with direct access to the locking system. As a general principle, ensure that only one finger of each hand is used to program in the master fingers.

11.2   Programming user fingers

Please perform the next steps on the biometric reader itself. The first two fingerprints learned are automatically stored as the master fingers!

1. Place your finger on the sensor to activate the biometric reader. The LED flashes slowly in green.

2. Draw a master finger across the sensor.

3. The biometric reader automatically switches to Learn mode (LED flashes slowly in yellow).

4. Draw the finger to be learned across the sensor, for as long as the LED keeps flashing slowly in yellow. (If the LED starts flashing quickly in yellow (indicating time-out), wait until the LED goes out and start again.)

5. If the fingerprint is recognised, the LED gives one long flash in green (fingerprint recognised). The LED gives one more long flash in green. The user finger has now been stored.

6. To program additional user fingers, repeat from step 1.

11.3 'Recognize' process

Please refer to chapter 4.0 Recognize process.

11.4 Deleting individual fingerprints

To delete an individual fingerprint, proceed as follows:

1. Place your finger on the sensor to activate the biometric reader. The LED flashes slowly in green.
2. Draw a master finger across the sensor.
3. The biometric reader automatically switches to Learn mode (LED flashes slowly in yellow).
4. Wait until the LED flashes quickly in yellow.
5. Touch the finger guide briefly three times with your finger.
6. The biometric reader automatically switches to Delete mode (LED flashes slowly in red).
7. Draw the user finger over the sensor.
8. The LED gives two slow flashes in green. The user finger has been deleted.

11.5 Deleting all fingerprints

To delete all stored fingerprints from the Q3008 biometric reader, you need to delete the complete fingerprint database. Please proceed as follows:

1. Place your finger on the sensor to activate the biometric reader. The LED flashes slowly in green.
2. Draw a master finger across the sensor.
3. The biometric reader automatically switches to Learn mode (LED flashes slowly in yellow).
4. Wait until the LED flashes quickly in yellow.
5. Touch the finger guide briefly three times with your finger.
6. The biometric reader automatically switches to Delete mode (LED flashes slowly in red).
7. Draw a master finger over the sensor.
8. The LED gives two slow flashes in green. All learned fingers (including both master fingers) are deleted.

The biometric reader retains all locking system data. It can now learn new master and user fingers. Once this is done the biometric reader will be available again in the locking system.

11.6   Resetting the biometric reader

To delete all stored fingerprints from the Q3008 biometric reader at the same time (including the locking system data), or if you want to exit master finger mode, you need to delete the complete fingerprint database and reset all locking system data. Please proceed as follows:

1.   Open the locking plan with the locking plan software.
2.   Select the appropriate biometric reader.
3.   Connect the SmartCD to the PC and bring within communication range of the 'biometric reader'.
4.   Highlight the biometric reader and launch '**Programming → Reset lock**' in the programming software.
5.   Once the lock has been successfully programmed, this is indicated by a pop-up window.

The biometric reader is now back in its original state and can be used for a different locking system.

12.0   Manipulation alarm

After 15 failed attempts, i.e. attempts to operate the biometric reader with a non-programmed fingerprint, the biometric reader reports a manipulation attempt. After each failed recognition, the LED will then flash red for 60 seconds. No fingers will be accepted during this time. Following correct recognition of a fingerprint, the manipulation counter is reset to zero.

13.0 Meaning of LED signals

The LED can light up in three colours: green, yellow and red. These colours have the following meanings:

- Green   Reader activated, awaiting fingerprint
          Fingerprint recognised, signal to open sent
          Fingerprint learning process successful

- Yellow Battery warning
          Learn mode

- Red   Fingerprint not recognised
          Delete mode
          Fingerprint not recognised during learning process
          Attempt to program master finger as user finger
          Maximum number of learnable fingers reached
          Lock not reached

14.0 Battery warning

The Q3008 biometric reader features a battery warning system to provide information about the status of the device and to minimise operating errors.

The system gives adequate warning of decreasing battery capacity. This alerts you to the need to change the battery in plenty of time.

Battery warning: A time delay is added to the 'recognise' process. The diode flashes YELLOW for 10 seconds. Once the 10 seconds have elapsed, the Q3008 biometric reader issues the command to open.

15.0 Replacing the battery

Generally speaking, the battery should only be replaced by a trained specialist. To open the housing you will need a Torx key of size TX6. Please proceed as follows:

1. Fully unscrew the two screws from the base of the housing.

2. Remove the front of the housing.

3. Remove the battery from the holder.

4. Insert the new battery, making sure that the positive terminal is to the right; refer to markings on circuit board. (Please note: polarity MUST be correct!).

5. Reassemble the housing.

6. Screw the two screws back into the base of the housing.

After the battery has been changed, all functions will be available again.

When replacing the battery it is essential to ensure that no water can penetrate into the housing and no electronic parts come into contact with water.

When replacing the battery, and immediately after inserting the battery, be careful not to touch the sensor or finger guide. This could lead to a loss of locking system data.

16.0 Assembly

Generally speaking, assembly should only be performed by a trained specialist. To mount the biometric reader on a wall, near the lock it is intended to open, you can use the screws (including dowels) supplied. To open the housing you will need a Torx key of size TX6. Please proceed as follows:

1. Fully unscrew the two screws from the base of the housing.

2. Remove the front of the housing. Be very careful not to drop the transponder or subject it to any other sudden impact.

3. Drill the appropriate holes in the wall, using the rear panel of the biometric reader as a drilling template if required.

4. Attach the rear panel to the wall using the screws.

5. Reassemble the housing.

6. Screw the two screws back into the base of the housing.

When assembling the unit it is essential to ensure that the sealing ring fits properly, that no water can penetrate into the housing and no electronic parts come into contact with water.

17.0 Special functions

17.1   Wireless circuit for SimonsVoss VdS shunt lock 3066

The biometric reader can be used to activate SimonsVoss arming units (VdS shunt lock 3066). The reader is fitted within the transmission range of the VDS arming unit for this purpose. When the correct fingerprint is recognised, the arming unit is addressed and the alarm system is armed or disarmed via the shunt lock.

For arming/disarming processes, VdS-certified arming units from SimonsVoss require a double opening protocol (double-click if to be armed/disarmed by transponder).

An external software tool from SimonsVoss allows the biometric reader to be reconfigured to shunt lock mode. The configuration emulates the required 'double-click' and the biometric reader is then suitable for arming/disarming processes.

Important: Please only set the double opening protocol (double-click) when using a SimonsVoss VDS shunt lock 3066. Otherwise it could result in malfunction or undesired effects.

You can switch off the shunt lock function at any time using the external tool and return to normal mode.

17.2   Miscellaneous

The quasiproximity, validation and expiry mode functions are not available with the biometric reader.

18.0 Technical data

Dimensions (W x H x D)	96 mm x 96 mm x 21.5 mm
Weight	115 g (incl. batteries)
Material	Plastic
Colour (housing)	Grey
Colour (finger guide)	Black
Number of fingers	50
Number of fingers (master finger programming)	48 users + 2 masters
Maximum number of activations with one set of batteries	Up to 60 000 activations or up to 7 years on stand-by
Operating distance from locking cylinder	Max. 40 cm (if transponder antenna parallel to cylinder antenna)
Operating distance from Smart Relay	Max. 120 cm (Transponder antenna parallel to antenna of Smart Relay)
Protection class	IP 41 (indoor only)
Operating temperature range	+5°C to +50°C
Battery type	1x 3.6 V DC lithium battery, type AA (SL760)
Replacing the battery	To be carried out by trained specialists only
Software	As of LDB 1.52, as of SmartLSM 1.1

CE