SIEMENS

SIMATIC Ident

RFID systems SIMATIC RF1000

Operating Instructions

Introduction 1

Security recommendations 2

Description 3

Installation 4

Connecting 5

Commissioning 6

Programming 7

Demo application 8

Technical specifications 9

Dimension drawings 10

Appendix A

Service & Support B

05/2023
C79000-G8976-C432-10

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C432-10
Ⓟ 05/2023 Subject to change

Copyright © Siemens AG 2017 - 2023.
All rights reserved

Table of contents

1 Introduction 5

2 Security recommendations 7

2.1 Security information 8

2.2 Cell protection concept 9

3 Description 11

3.1 Properties of the reader 11

3.2 Connection options and supported transponders 13

4 Installation 17

5 Connecting 25

6 Commissioning 29

7 Programming 33

7.1 Typical applications 33

7.2 Programming via USB/RS232 interface (using DLL functions) 34
7.2.1 Functions of the USB/RS232 interface for Windows 34
7.2.1.1 brp_open_usb_session 34
7.2.1.2 brp_open_serial_session 35
7.2.1.3 brp_set_checksum 38
7.2.1.4 brp_set_bufsize 38
7.2.1.5 brp_close_session 39
7.2.1.6 syscmd_reset 40
7.2.1.7 syscmd_get_info 40
7.2.1.8 syscmd_get_boot_status 41
7.2.1.9 syscmd_set_port 42
7.2.1.10 vhl_select 43
7.2.1.11 vhl_get_snr 45
7.2.1.12 vhl_is_selected 46
7.2.1.13 vhl_read 47
7.2.1.14 vhl_write 48
7.2.1.15 Autoread_SetMode (called via "exec_command") 49
7.2.1.16 Autoread_GetMessage (called via "exec_command") 50
7.2.1.17 GetLicenses (called via "exec_command") 51
7.2.1.18 Return values 52
7.2.2 Functions of the USB interface for Linux 53

7.3 Programming via the RS232 interface (using the Freeport protocol) 53
7.3.1 Implementation of the commands 54
7.3.2 Commands 55
7.3.2.1 syscmd_reset 55
7.3.2.2 syscmd_get_info 56
7.3.2.3 syscmd_get_boot_status 56
7.3.2.4 syscmd_set_port 57

7.3.2.5 syscmd_get_licenses ... 58
7.3.2.6 vhl_select ... 59
7.3.2.7 vhl_get_snr ... 60
7.3.2.8 vhl_is_selected ... 61
7.3.2.9 vhl_read ... 62
7.3.2.10 vhl_write ... 63
7.3.2.11 Autoread_SetMode ... 64
7.3.2.12 Autoread_GetMessage ... 65
7.4 Status codes ... 66
8 Demo application ... 69
8.1 User interface of the demo application ... 69
8.2 Creating a custom application ... 72
9 Technical specifications ... 79
9.1 Technical specifications of SIMATIC RF1000 ... 79
9.2 Technical specifications, RF1100T Configuration Card ... 81
9.3 Technical specifications of the license cards ... 82
9.4 Technical specifications of table/wall housing ... 83
9.5 Technical specifications of cleanroom cover ... 83
10 Dimension drawings ... 85
A Appendix ... 87
A.1 Certificates & approvals ... 87
A.2 Connection via Remote Desktop Protocol (RDP) ... 89
A.3 Ordering data ... 90
B Service & Support ... 93

Introduction

1

Purpose of this document

This documentation provides you with an overview of the installation and programming of the SIMATIC RF1040R, RF1060R and RF1070R readers. The operating instructions are intended for users and programmers involved in configuration, commissioning and servicing of SIMATIC RF1000 readers.

Basic knowledge required

These operating instructions assume general knowledge of automation engineering and identification systems.

Scope of validity of this documentation

These operating instructions are valid for the SIMATIC RF1040R (6GT2831-6CA60), RF1060R (6GT2831-6AA60) and RF1070R (6GT2831-6BA60) from firmware version V2.03.05, as well as for SIMATIC RF1040R (6GT2831-6CA50), RF1060R (6GT2831-6AA50) and RF1070R (6GT2831-6BA50) from firmware version V2.0.7 and describe the delivery status as of 05/2023.

NOTICE
The scope of functions depends on the specific reader Please note that all Bluetooth (BLE) and license card (HID license) contents mentioned in this manual are valid only for the new devices with article numbers "6GT2831-6xA**60**".

Registered trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SIMATIC ®, SIMATIC RF ® and MOBY ®

Orientation in the documentation

Detailed information on creating and customizing configurations as well as their transfer to the SIMATIC RF1000 reader is available in the configuration manual "SIMATIC RF1000 (https://support.industry.siemens.com/cs/ww/en/ps/24224/man)".

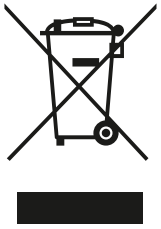
The manuals of the relevant SIMATIC Ident products (e.g. SIMATIC RF170C) on the Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/14970/man) pages contain additional information on the devices specified in this document.

Decommissioning

Decommission the device properly to prevent unauthorized persons from accessing confidential data in the device memory.

To do this, reset the device to the factory settings.

Recycling and disposal



The products are low in harmful substances, can be recycled and meet the requirements of the Directive 2012/19/EU for disposal of waste electrical and electronic equipment (WEEE).

Do not dispose of the products at public disposal sites.

For environmentally compliant recycling and disposal of your electronic waste, please contact a company certified for the disposal of electronic waste or your Siemens representative.

Note the different country-specific regulations.

Security recommendations

2

To prevent unauthorized access, observe the following security recommendations when working with the reader.

General

- Check regularly that the device complies with these recommendations and/or other internal security policies.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Keep the software up to date. Always use the latest firmware/software version of the device. Check regularly for security updates of the products and use them. After the release of a new version, previous versions are no longer supported and are not maintained.
  Information regarding product news and new software versions is available at the following address:
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/24224)
- Use the device only for system access control (and not for physical access control).

Physical access

- Restrict physical access to the device to qualified and authorized personnel.
- Restrict access to the configuration cards to qualified and authorized personnel and log their release.

Security functions

- Only enable functions that you actually need to use the device. Note that, in the factory setting, all transponders and card types listed below are recognized.
- Make sure that the configuration files are adequately protected. You can, for example, digitally sign and encrypt the files, store them at a safe location or transfer configuration files only via secure communication channels.

Certificates and keys

- Before sending the device to Siemens for repair, restore the factory settings.
- Make sure that the data stored on the transponders/cards is encrypted and that decryption/encryption of the data takes place on the connected devices.

Firmware/software

Make sure that only firmware created by Siemens is loaded to the device.

Check regularly for new firmware/software versions or security updates and install them. After the release of a new version, previous versions are no longer supported and are not maintained.

Decommissioning

Decommission the device properly to prevent unauthorized persons from accessing confidential data in the device memory.
Reset the device to factory settings for this purpose.

2.1 Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
https://www.siemens.com/cert.

2.2 Cell protection concept

The following graphic shows an example of a cell protection concept for the RF1000 readers.

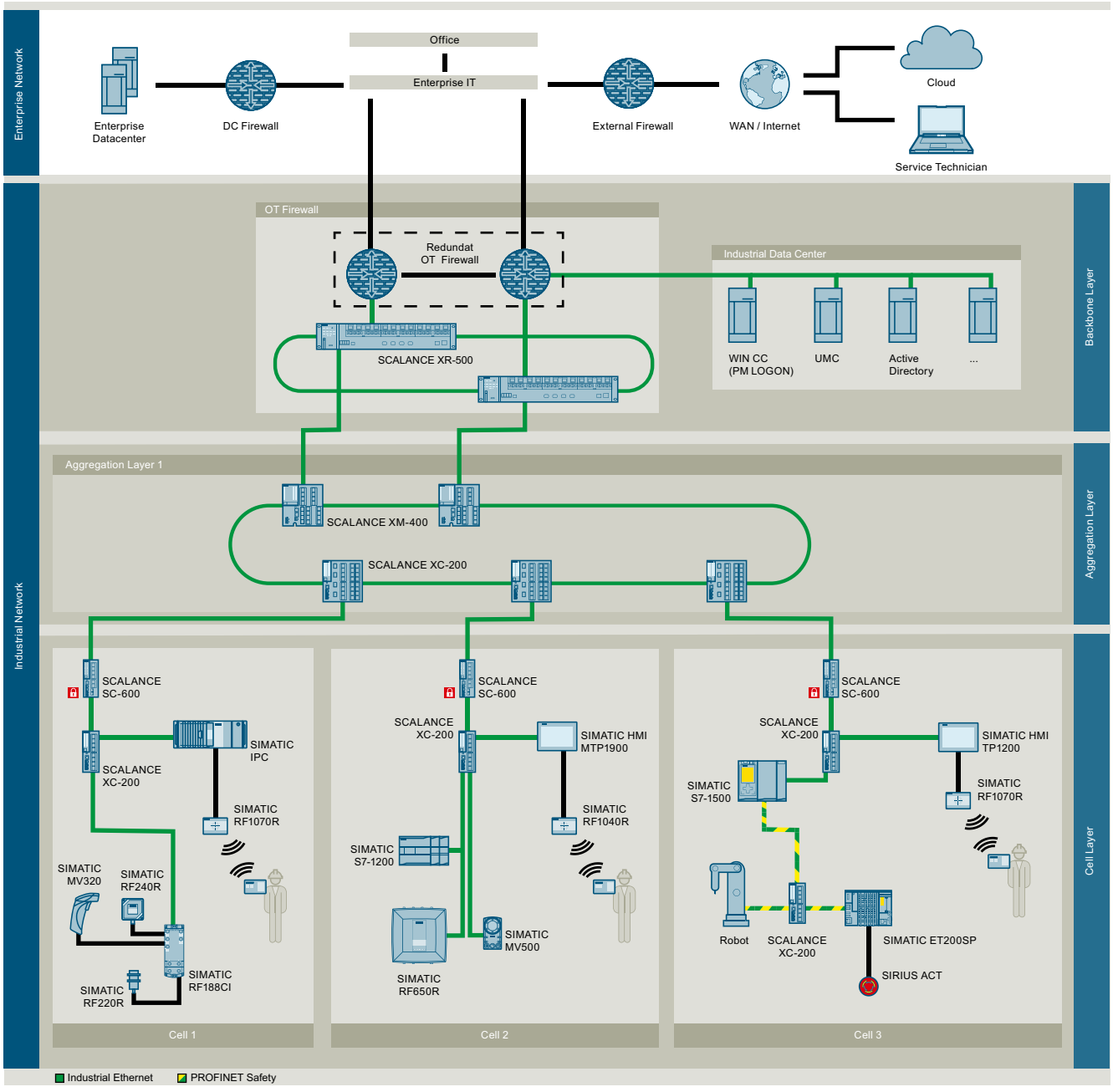


Figure 2-1 Schematic display of a cell protection concept for the RF1000 readers

Description

3

3.1 Properties of the reader

Area of application

Companies have been using RFID-based identification card systems for many years. With the increasing need for security and growing requirements for documentation, solutions are demanded with which access to machines and plants can be controlled on a user-specific basis. You can implement these requirements in access secured areas by using the SIMATIC RF1040R, RF1060R and RF1070R readers and an employee ID card so that machines and plants must be released with an employee ID before they can be operated. With an appropriate configuration, the data on the transponders/cards can be encrypted and read only by those devices that have the appropriate key. You can adapt the readers to your security requirements as needed. This allows a finely graded access concept to be implemented or user-specific information and instructions to be stored – all with one card.

For security reasons, you should only operate the readers within a protected area. Make sure that the USB interface is not openly accessible after installation.

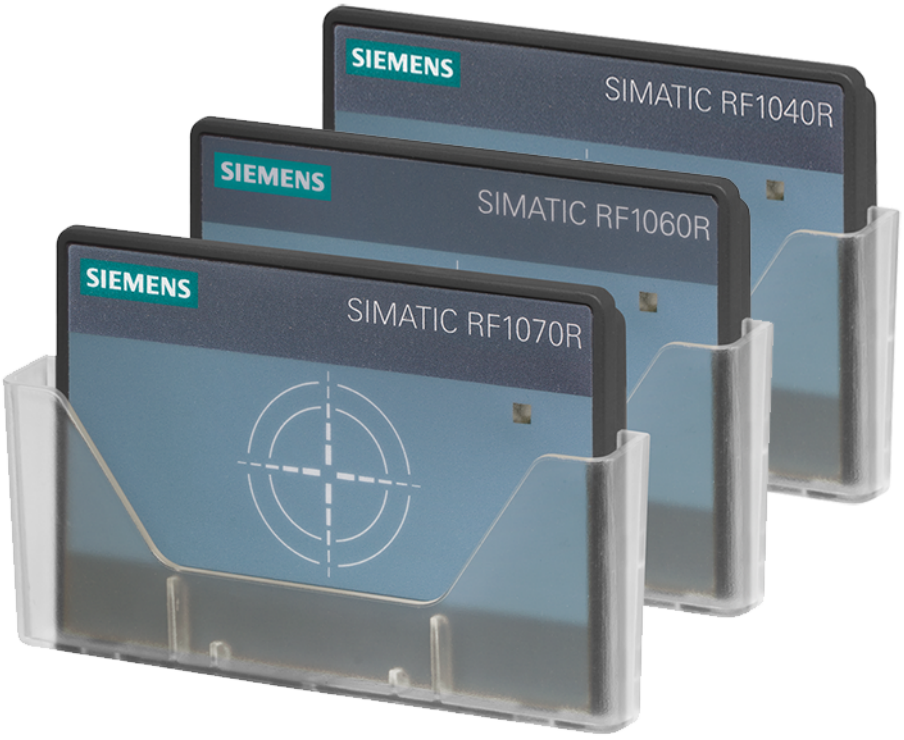


Figure 3-1 Product photos of the SIMATIC RF1000 reader

The SIMATIC RF1000 readers are designed for connection to a Windows computer. Alternatively, they can also be operated on a Linux-based system.

Reader-specific differences

The connection is via a USB interface of the computer. SIMATIC RF1040R and RF1070R readers can also be connected via the RS232 interface. The RF1070R reader is also available as an OEM version. This reader variant is identical to the RF1070R, but is supplied with a neutral front foil. A separate foil can be created as an alternative.

Interface-specific programming

The Siemens support site "Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/109741590)" provides access functions for the readers in the form of DLL files for Windows, as well as a demo application. With operation via the USB interface on a PC (Windows), you can implement user identification for access to your own applications quickly and simply with the help of the DLL file. The reader reads/processes the serial numbers and data of transponders for this.

If no DLL is available for the interface of your USB device (e.g. HMI Basic Panels), you can use the configuration card to activate the keyboard emulation for your readers. You can find detailed information on this in the section "Commissioning (Page 29)". In this mode, the readers are sending the read data without being prompted to do so.

If SIMATIC RF1040R/RF1070R readers are operated on a communications module via the RS232 interface, communication is performed using the Freeport protocol.

Features

The following table provides an overview of the characteristics of the RF1000 readers.

Table 3-1 Features of the communications modules

Features	RF1040R	RF1070R	RF1060R
Operating frequency	125 kHz, 13.56 MHz	13.56 MHz	
Transmit power (max.)	125 kHz: < 50 mW, 13.56 MHz: 250 mW	200 mW	250 mW
Interfaces	USB 2.0 (Type A) RS232		USB 2.0 (Type A)
Degree of protection (front)	IP41 ... IP67 (depending on the type of installation)		
Configuration/ diagnostic options	Demo application, DLL functions, Freeport protocol		Demo application, DLL functions
Application protocols			

Integration

The following graphics show examples of some of the integration options of the readers.

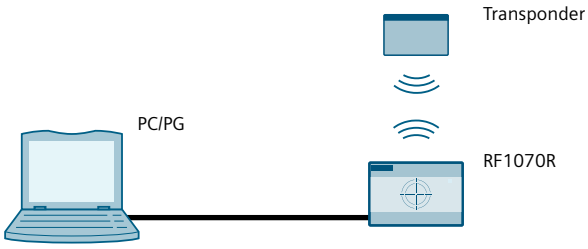


Figure 3-2 Reader connection via PC/PG

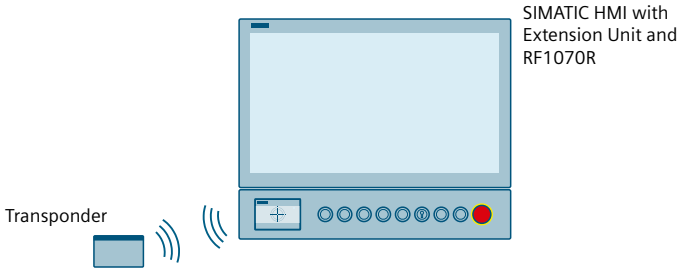


Figure 3-3 Reader connection via SIMATIC HMI

3.2 Connection options and supported transponders

Depending on the interface protocol used, the readers can be used for various applications. The following table provides an overview of the possible uses of the readers.

Table 3-2 Possible uses

	SIMATIC RF1060R	SIMATIC RF1040R/RF1070R		
Interface/Protocol	USB	USB	RS232 / Freeport	
application	PM LOGON, demo application	PM LOGON, demo application	STEP 7 (TIA Portal) [1]	
Programming	DLL for PC	DLL for PC	Ident profile/ blocks	P2P blocks
Connector	SIMATIC Panel, PC	SIMATIC Panel, PC	RF166C, RF170C, RF18xC/CI	RF120C	Serial module (e.g. ET 200SP)
Cable	Included in the scope of delivery	Included in the scope of delivery	6GT2891-4UH20	6GT2891-4UH20	6GT2891-2UH30

[1] A connection via other applications is possible. You can find additional information on this in the section "Programming via the RS232 interface".

Supported transponders and protocols

The following table provides an overview of the transponders and protocols supported by the readers.

Table 3-3 Supported transponders

	SIMATIC RF1040R	SIMATIC RF1060R	SIMATIC RF1070R
MDS D100, D124, D126, D324, E600, E611	✓	✓	✓
MDS D200	✓	✓	✓
MDS D400, D424, D426, D524, D526	✓	✓	--

✓: Reading the serial number as well as reading and writing the user memory area

Table 3-4 Supported protocols and card types

	SIMATIC RF1040R	SIMATIC RF1060R	SIMATIC RF1070R
ISO 14443 A/B general	Serial number	Serial number	Serial number
ISO 15693 general	✓	✓	✓
LEGIC prime	--	--	✓ [2)]
LEGIC advant (ISO 14443 A) [1)]	Serial number	Serial number	✓ [2)]
LEGIC advant (ISO 15693) [1)]	Serial number	Serial number	✓ [2)]
MIFARE Classic, EV1 [1)] (1k, 4k, Mini)	✓	✓	✓
MIFARE DESFire, EV1/EV2 [1)] (2k, 4k, 8k)	✓	✓	✓
MIFARE Plus, EV1 [1)] (S, X, L1, L2, L3)	✓	✓	Serial number
MIFARE Ultralight / C / EV1	✓	✓	✓
HID iClass, Inside PicoPass	Serial number	Serial number	Serial number
NXP NTAG21x	Serial number	Serial number	Serial number
FeliCa	Serial number	Serial number	Serial number
EM4100/EM4102, Casi-Rusco	Serial number	--	--
EM4450/EM4550, EKS	✓ [3)]	--	--
HITAG 1, HITAG S	✓	--	--
HITAG 2	Serial number	--	--
Keri [4)]	Serial number	--	--
SecuraKey	Serial number	--	--

	SIMATIC RF1040R	SIMATIC RF1060R	SIMATIC RF1070R
AWID	Serial number	--	--
ioProx	Serial number	--	--

✓: Reading the serial number as well as reading and writing the user memory area

1) Transponder card must be formatted.

2) An identification card is required to access encrypted user memory areas (see section "Commissioning").

3) Only for read access. Write access to the user memory area is not possible.

4) The license must be transferred to the reader with a license card (HID).

In addition to the specified protocols and card types, a variety of transponder cards are generally supported by the readers. If you cannot find the card type that you use in the table, you can ask Siemens Customer Support about the functionality.

Note that serial numbers (UIDs) of transponders that begin with the byte "0x08" are always newly generated by the transponder. This makes an assignment of serial numbers and transponders impossible. For transponders with a combo-chip (e.g. LEGIC CTC4096), the serial number of the LEGIC Prime chip is always read and not that of the ISO chip 14443/15693. For transponders with two integrated chips (125 kHz / 13.56 MHz), you must ensure which chip is addressed via the reader configuration.

SIMATIC RF1000 readers can also recognize multiple transponders that are simultaneously located in the antenna field. You can find information on selecting multiple transponders in the section "vhl_select (Page 43)".

The reader can be addressed and controlled by functions, for example to change the status of the reader or to communicate with a transponder. With the aid of the functions, you can for example control the three-color reader LED. The functions and their calls are described in this manual.

Installation

4

Depending on the operating environment, you can install the RF1000 readers inside a wall or control cabinet (in-wall/cabinet installation) as well as on a wall or table (surface/table installation). When installing the readers inside or on a wall, you may also want to install a card holder. However, if the readers are to be operated in a cleanroom, you must "seal" the readers using a silicone joint and the matching cleanroom cover.

Installation types and options:

- In-wall or cabinet installation
  - without accessories
  - with card holder "6GT2890-0CA00" or
  - with cleanroom cover cabinet installation "6GT2890-0CD00" (relevant for operation in a cleanroom)
- Surface or table installation
  - with table/wall housing "6GT2890-0CB00" and
  - with card holder "6GT2890-0CA00" and/or
  - with cleanroom cover surface installation "6GT2890-0CC00" (relevant for operation in a cleanroom)

NOTICE

Interference due to metallic environments

Electrically conductive materials can interfere with the HF field of the reader to the point that it is completely shielded. Observe the following guidelines to avoid interference:

- Ensure that there is no metal between reader and transponder.
  Coins and other metal parts that are significantly smaller than the transponder antenna, usually do not cause any interference.
- Ensure that there is no metal close to the rear of the transponder.
  Observe a minimum clearance that is at least half the size of the transponder diameter or the card width.
- When installed in metal, note that the read/write range and the detection reliability can be restricted. if the antenna of the transponder is larger than the antenna of the reader (57 x 35 mm).

Note that a short test with a number of example cards is not sufficient to test how large the metal-free area around the reader must be. Even in the event of a positive result, communication failures can occur during operation. This is due to deviations in card antennas, card IC parameters and RFID interface parameters, which can influence both energy transfer and the quality of the data transfer.

NOTICE

Using the reader in a cleanroom

Note that when operating the reader in a cleanroom, the cleanroom cover must be installed and the reader or the table/wall housing must be sealed with a silicone joint.

Recommendations for the silicone joint:

- Silicone recommended for cleanroom: Silirub Cleanroom
- Radius of the joint tool for wiping: 5 mm

NOTICE

Repair and maintenance

Do not try to repair the reader in case of a problem. Repair and maintenance work must only be carried out by qualified personnel. Contact Siemens Support in case of repair or maintenance problems. For more information, refer to the section "Service & Support".

Required tools

The following tool is required:

- Torx screwdriver (T10)
- Slotted screwdriver
- If necessary, caulking gun, silicone cartridge and joint tool (relevant for operation in a cleanroom)

Accessories required

Depending on the type of installation, you may require the following accessories to install the reader:

- for in-wall or cabinet installation
  - If necessary, card holder "6GT2890-0CA00" or
  - If necessary, cleanroom cover cabinet installation "6GT2890-0CD00" (relevant for operation in a cleanroom)
- for surface or table installation
  - table/wall housing "6GT2890-0CB00"
  - 4x screws (∅ 4 mm) and matching anchors
  - If necessary, card holder "6GT2890-0CA00" or
  - If necessary, cleanroom cover surface installation "6GT2890-0CC00" (relevant for operation in a cleanroom)

Mounting the reader

The procedure for installing the reader depends on the operating environment or the type of installation.

NOTICE
Protection class dependent on type of installation Note that the protection class of the reader depends on the type of installation. If the reader is installed inside a wall (in-wall installation), the reader has degree of protection IP65 on the front. If the reader is installed using the table/wall housing on a wall or on a table (surface/table installation), the reader has degree of protection IP41.

In-wall or cabinet installation

NOTICE
Installation conditions • The thickness of the wall on which the reader is mounted must be 2-7 mm. • The installation opening must have the following dimensions: 76.5 (± 0.3) × 48.5 (± 0.3) mm

Follow the steps below to install the RF1000 reader inside a wall or in a control cabinet:

1. When operating via the RS232 interface:
   Replace the pre-installed USB cable with the supplied RS232 cable as described in the section "Connecting (Page 25)".
2. Optionally when using the cleanroom cover:
   Drill condensate holes below the installation opening.

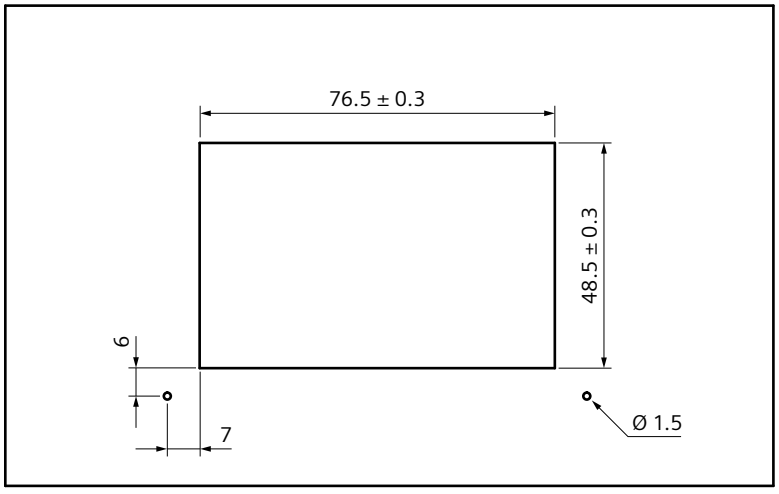


Figure 4-1 Condensate holes

3. Optional: Depending on your requirements, install the card holder or the cleanroom cover.
   - When using a card holder:
     Place the card holder on the side of the reader housing and press it over the reader front so that the card holder locks in place.
     Note that you cannot use the card holder in combination with the cleanroom cover.
   - When using the reader in a cleanroom:
     Place the cleanroom cover on the side of the reader housing and press it over the reader front so that the cover locks in place.
     Note that you cannot use the cleanroom cover in combination with the card holder.
4. Push the reader through the mounting opening intended for this purpose (76.5 [± 0.3] × 48.5 [± 0.3] mm) ①.
   Make sure that the reader locks in place so that it cannot fall out.
5. Mount the cover plate on the rear of the reader with the 4 Torx screws (max. 1.5 Nm) ②.
6. Attach the reader by tightening the 4x stud screws ③.
   Ensure that the reader housing is flush with the base and that the circumferential gap is < 0.5 mm.

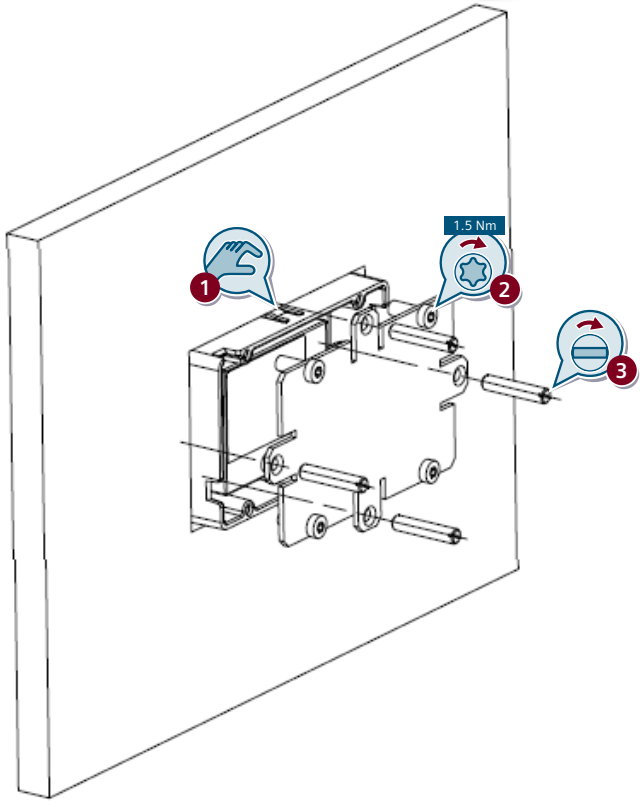


Figure 4-2 In-wall installation of the SIMATIC RF1000 reader

7. Optionally when using the reader in a cleanroom:
   Apply a silicone joint on the front between the reader edge or the cleanroom cover and the surface or the wall.

Surface or table installation

NOTICE
Cleanroom cover: Non-detachable connection Note that the connection between the cleanroom cover in connection with the table/wall housing is a non-detachable connection. Attempting to remove the cover deforms or tears off the snap-in clips of the cover.

NOTICE
Installation condition Note the dimensions of the mounting holes in case of surface mounting.

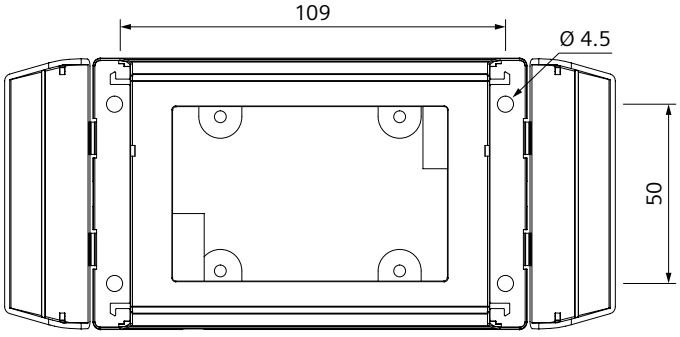


Figure 4-3 Drill pattern for surface mounting with the table/wall housing

Follow the steps below to install the RF1000 reader on a wall or table:

1. Open the table/wall housing by sliding the screwdriver into the grooves on the front of the table/wall housing and carefully pry it off to the side ①.

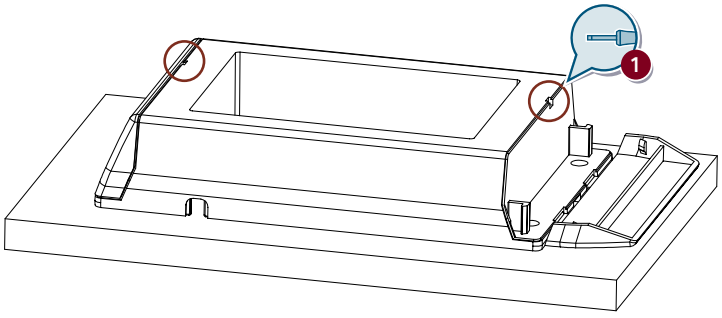


Figure 4-4 Opening the table/wall housing

2. Optionally when operating via the RS232 interface:
   Replace the pre-installed USB cable with the supplied RS232 cable as described in the section "Connecting (Page 25)".
3. Optionally when using the card holder:
   Place the card holder on the side of the reader housing and press it over the reader front so that the card holder locks in place.
   Note that you cannot use the card holder in combination with the cleanroom cover.

4. Push the reader through the opening intended for this purpose in the table/wall housing. Make sure that the connected cable is routed through one of the rectangular cutouts in the rear panel of the housing.
5. Turn the table/wall housing, together with the reader contained therein, to the front so that the rear of the table/wall housing is at the top.
6. Fasten the reader in the table/wall housing by installing the reader in the housing ② using the 4x Torx screws (max. 1.5 Nm) and the four inside mounting holes of the table/wall housing.

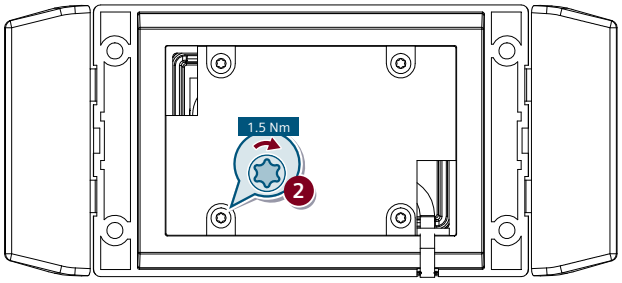


Figure 4-5 Installing the reader in the table/wall housing

7. Optional: Follow these steps depending on whether you want to install the reader on a wall or a table:
   - With surface installation on a wall:
     Position the table/wall housing at the desired location (wall) and install the table/wall housing using four screws (Ø 4 mm) and the external mounting holes of the housing ③.
     Make sure that the connecting cable is routed through the mounting cutout in the housing. When using a cleanroom cover, the connecting cable must be routed to the rear.
   - When installing on a table:
     As an alternative to installing the reader on a table, you can place the reader installed in the table/wall housing on a table.
     Make sure that the connecting cable is routed through the mounting cutout in the housing. When using a cleanroom cover, the connecting cable must be routed to the rear.

Note

Cable routing

Make sure that the connecting cable is routed without any interference. In case of a surface installation, the housing bottom (with the cutout for the connecting cable) should always point down.

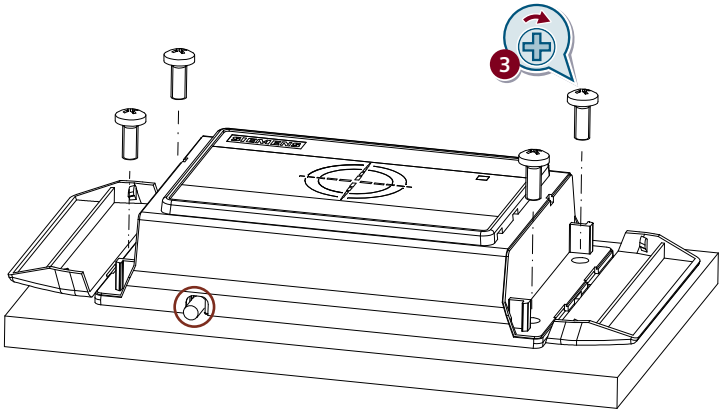


Figure 4-6 Surface installation of the SIMATIC RF1000 reader using the table/wall housing

8. Close the table/wall housing.
   Make sure that the housing sides lock in place.
9. Optionally when using the reader in a cleanroom:
   Place the cleanroom cover on the side of the table/wall housing and press it over the reader front and the table/wall housing so that the cover locks in place.
   Apply a silicone joint between the reader edge or the cleanroom cover and the surface or the wall.

Connecting

5

Depending on the operating environment, you can operate the RF1000 readers using a USB or an RS232 interface.

NOTICE
Permissible power supply The equipment is designed for operation with a Safety Extra-Low Voltage (SELV) system via a Limited Power Source (LPS) and must only be operated with 5 V DC. The power supply must therefore meet one of the following conditions: • Only SELV / LPS complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 or IEC 62368-1 / EN 62368-1 / VDE 62368-1 can be connected to the power supply terminals. • The power supply unit for the device must meet NEC Class 2 according to the National Electrical Code (r) (ANSI / NFPA 70).

Required tools

When using the RS232 interface, you need to attach the corresponding cable to the reader first. You require the following tools for this purpose:

- Torx screwdriver (T10)
- Additional tools depending on the connector used

Accessories required

Depending on the device to which the reader will be connected, you may need the following accessories for connecting the reader:

- For communication via the USB interface,
  the pre-assembled connecting cable included in the scope of delivery
- For communication with the SIMATIC F120C communication module via the RS232 interface
  the connecting cable (6GT2891-6UH20)
- For communication with a SIMATIC RF166C, RF170C or RF18xC/RF18xCI communication module via the RS232 interface
  the connecting cable (6GT2891-4UH20)
- For communication via the RS232 interface with any serial module,
  the connecting cable with open ends (6GT2891-2UH30)

Connect the plug

The procedure for connecting the reader depends on the interface over which the reader is being operated.

Connection via USB interface

Proceed as follows to connect the SIMATIC RF1000 reader via the USB interface:

1. Connect the reader to the PC or Panel using the USB cable.

Connection via RS232 interface

Proceed as follows to connect the SIMATIC RF1040R/RF1070R reader via the RS232 interface:

1. Optionally when using the cable 6GT2891-2UH30:
   Install the cable connector at the open cable end.
   You can find the connector assignment in the following table.
2. Loosen the cleat on the USB cable and remove the USB cable.
3. Connect the matching RS232 cable to the RS232 interface of the reader (5-pin socket).
4. Fasten the RS232 cable using the cleat.
5. Connect the reader to the communications module or the controller with the RS232 cable.

The table below contains the connector assignment for the connecting cable with open ends (6GT2891-2UH30).

Table 5-1 Connector assignment of the cable 6GT2891-2UH30

Wire color (open cable end)	**PINs (5-pin socket housing; PicoBlade)**	**Assignment**
Red	1	+5 V
Black (x2)	2	GND
Brown	3	Data line, RxD
Orange	4	Data line, TxD

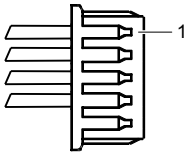
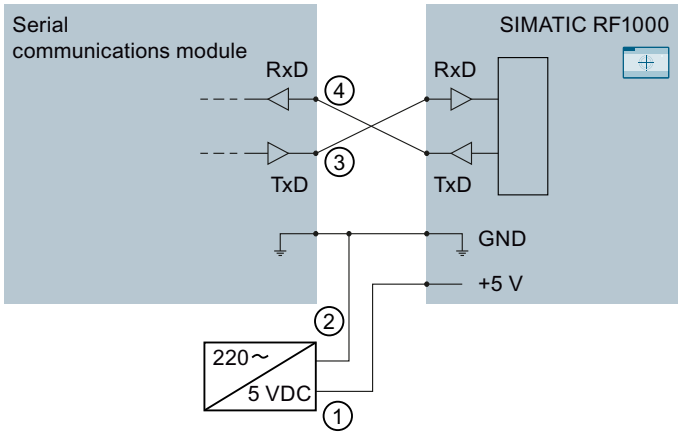


Figure 5-1 PIN assignment of 5-pin socket housing (PicoBlade)

When connecting the SIMATIC RF1000 reader to a serial communications module, ensure that you wire the devices as illustrated below.



① Red
② Black
③ Brown
④ Orange

Figure 5-2 Connection diagram: Connecting the reader to a serial communications module

Commissioning

6

The procedure for installing and commissioning the reader depends on the interface over which the reader is being operated.

Scope of functions of the basic configuration

The reader is delivered ex works with a basic configuration. This configuration enables you to read the UIDs of all transponder/card types. For ISO 15693 transponders, you can also read and write to the user memory using the VHLFile ID "255". In order to read the memory area of other transponder/card types or to use additional functions (e.g. autoread functions), you need to create a custom configuration and transfer it to the reader.

Commissioning via the USB interface

Windows operating systems

The readers are tested and approved for operation under Windows 10.

Proceed as follows to commission the SIMATIC RF1000 reader via the USB interface

1. Connect the reader to the PC or Panel using the USB cable.
   Reaction: The message "An RF10x0R is being set up." appears.
2. Copy the "RF1000R_Vxxx.exe" file to your PC.
   You can find the file on the Internet on the pages of the Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/109741590).
3. Extract the file.
4. Start the demo application by double-clicking on the file "AccessControlDemo.exe".

You will find more information on the demo application in the section "Demo application (Page 69)".

Linux environment

You can also operate the SIMATIC RF1000 reader in a Linux environment. The programming in Linux is made via an API and Software Development Kit. For additional information, contact the Siemens Industry Online Support (Page 93).

Commissioning via the RS232 interface

Proceed as follows to commission the SIMATIC RF1040R/RF1070R reader via the RS232 interface and with the aid of a controller:

1. Connect the reader to the communications module or the controller with the RS232 cable.
2. Configure the freeport protocol (e.g. data bits, parity, stop bits, transmission speed).
3. Program the blocks of the controller.

You will find more information on the freeport protocol in the section "Programming via the RS232 interface (using the Freeport protocol) (Page 53)".

License and configuration cards

License cards

You can transfer a HID license to a SIMATIC RF1040R reader using a license card. Note that a single license is saved on each license card which you can transfer to a reader once. With this process, the license card is automatically linked to the serial number of the reader.

The following options are available for transferring a license card to a reader using a license card:

- Using the demo application ("AccessControlDemo.exe")
  Start the demo application, click the "Start" button and select the "Read Data (auto)" or "Configcard"check box while the license card is in the antenna field of the reader.
- Programming your own application using the "Autoread_SetMode" or "vhl_select" function with "AllowConfig = true"
  When programming your own application, you need to set the "param = 1" tag when calling the "exec_command" function and then hold the license card in the antenna field of the reader. After you have transferred the license, the reader automatically restarts.

"RF1100T" configuration card

Using configuration cards, you can transfer reader configurations (e.g. memory areas, addresses, passwords, write permissions, etc.) and "Autoread" configurations to RF1000 readers. A configuration with several functions can be transferred from the configuration card to the reader.

The following options are available for changing the configuration of a reader using a configuration card:

- Using the demo application ("AccessControlDemo.exe")
  Start the demo application, click the "Start" button and select the "Configcard" check box while the configuration card is in the antenna field of the reader.
- Programming your own application using the "vhl_select" function
  When programming your own application, you need to set the "AllowConfig = true" tag when calling the function "vhl_select" and then hold the configuration card in the antenna field of the reader. After you have changed the configuration, the reader automatically restarts. After the restart, you need to set the "AllowConfig" parameter back to "false".
- Automatically with enabled "Autoread" mode
  The "Autoread" mode is switched on in the factory for the reader. In the delivery state of the reader, hold the configuration card in front of the reader after switching on the power.

An existing configuration in which "Autoread" mode is still active can only be replaced by a configuration with the same Config Security Code and Customer Key Signature. This prevents accidental overwriting. Note that working with the "vhl_select" command ("AllowConfig = false") or transferring a VHL configuration switches off "Autoread" mode. In this case, the configuration card can only be read in again using the demo application and the "vhl_select()" function (with "AllowConfig = true") or after the reader is reset to factory settings ("syscmd_reset").

The rewritable configuration cards are supplied in packs of five. Two of the supplied cards are unwritten, while three cards are written with sample configurations. These are identified by the corresponding labels on the rear of the configuration card. You can also order configuration cards with preset, customer-specific configurations. To do this, please contact Service & Support (Page 93).

You will find more detailed information on the configuration card in the configuration manual "SIMATIC RF1000 (https://support.industry.siemens.com/cs/ww/en/ps/24223/man)".

VHL functions

VHL stands for "Very High Level". VHL functions have a higher priority and are valid for all card systems supported by the reader. The card system-specific details are in the VHL functions of a configuration. By using VHL functions it is possible, for example, to change the card system without having to adapt the code to the application - provided that the configuration stored in the reader has been adapted accordingly.

Identification card for LEGIC systems

When using encrypted LEGIC systems/cards, you need an identification card to transfer reader configurations to the reader. For this purpose, contact the project owner or the original project supplier.

Programming

7

Depending on the interface over which the SIMATIC RF1000 readers are being operated, programming must take place either over the USB or the RS232 interface.

7.1 Typical applications

Below you will find typical applications for using the SIMATIC RF1000 readers. The applications are shown as an example using the DLL functions. These can be implemented in the same way with the commands.

Cyclic reading of serial numbers

A card that is located in the antenna field is selected with the "vhl_select" function. The serial number of the respective card is read with the "vhl_get_snr" function.

Unidirectional data receipt without using the programming interface

The prerequisite for the unidirectional data receipt that an "Autoread" configuration is stored in the reader. Data transfer can only take place via the RS232 interface or the virtual COM port of the reader in this case. The "Autoread" configuration can be transferred to the reader using the configuration card or directly using the ConfigEditor. During autonomous reading, you can automatically read a desired memory area of the respective card up to 16 bytes. In the configuration used, the "RawSerial" protocol must be set in the device settings ("Extend Configuration > Settings > Device Settings"). Prefix and postfix data can be selected if applicable. The data of the card in the antenna field is output via the serial interface.

Read and write user memory

Prerequisite for reading/writing the memory areas is that the corresponding card type and the application are stored in the reader.

A card that is located in the antenna field is selected with the "vhl_select" function. You can read or write to a required memory area of the respective card with the functions "vhl_read" / "vhl_write". Since there can be multiple VHL functions on the reader, the desired function is selected via the variable "VHLFile".

Autonomous reading ("Autoread")

Prerequisite for autonomous reading of the memory areas is that an "Autoread" configuration is stored in the reader. The "Autoread" configuration can be transferred to the reader using the configuration card or directly using the ConfigEditor.

During autonomous reading, you can automatically read a desired memory area of the respective card up to 16 bytes. The "Autoread_SetMode" function switches autonomous reading permanently or one time on or off. During autonomous reading the reader

synchronizes the card in the antenna field with the stored configurations. If a match is found, the corresponding memory area is read and output with "Autoread_GetMessage".

In "Autoread" mode, after a card has been detected by the user, the data must be fetched using the "Autoread_GetMessage" function within 5 seconds. Otherwise, this data is lost.

7.2 Programming via USB/RS232 interface (using DLL functions)

7.2.1 Functions of the USB/RS232 interface for Windows

You can program the reader using access functions. You can find the "RF1000R.zip" file on the Siemens support page "Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/109741590)". It includes the DLL files ("BrpDriver_x64" and "BrpDriver_x86"), the DLL functions as well as a demo application which demonstrates the use of the DLL functions.

With the demo application "AccessControlDemo" you can address the reader directly from your application via the USB interface. A precompiled DLL file for Windows systems that provides this function is included in the package.

The DLL files provide various DLL functions for communication with the reader for integration in your application. The reader has return values and status codes to inform you of the reader status and execution of the functions.

You can integrate the DLL files in your application under Microsoft Windows 7/8/10 and use them to call the described functions directly.

Connection options for programming via DLL functions

The type of programming depends on the connection option used. Programming via the following DLL functions can be performed when using the following connection options:

- Via the USB interface
- Via the USB interface, when using an RS232 interface converter
- Via the RS232 interface, when connected to a PC
- Via the virtual COM port interface, when connected to a PC

7.2.1.1 brp_open_usb_session

The function opens a connection to the reader via the USB interface and returns a session key that is required for all functions and continued communication via this connection. If the connection was successfully established, the value "BRP_OK" is returned.

Note that all the following functions, when operating via the USB interface, can only be performed once a connection to the reader has been established with the "brp_open_usb_session" function. If this is not the case, an error is signaled back.

Note

Parallel operation not possible

Note that with the application, a connection can only be established to one reader at any one time. For this reason "brp_open_usb_session" may only be called once and before it can be called again must first be closed by the function "brp_close_session".

After a "brp_open_usb_session", the parameter "Handle" must always be = "0". If the parameter ≠ "0", there is either an error or the function "brp_open__usb_session" was called several times in succession.

Function call

```
int
brp_open_usb_session(
  int * Handle,
  DWORD ProductID
);
```

Table 7-1 Description of the parameters

Parameter		Description
brp_open_usb_session		This function call opens a connection to the reader via the USB interface.
	Handle	Session key initialized by this function. The session key is valid as soon as "BRP_OK" is returned.
	ProductID	0x00
Return value		• BRP_OK • BRP_ERR_BUSY • BRP_ERR_GENERAL_IO • BRP_ERR_BUFFER_OVERFLOW • BRP_ERR_NO_MORE_HANDLES • BRP_ERR_INSUFFICIENT_MEM You will find more information on return values in the section "Return values (Page 52)".

7.2.1.2 brp_open_serial_session

The function opens a connection to the reader via the RS232 interface and returns a session key that is required for all functions and continued communication via this connection. If the connection was successfully established, the value "BRP_OK" is returned.

Note that all the following functions, when operating via the RS232 interface, can only be performed once a connection to the reader has been established with the "brp_open_serial_session" function. If this is not the case, an error is signaled back.

Note

Parallel operation

Note that you can operate several RF1040R/RF1070R readers in parallel via the RS232 interface or with the help of a COM port emulator.

Function call

```
int
brp_open_serial_session(
  int * Handle,
  int com_port,
  ser_baudrate baudrate,
  ser_parity parity
);
```

Table 7-2 Description of the parameters

Parameter		Description
brp_open_serial_session		This function call opens a connection to the reader via the RS232 interface.
	Handle	Session key initialized by this function. The session key is valid as soon as "BRP_OK" is returned.
	com_port	Number of the COM port Possible values: • 0x00: COM1 • 0x01: COM2 • ...
	ser_baudrate baudrate	Transfer speed [Baud] typedef enum {ser_baud_xxx} ser_baudrate; Possible values: • 0x00: ser_baud_300 • 0x02: ser_baud_600 • 0x03: ser_baud_1200 • 0x04: ser_baud_2400 • 0x05: ser_baud_4800 • 0x06: ser_baud_9600 • 0x07: ser_baud_14400 • 0x08: ser_baud_19200 • 0x09: ser_baud_28800 • 0x0A: ser_baud_38400 • 0x0B: ser_baud_57600 • 0x0C: ser_baud_115200 (Default) • 0x0D: ser_baud_576000 • 0x0E: ser_baud_921600 • 0x0F: ser_baud_500000
	ser_parity parity	Parity value typedef enum {ser_par_xxx} ser_parity; Possible values: • 0x00: ser_par_none • 0x01: ser_par_odd • 0x02: ser_par_even
Return value		• BRP_OK • BRP_ERR_BUSY • BRP_ERR_GENERAL_IO • BRP_ERR_BUFFER_OVERFLOW • BRP_ERR_NO_MORE_HANDLES • BRP_ERR_INSUFFICIENT_MEM You will find more information on return values in the section "Return values (Page 52)".

7.2.1.3 brp_set_checksum

You start a checksum algorithm with this function. The checksum allows you to check/protect the communication via the RS232 interface. This check is performed automatically when communicating via the USB interface.

Function call

```
int
brp_set_checksum(
  int Handle,
  int checksum
);
```

Table 7-3 Description of the parameters

Parameter		Description
brp_open_usb_session		Function call to configure the checksum algorithm
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	checksum	Definition of the checksum procedure: • 0x00: BRP_CECKSUM_NONE (Default) • 0x01: BRP_CECKSUM_BCC8 • 0x02: BRP_CECKSUM_CRC16 • 0x03: BRP_CECKSUM_BCC16
Return value		• BRP_OK • BRP_ERR_BUSY You will find more information on return values in the section "Return values (Page 52)".

7.2.1.4 brp_set_bufsize

This function allows you to define the buffer size for the job and response telegrams. The maximum permissible buffer size depends on the reader type used. Note that the buffer size is automatically set to the default value of 128 bytes after the restart.

Function call

```
int
brp_set_bufsize(
  int Handle,
  int TotalBufsize,
  int SendBufsize,
  int RecvBufsize
);
```

Table 7-4 Description of the parameters

Parameter		Description
brp_set_bufsize		Function call to configure the buffer size for the request and response telegrams
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	TotalBufsize	Specifying the maximum size of the job and response telegram • Default value: 128 bytes (data length 122 bytes) • RF1060R: max. 512 bytes (data length 506 bytes) • RF1040R/RF1070R: max. 1024 bytes (data length 1018 bytes)
	SendBufsize	Specifying the maximum size of the request telegram • Default value: 128 bytes (data length 122 bytes) • RF1060R: max. 512 bytes (data length 506 bytes) • RF1040R/RF1070R: max. 1024 bytes (data length 1018 bytes)
	RecvBufsize	Specifying the maximum size of the response telegram • Default value: 128 bytes (data length 122 bytes) • RF1060R: max. 512 bytes (data length 506 bytes) • RF1040R/RF1070R: max. 1024 bytes (data length 1018 bytes)
Return value		• BRP_OK • BRP_ERR_BUSY You will find more information on return values in the section "Return values (Page 52)".

7.2.1.5 brp_close_session

This function terminates an existing connection to the reader that was previously established.

Function call

```
int
brp_close_session(
   int Handle
);
```

Table 7-5 Description of the parameters

Parameter		Description
brp_close_session		This function call terminates a connection.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
Return value		• BRP_OK • BRP_ERR_WRONG_HANDLE You will find more information on return values in the section "Return values (Page 52)".

7.2.1.6 syscmd_reset

This function restarts the reader.

Note that you wait for about 3 seconds after the function "syscmd_reset" and then have to execute the functions "brp_close_session" and "brp_open_usb_session" once again.

Function call

```
int
syscmd_reset (
    int Handle,
    int * Status
);
```

Table 7-6 Description of the parameters

Parameter		Description
syscmd_reset		This function call restarts the reader.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	Status	OK You can find more detailed information on the reader status in the section "Status codes (Page 66)".
Return value		• BRP_OK You will find more information on return values in the section "Return values (Page 52)".

7.2.1.7 syscmd_get_info

The function reads out information about the firmware of the reader.

The value read out contains information on the type of firmware, the version and the serial number of the reader.

Function call

```
int
syscmd_get_info(
  int Handle,
  char * fws,
  int * Status
);
```

Table 7-7 Description of the parameters

Parameter		Description	
syscmd_get_info		This function call reads out information about the firmware of the reader.	
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.	
	fws	This parameter contains information on the type of firmware, the version and the serial number of the reader. Format: xx...xx r.rr.rr dd/dd/dd ssssssss	
		xx...xx	Firmware type
		r.rr.rr	Version (major release, minor release, build ID)
		dd/dd/dd	Date of the version
		ssssssss	Serial number of the reader
	Status	OK You can find more detailed information on the reader status in the section "Status codes (Page 66)".	
Return value		• BRP_OK You will find more information on return values in the section "Return values (Page 52)".	

7.2.1.8 syscmd_get_boot_status

The function returns a boot status.

Each bit of the value returned by the function represents an internal component of the reader. If the component of the reader could not be initialized the corresponding bit is set. Check the value of "boot_status" for the value "0" and output an error or a warning if the values do not match.

Function call

```
int syscmd_get_boot_status(
  int Handle,
  dword * boot_status,
  int * Status
);
```

Table 7-8 Description of the parameters

Parameter		Description
syscmd_get_boot_status		This function call returns a boot status value.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	boot_status	Each bit represents an internal component of the reader.
	Status	OK You can find more detailed information on the reader status in the section "Status codes (Page 66)".
Return value		You will find more information on return values in the section "Return values (Page 52)".

Note

Value of boot status not equal to "0"

If the function returns a value not equal to "0", please contact "Service & Support".

7.2.1.9 syscmd_set_port

You can use this function to assign parameters to the LEDs and the acoustic signal of the reader. In this way, you can view reader status changes or feedback from the application (e.g. incorrect authentication) via the LED and the acoustic signal.

You can select the desired LED color and/or the acoustic signal using the "port_mask" parameter. You will find a list of possible values in the following table.

Note that the LED function is pre-assigned at the factory. The readiness for operation of the readers is indicated by a green LED and the presence of a transponder by a yellow LED.

Function call

```
int
syscmd_set_port(
  int Handle,
  word port_mask,
  int * Status
);
```

Table 7-9 Description of the parameters

Parameter		Description
syscmd_set_port		This function call sets the LED of the reader.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	port_mask	Each value of the parameter is assigned to a specific LED color or the acoustic signal.
	Status	OK You can find more detailed information on the reader status in the section "Status codes (Page 66)".
Return value		• BRP_OK You will find more information on return values in the section "Return values (Page 52)".

Table 7-10 Values of the "port_mask" parameter

Value	LED color / acoustic signal	
0x0000		LED and acoustic signal
0x0001		LED lit green
0x0002		LED lit red
0x0003		LED lit yellow
0x0004	--	Acoustic signal (only for RF1040R/RF1070R)
0x0005		Acoustic signal (only for RF1040R/RF1070R) and LED lit green
0x0006		Acoustic signal (only for RF1040R/RF1070R) and LED lit red
0x0007		Acoustic signal (only for RF1040R/RF1070R) and LED lit yellow

7.2.1.10 vhl_select

With the help of this function you select a card located in the antenna field. If successful, the status "OK" is returned.

The type of the selected card is returned in the parameter "CardType".

With the "vhl_select" function you can select the card located in the antenna field of the reader. When "VHLSelect" is called again, the currently selected card is changed to the "Hold mode" and "vhl_select" returns the value "NOTAG_ERR".

If you want to select a card again without removing it physically from the antenna field, you need to set the "Reselect" parameter to "true". If there are several cards in the antenna field of the reader and you want to select all cards, set the parameter "Reselect = false". Then call the "vhl_select" function until all cards in the antenna field are recognized. If no new card is detected, "CARD_NOT_SELECTED_ERR" is returned.

Function call

```
int
vhl_select(
  int Handle,
  word CardTypeMask,
  bool Reselect,
  bool AllowConfig,
  byte * CardType,
  int * Status
);
```

Table 7-11 Description of the parameters

Parameter		Description
vhl_select		You can use this function to select a card located in the antenna field.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	CardTypeMask	Use this parameter to specify the card family to be recognized. When all card families should be detected, set the parameter to the value "0xFFFF" (see following table).
	Reselect	Select "Reselct = true" if there is only one card in the antenna field which should be detected. Select "Reselct = false" if there are several cards in the antenna field which should be detected.
	AllowConfig	This value is "true" when a configuration card is to be read. In normal operation, the value must be set to "false" to prevent unintentional acceptance of the reader configuration.
	CardType	The returned value indicates the card type (see following table).
	Status	• OK • NOTAG_ERR • HF_ERR • HW_ERR • CONFCARD_READ You can find more detailed information on the reader status in the section "Status codes (Page 66)".
Return value		• BRP_OK You can find more information on return values in the section "Return values (Page 52)".

The "CardTypeMask" parameter allows only specific card families to be selected. If you want to select all cards supported by the hardware of the reader, you need to set the parameter to "0xFFFF". The more significant half byte of the "CardType" parameter specifies the card family (1-6) while the less significant half byte (X) refers to the recognized card type.

Table 7-12 Assigning the card types

CardTypeMask	CardType	Protocols/card types
0x0001 (bit 1)	0x1X	ISO 14443 A / MIFARE
0x0002 (bit 2)	0x2X	LEGIC Legacy (only for RF1070R)
0x0004 (bit 3)	0x3X	ISO 15693

CardTypeMask	CardType	Protocols/card types
0x0008 (bit 4)	0x4X	ISO 14443 B
0x0010 (bit 5)	0x5X	iCLASS via proprietary ISO14443/B protocol derivate (Level 2 compatible)
0x0020 (bit 6)	0x6X	iCLASS via ISO15693
0x0040 (Bit 7)	0x7X	FeliCa
0x0080 (Bit 8)	0x8X	(only with RF1040R) EM4100/EM4102, EKS, HITAG 1/2/S, HID Prox/ioProx, Keri
0x0100 (Bit 9)	0x9X	ST SRIX
0x0200 (Bit 10)	0xAX	(only with RF1040R) SecuraKey
0x0800 (bit 12)	0xCX	LEGIC Prime (only for RF1070R)
0xFFFF	0xFF	All card families supported by the reader

7.2.1.11 vhl_get_snr

The function returns the serial number of the currently selected card. If the function "vhl_select" could not be executed earlier or the card is no longer in the antenna field, the value "CARD_NOT_SELECTED_ERR" (status code "0x0102") is returned. In this case, an undefined serial number is returned. Note that the least significant byte of the serial number is output first. For RF200/RF300 readers, the most significant byte is usually output first.

Function call

```
int
vhl_get_snr(
  int Handle,
  byte * Snr,
  byte * Length,
  int * Status
);
```

Table 7-13 Description of the parameters

Parameter		Description
vhl_get_snr		This function call returns the serial number of the currently selected card.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	Snr	Serial number of the card (LSB first)
	Length	Length of the serial number in bytes
	Status	• OK • CARD_NOT_SELECTED_ERR You can find more detailed information on the reader status in the section "Status codes (Page 66)".
Return value		• BRP_OK • CARD_NOT_SELECTED_ERR You will find more information on return values in the section "Return values (Page 52)".

7.2.1.12 vhl_is_selected

This function checks whether the card selected the last time the "vhl_select" function was executed is still or once again located in the antenna field. If the card is there, the status "OK" is returned.

Note that this function always returns the return value "CARD_NOT_SELECTED_ERR" when a card is displayed to the reader without the "vhl_select" function being executed first.

Function call

```
int
vhl_is_selected(
  int Handle,
  int * Status
);
```

Table 7-14 Description of the parameters

Parameter		Description
vhl_is_selected		This function call checks if the card selected during the last execution of the "vhl_select" function is still in the antenna field or if it has returned to the antenna field.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	Status	• OK • CARD_NOT_SELECTED_ERR You can find more detailed information on the reader status in the section "Status codes (Page 66)".
Return value		• BRP_OK You will find more information on return values in the section "Return values (Page 52)".

7.2.1.13 vhl_read

This function reads the memory area which is stored in a VHL function previously stored in the reader. The "VHLFile" parameter is used to reference the VHL function stored in the reader. With the configuration stored in the reader ex works, you can read out an ISO 15693 transponder from address 0 via "VHLFile = 255".

When a card is located in the antenna field and the function was completed, the status "OK" is returned.

Note that this function always returns the return value "CARD_NOT_SELECTED_ERR" when a card is displayed to the reader without the "vhl_select" function being executed first.

Function call

```
int
vhl_read(
  int Handle,
  byte VHLFile,
  word Address,
  word Length,
  byte * Data,
  int * Status
);
```

Table 7-15 Description of the parameters

Parameter		Description
vhl_read		This function call reads a previously defined memory area from the card.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	VHLFile	ID of the VHL function that is to be used.
	Address	Start address of the data that is going to be read.
	Length	Length of the data that is going to be read as of the start address.
	Data	Area in which the received data is stored (max. 65535 bytes).
	Status	• OK • CARD_NOT_SELECTED_ERR • HF_ERR • HW_ERR • CONFIG_ERR • AUTH_ERR • READ_ERR You can find more detailed information on the reader status in the section "Status codes (Page 66)".
Return value		• BRP_OK You will find more information on return values in the section "Return values (Page 52)".

7.2.1.14 vhl_write

This function writes data to a memory area that is stored in a VHL function previously stored in the reader. The VHL configuration stored in the reader is configured via the "VHLFile" parameter. With the configuration stored in the reader ex works, you can write to an ISO 15693 transponder from address 0 via "VHLFile = 255".

When a card is located in the antenna field and the function was completed, the status "OK" is returned.

Note that this function always returns the return value "CARD_NOT_SELECTED_ERR" when a card is displayed to the reader without the "vhl_select" function being executed first.

Function call

```
int
vhl_write(
  int Handle,
  byte VHLFile,
  word Address,
  word Length,
  byte * Data,
  int * Status
);
```

Table 7-16 Description of the parameters

Parameter		Description
vhl_write		This function call writes data into a previously defined memory area of the card.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	VHLFile	ID of the VHL function that is to be used.
	Address	Start address of the data that is going to be written.
	Length	Length of the data that is going to be written as of the start address.
	Data	Area in which the written data is stored (max. 65535 bytes).
	Status	• OK • CARD_NOT_SELECTED_ERR • HF_ERR • HW_ERR • CONFIG_ERR • AUTH_ERR • READ_ERR You can find more detailed information on the reader status in the section "Status codes (Page 66)".
Return value		• BRP_OK You will find more information on return values in the section "Return values (Page 52)".

7.2.1.15 Autoread_SetMode (called via "exec_command")

This function controls the "Autoread" functionality during runtime. The memory content of the cards that enter the antenna field of the reader is automatically read in "Autoread" mode without an explicit read job. You can specify in your reader configuration whether only the UID or also explicit memory areas should be read. The read data is output with the "Autoread_GetMessage" function.

In "Autoread" mode, after a card has been detected by the user, the data must be fetched using the "Autoread_GetMessage" function within 5 seconds. Otherwise, this data is lost.

Note that in "Autoread" mode, the "vhl_select" function is automatically executed cyclically by the reader. If the "vhl_select" function is executed from the Demo application as well, this can result in the card not being recognized when it enters the antenna field of the reader because it was already read in "Autoread" mode. In addition, the mode is ended with the function call "vhl_select" in "Autoread" mode. Make sure that the "vhl_select" function is not executed in addition in "Autoread" mode.

By activating/deactivating the "Autoread" function, the "MessageBuffer" is deleted. This ensures that no incorrect results are supplied by a subsequent call of the "Autoread_GetMessage" function when no card is located in the antenna field.

Function call

```
int
brp_exec_command(
  int Handle,
  byte devcode,
  byte cmdcode,
  byte * param,
  byte param_len,
  init timeout,
  init * Status,
  byte * resp,
  int * resp_len,
  init max_resp_len
);
```

Table 7-17 Description of the parameters

Parameter		Description
brp_exec_command		The parameter activates/deactivates the "Autoread" function.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	devcode	0x05
	cmdcode	0x00
	param	Buffer for the function parameters: • 0x00: The "Autoread" functionality is deactivated and VHL functions can be used. • 0x01: The "Autoread" functionality is permanently switched on. There is a permanent check as to whether a card is located in the antenna field. • 0x02: The "Autoread" functionality is executed once as soon as a card enters the antenna field. This is followed by a switch to VHL mode. The card identification is executed one more time with another call using the parameter value 0x02.
	param_len	0x01
	timeout	Time in [ms] until the action is aborted (500 is the recommended value).
	Status	OK You will find more information on the reader status in the section "Status codes (Page 66)".
	resp	Buffer for the received data
	resp_len	Current length of the response data in bytes
	max_resp_len	Maximum length of the response data
Return value		• BRP_OK You will find more information on return values in the section "Return values (Page 52)".

7.2.1.16 Autoread_GetMessage (called via "exec_command")

This function reads data from a transponder located in the antenna field. Up to 16 bytes of data can be read autonomously with this function.

Function call

```
int
brp_exec_command(
  int Handle,
  byte devcode,
  byte cmdcode,
  byte * param,
  byte param_len,
  init timeout,
  init * Status,
  byte * resp,
  int * resp_len,
  init max_resp_len
);
```

Table 7-18 Description of the parameters

Parameter		Description
brp_exec_command		This function call reads data from the transponder located in the antenna field.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	devcode	0x05
	cmdcode	0x01
	param	--
	param_len	0x00
	timeout	Time in [ms] until the action is aborted (100 is the recommended value).
	Status	• OK • ERR_NOMESSAGE • ERR_AR_DISABLED You will find more information on the reader status in the section "Status codes (Page 66)".
	resp	Buffer for the received data • Byte 0: Message type (0x00 for card identification) • Byte 1: Message length in bytes • Byte 2: ... message length +1: Message data
	resp_len	Current length of the response data in bytes
	max_resp_len	Maximum length of the response data
Return value		• BRP_OK You will find more information on return values in the section "Return values (Page 52)".

7.2.1.17 GetLicenses (called via "exec_command")

This function reads out which licenses are available on the reader.

Function call

```
int
brp_exec_command(
  int Handle,
  byte devcode,
  byte cmdcode,
  byte * param,
  byte param_len,
  init timeout,
  init * Status,
  byte * resp,
  int * resp_len,
  init max_resp_len
);
```

Table 7-19 Description of the parameters

Parameter		Description
brp_exec_command		This function call provides information on the licenses available on the reader.
	Handle	The session key returned by the "brp_open_usb_session" or "brp_open_serial_session" function.
	devcode	0x00
	cmdcode	0x29
	param	--
	param_len	0x04
	timeout	Time in [ms] until the action is aborted (500 is the recommended value).
	Status	• OK You will find more information on the reader status in the section "Status codes (Page 66)".
	resp	Screen form for the license: Byte 3: • Bit 0: – 0: No HID license found. – 1: HID license found. • Bit 3: – 0: No BLE license found. – 1: BLE license found.
	resp_len	Current length of the response data in bytes (4)
	max_resp_len	Maximum length of the response data
Return value		• BRP_OK You will find more information on return values in the section "Return values (Page 52)".

7.2.1.18 Return values

The following table contains a list of the possible values that the reader can return for the various functions.

Table 7-20 Return values

Value	Variable	Description
0x00	BRP_OK	No error has occurred
0x01	BRP_ERR_STATUS	The reader has returned a status code that is ≠ "0".
0x02	BRP_ERR_BUSY	The reader is currently processing a function.
0x03	BRP_ERR_IDLE	The reader is waiting for a function.
0x04	BRP_ERR_TIMEOUT	The response time has been exceeded.
0x05	BRP_ERR_CORRUPTED_FRAME	A bad frame was detected.
0x06	BRP_ERR_UNEXPECTED_FRAME	An unexpected frame was detected.
0x07	BRP_ERR_GENERAL_IO	The underlying serial port has caused an error.
0x08	BRP_ERR_BUFFER_OVERFLOW	The reader sent more data than expected.

Value	Variable	Description
0x09	BRP_ERR_NO_MORE_HANDLES	There is no free session key.
0x0A	BRP_ERR_INSUFFICIENT_MEM	There is not enough memory to generate a new session key.
0x0B	BRP_ERR_WRONG_HANDLE	The specified session key does not exist.
0x0C	BRP_ERR_WRONG_PARAMETERS	The parameters of a function are incorrect.

7.2.2 Functions of the USB interface for Linux

The programming in Linux is made via an API and Software Development Kit. For additional information, contact the Siemens Industry Online Support (Page 93).

Alternatively, you can program the USB interface in Linux based on the serial telegrams. These are described in section "Programming via the RS232 interface (using the Freeport protocol) (Page 53)".

7.3 Programming via the RS232 interface (using the Freeport protocol)

When the RF1040R/RF1070R readers are connected to a SIMATIC controller or any serial interface, communication is performed via the Freeport protocol. The freeport protocol allows you to communicate with the reader directly on the lowest level. A USB connection is not required for this.

The telegrams are listed in a byte coding in the following sections; you can apply the byte coding directly to the user program of the controller.

The communication parameters of the RS232 interface of the reader are set as follows in the factory:

- Data bits: 8
- Parity: None
- Stop bits: 1
- Transmission speed: 115.2 kBd

Connection via a communications module or serial module

The reader can be connected to a SIMATIC controller using a SIMATIC Ident communication module with RS232 interface. With a connection via the CM, you need to set the communication parameters of the CM as follows:

Table 7-21 Setting options in the "Module parameters" parameter group of the CM when using the freeport protocol

Parameter	Parameter value	Description
User mode	Ident profile/RFID standard profile FB 45 / FC 45	Selection of the block with which you want to assign parameters to the reader.
MOBY mode	Freeport protocol	The parameter value "Freeport protocol" must be selected in this parameter.
Transmission speed	115.2 kBd	The parameter value "115.2 kBd" must be selected in this parameter.
Diagnostic messages	None Hard errors	Selection of whether hardware diagnostics messages are reported.
Suppression of error LED	None Channel 1 Channel 2	Selection of whether the error LED (ERR) of a channel is suppressed.
Interface	RS232	The parameter value "RS232" must be selected in this parameter.

Alternatively, the connection can be made using a serial module with RS232 interface and P2P communication (e.g. ET 200SP CM PTP).

Connection via a third-party controller or any serial module

When using third-party controllers or any serial modules, programming and parameter assignment can also be performed using the following commands.

Application example

The following link shows an application example for connecting the RF1040R/RF1070R readers via an RF170C communication module.

Application example (https://support.industry.siemens.com/cs/ww/en/view/109770535)

7.3.1 Implementation of the commands

The different jobs are described in more detail below. Note that you must wait for the respective response telegram (reader response time) before you can send new request telegrams.

The parameter length is entered in "Big Endian" format and always refers to the user data as of byte 5 excluding the optional checksum. All other data is output in "Little Endian" format.

Implementation for connection via a SIMATIC Ident communication module

Communication takes place using the ident blocks / the ident profile or the function block FB 45. The "Write" command handles the sending of data and the "Read" command the receipt of data. The maximum length of the telegrams (header and data) is 233 bytes or 229 bytes with the Ident profile.

Before you execute a "Read" or "Write" command for the first time, you need to once execute a "Reset" command ("syscmd_reset"). With the "Reset" command, communication between the CM and reader is reset and the buffer is emptied.

Alternatively, you can also communicate with the reader via OPC UA or XML. In this case, the data is sent and received using the OPC UA methods "WriteTag" and "ReadTag" or the XML commands "writeTagMemory" and "readTagMemory".

Checksum calculation ("BCC8")

Note that all bytes of the telegram must be linked with an "XOR" logical operator to calculate the checksum. The result is shown in the "Optional checksum" field.

7.3.2 Commands

For a textual description of how the various commands work, refer to the section "Functions of the USB/RS232 interface for Windows (Page 34)".

7.3.2.1 syscmd_reset

Max. reader response time: 100 ms

Table 7-22 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x00	DevCode of the command set containing the command to be called.
2	0x03	CmdCode of the command to be called.
3 ... 4	0x00	Parameter length (0 bytes)
5	0xC2	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-23 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x00	DevCode of the command set containing the command to be called.
2	0x03	CmdCode of the command to be called.

Byte	Value	Description
3 ... 4	0x00	Parameter length (0 bytes)
5	0xC2	Optional checksum (when the value "0x1C" is set in byte 0)

7.3.2.2 syscmd_get_info

Max. reader response time: 50 ms

Table 7-24 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x00	DevCode of the command set containing the command to be called.
2	0x04	CmdCode of the command to be called.
3 ... 4	0x00	Parameter length (0 bytes)
5	0xC5	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-25 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x00	DevCode of the command set containing the command to be called.
2	0x04	CmdCode of the command to be called.
3	0x29	Parameter length (e.g. 41 bytes)
4	0x00	
5 ... 45	0x01 ...	Firmware version of the reader, date of manufacture as ASCII value Example: 1100 IDE Z 1.02.00 09/18/18 43025112
46	0xXX	Optional checksum (when the value "0x1C" is set in byte 0)

7.3.2.3 syscmd_get_boot_status

Max. reader response time: 50 ms

Table 7-26 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x00	DevCode of the command set containing the command to be called.
2	0x05	CmdCode of the command to be called.

Byte	Value	Description
3 ... 4	0x00	Parameter length (0 bytes)
5	0xC4	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-27 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x00	DevCode of the command set containing the command to be called.
2	0x05	CmdCode of the command to be called.
3	0x04	Parameter length (4 bytes)
4	0x00	
5 ... 8	0x00	Boot status = 0x00 (OK)
9	0x48	Optional checksum (when the value "0x1C" is set in byte 0)

7.3.2.4 syscmd_set_port

Max. reader response time: 100 ms

Table 7-28 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x00	DevCode of the command set containing the command to be called.
2	0x07	CmdCode of the command to be called.
3	0x02	Parameter length (2 bytes)
4	0x00	
5	0x00	port_msk:
6	0xXX	• 0x00: LED and acoustic signal • 0x01: LED lit green • 0x02: LED lit red • 0x03: LED lit orange • 0x04: Acoustic signal (only for RF1040R/RF1070R) • 0x05: Acoustic signal (only for RF1040R/RF1070R) and LED lit green • 0x06: Acoustic signal (only for RF1040R/RF1070R) and LED lit red • 0x07: Acoustic signal (only for RF1040R/RF1070R) and LED lit orange
7	0xXX	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-29 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x00	DevCode of the command set containing the command to be called.
2	0x07	CmdCode of the command to be called.
3	0x00	Parameter length (0 bytes)
4	0x00	
5	0xC6	Optional checksum (when the value "0x1C" is set in byte 0)

7.3.2.5 syscmd_get_licenses

Max. reader response time: 100 ms

Table 7-30 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x00	DevCode of the command set containing the command to be called.
2	0x29	CmdCode of the command to be called.
3 ... 4	0x00	Parameter length (0 bytes)
5	0x35	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-31 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x00	DevCode of the command set containing the command to be called.
2	0x29	CmdCode of the command to be called.
3	0x04	Parameter length (e.g. 4 bytes)
4	0x00	
5	0x00	Reserved
6	0x00	
7	0x00	

Byte	Value	Description
8	0xXX	Screen form for the license: • Bit 0: – 0: No HID license found. – 1: HID license found. • Bit 3: – 0: No BLE license found. – 1: BLE license found.
9	0xXX	Optional checksum (when the value "0x1C" is set in byte 0)

7.3.2.6 vhl_select

Max. reader response time: 3 s

Table 7-32 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x00	CmdCode of the command to be called.
3	0x04	Parameter length (4 bytes)
4	0x00	
5	0xFF	Mask for the card type (e.g. 0xFFFF) You can find detailed information on the card types in the section "vhl_select (Page 43)".
6	0xFF	
7	0x01	Reselect = 0x01
8	0x00	AllowConfig = 0x00
9	0xXX	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-33 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x00	CmdCode of the command to be called.
3	0x01	Parameter length (1 byte)
4	0x00	
5	0x30	Card type (e.g. 0x30) You can find detailed information on the card types in the section "vhl_select (Page 43)".
6	0x0D	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-34 Response telegram with errors

Byte	Value	Description
0	0x8C	Without checksum
	0x9C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x00	CmdCode of the command to be called.
3	0x01	Parameter length (1 byte)
4	0x00	
5	0xXX	Status Possible status codes: • 0x01: NOTAG_ERR • 0x03: HF_ERR • 0x08: CONFCARD_READ • 0x0C: HW_ERR You can find more detailed information on the reader status in the section "Status codes (Page 66)".
6	0xD9	Optional checksum (when the value "0x9C" is set in byte 0)

7.3.2.7 vhl_get_snr

Max. reader response time: 100 ms

Table 7-35 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x01	CmdCode of the command to be called.
3 ... 4	0x00	Parameter length (0 bytes)
5	0x0D	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-36 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x01	CmdCode of the command to be called.
3	0x04	Parameter length, depending on card type (e.g. 4 bytes)
4	0x00	

Byte	Value	Description
5	0x11	Serial number of the card, depending on card type
6	0x22	
7	0x33	
8	0x44	
9	0xXX	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-37 Response telegram with errors

Byte	Value	Description
0	0x8C	Without checksum
	0x9C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x01	CmdCode of the command to be called.
3	0x01	Parameter length (1 byte)
4	0x00	
5	0x02	CARD_NOT_SELECTED_ERR
6	0x9F	Optional checksum (when the value "0x9C" is set in byte 0)

7.3.2.8 vhl_is_selected

Max. reader response time: 3 s

Table 7-38 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x04	CmdCode of the command to be called.
3 ... 4	0x00	Parameter length (0 bytes)
5	0x08	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-39 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x04	CmdCode of the command to be called.
3 ... 4	0x00	Parameter length (0 bytes)
5	0x08	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-40 Response telegram with errors

Byte	Value	Description
0	0x8C	Without checksum
	0x9C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x04	CmdCode of the command to be called.
3	0x01	Parameter length (e.g. 1 byte)
4	0x00	
5	0x02	CARD_NOT_SELECTED_ERR
6	0x9A	Optional checksum (when the value "0x9C" is set in byte 0)

7.3.2.9 vhl_read

Max. reader response time: 3 s

Table 7-41 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x02	CmdCode of the command to be called.
3	0x05	Parameter length (e.g. 5 bytes)
4	0x00	
5	0xFF	ID of the VHL function (e.g. 0xFF [factory setting for ISO 15693])
6	0x00	Address (e.g. 0x37)
7	0x37	
8	0x00	Length (e.g. 0x08)
9	0x08	
10	0xXX	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-42 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x02	CmdCode of the command to be called.
3	0x08	Parameter length (e.g. 8 bytes)
4	0x00	
5 ... 12	0xCC	Read data (e.g. 0xCC)
13	0xXX	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-43 Response telegram with errors

Byte	Value	Description
0	0x8C	Without checksum
	0x9C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x02	CmdCode of the command to be called.
3	0x01	Parameter length (e.g. 1 byte)
4	0x00	
5	0xXX	Status Possible status codes: • 0x02: CARD_NOT_SELECTED_ERR • 0x03: HF_ERR • 0x05: AUTH_ERR • 0x06: READ_ERR • 0x08: CONFCARD_READ • 0x0C: HW_ERR You can find more detailed information on the reader status in the section "Status codes (Page 66)".
6	0xXX	Optional checksum (when the value "0x9C" is set in byte 0)

7.3.2.10 vhl_write

Max. reader response time: 3 s

Table 7-44 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x03	CmdCode of the command to be called.
3	0x0D	Parameter length (e.g. 13 bytes)
4	0x00	
5	0xFF	ID of the VHL function (e.g. 0xFF [factory setting for ISO 15693])
6	0x00	Address (e.g. 0x42)
7	0x42	
8	0x00	Length (e.g. 0x08)
9	0x08	
10 ... 17	0x33	Data to be written (e.g. 0x33)
18	0xXX	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-45 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x03	CmdCode of the command to be called.
3 ... 4	0x00	Parameter length (0 bytes)
5	0x0F	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-46 Response telegram with errors

Byte	Value	Description
0	0x8C	Without checksum
	0x9C	With checksum
1	0x01	DevCode of the command set containing the command to be called.
2	0x03	CmdCode of the command to be called.
3	0x01	Parameter length (e.g. 1 byte)
4	0x00	
5	0xXX	Status Possible status codes: • 0x02: CARD_NOT_SELECTED_ERR • 0x03: HF_ERR • 0x05: AUTH_ERR • 0x06: READ_ERR • 0x08: CONFCARD_READ • 0x0C: HW_ERR You can find more detailed information on the reader status in the section "Status codes (Page 66)".
6	0x9C	Optional checksum (when the value "0x9C" is set in byte 0)

7.3.2.11 Autoread_SetMode

Max. reader response time: 100 ms

Table 7-47 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x05	DevCode of the command set containing the command to be called.
2	0x00	CmdCode of the command to be called.
3	0x01	Parameter length (1 byte)
4	0x00	

Byte	Value	Description
5	0xXX	Autoread: • Off (0x00) • On, permanently (0x01) • On, once (0x02)
6	0xXX	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-48 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x05	DevCode of the command set containing the command to be called.
2	0x00	CmdCode of the command to be called.
3 ... 4	0x00	Parameter length (0 bytes)
5	0xC4	Optional checksum (when the value "0x1C" is set in byte 0)

7.3.2.12 Autoread_GetMessage

Max. reader response time: 100 ms

Table 7-49 Request telegram

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x05	DevCode of the command set containing the command to be called.
2	0x01	CmdCode of the command to be called.
3 ... 4	0x00	Parameter length (0 bytes)
5	0x4D	Optional checksum "BCC8" (when the value "0x1C" is set in byte 0)

Table 7-50 Response telegram without errors

Byte	Value	Description
0	0x0C	Without checksum
	0x1C	With checksum
1	0x05	DevCode of the command set containing the command to be called.
2	0x01	CmdCode of the command to be called.
3	0x07	Parameter length (7 bytes)
4	0x00	
5	0x00	Message type
6	0x05	Message length (e.g. 0x05)

Byte	Value	Description
7 ... 11	0x11	Data from the user memory (e.g. 0x11)
12	0xXX	Optional checksum (when the value "0x1C" is set in byte 0)

Table 7-51 Response telegram with errors

Byte	Value	Description
0	0x8C	Without checksum
	0x9C	With checksum
1	0x05	DevCode of the command set containing the command to be called.
2	0x01	CmdCode of the command to be called.
3	0x01	Parameter length (1 byte)
4	0x00	
5	0xXX	Status Possible status codes: • 0x01: NO_MESSAGE_ERR • 0x10: AR_DISABLED_ERR
6	0xDC	Optional checksum (when the value "0x9C" is set in byte 0)

7.4 Status codes

The following table contains a list of the general status codes.

Table 7-52 General status codes

Value	Variable	Description
0x00	OK	No error
0x40	CMD_WORK	The job is currently being processed.
0x41	INVAILD_CMD_ERR	Invalid function Causes: • The function is not valid. • The parameters are invalid. • The response exceeds 255 bytes. • Missing configuration
0x42	ACCESS_DENIED_ERR	Missing authentication
0x81	TIMEOUT_ERR	The reader is currently in timeout.
0x82	FRAME_ERR	Invalid command from host.
0x83	AME_OVERFLOW_ERR	The length of the response exceeds the maximum permissible length.
0x84	CHK_ERR	Invalid checksum in the host command.

The following table contains a list of the status codes of the VHL command set divided up into command groups.

Table 7-53 Status code of the VHL command set

Value		Variable	Description
USB	**RS232**		
syscmd			
0x0000	0x00	STATUS_OK	No error
vhl			
0x0101	0x01	NOTAG_ERR	Transponder does not exist or no response. This status code requires reselection of the card with the function "vhl_select".
0x0102	0x02	CARD_NOT_SELECTED_ERR	The function cannot be executed because no transponder is selected.
0x0103	0x03	HF_ERR	Communications problems with the transponder.
0x0104	0x04	CONFIG_ERR	The structure of the VHL function is invalid or was not found.
0x0105	0x05	AUTH_ERR	Authentication error. The keys in the VHL function are invalid (MIFARE) or the stamp in the reader is invalid (LEGIC cards).
0x0106	0x06	READ_ERR	The communications sequence is successful, but reading failed.
0x0107	0x07	WRITE_ERR	This value is currently not supported.
0x0108	0x08	CONFCARD_READ	A transponder was recognized.
0x0109	0x09	INVALID_CARD_FAMILY_ERR	The required transponder type does not match the transponder family of the currently selected transponder.
0x010A	0x0A	NOT_SUPPORTED_ERR	The function is not supported.
0x010B	0x0B	VHL_FORMAT_ERR	Format error
0x010C	0x0C	VHL_HW_ERR	Hardware problems during access (e.g. on the reader chip)
Autoread			
0x0501	0x01	NO_MESSAGE_ERR	No valid card / no valid transponder recognized.
0x0502	0x02	SCRIPT_RUNTIME_ERR	Runtime error detected during script execution.
0x0503	0x03	SCRIPT_SYNTAX_ERR	Syntax error in the script
0x0504	0x04	SCRIPT_NOT_IMPL_ERR	Scripts does not exist.
0x0510	0x10	AR_DISABLED_ERR	"Autoread" function is switched off.

The functions are constructed so that if execution fails, they are automatically repeated. This compensates any communications problems that may occur, e.g. due to bad RF signal quality as a result of external influences.

Demo application

8

The demo application contained in the file "RF1000R_Vxxx.exe" helps you to understand the available functions. You will find the file on the Siemens "Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/109741590)".

The available software package contains a demo application based on "Windows .NET 3.5" including source code files. This demo application serves as a model on the basis of which you can program your own user application. The demo application includes all the functions described in the following sections and is fully functional. This gives you the opportunity of testing your readers directly using the demo application.

Note

Disclaimer of liability

Note that Siemens AG accepts no liability for the demo application.

8.1 User interface of the demo application

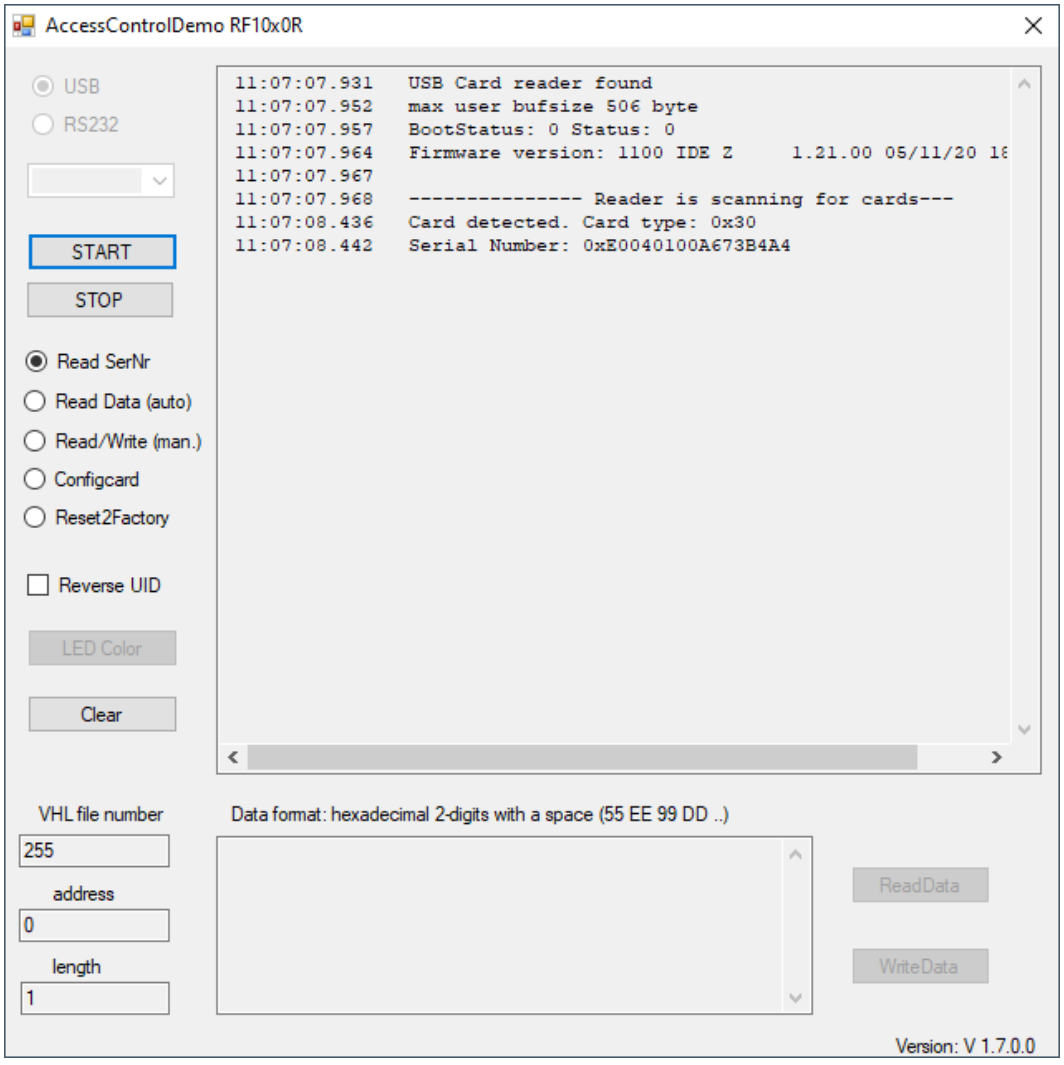
Requirement

To work with the demo application, .NET 3.5 must be installed on your PC (Windows) and the "RF1000R_Vxxx.exe" file must be unzipped.

Working with the demo application

Follow the steps below to work with the demo application:

1. Start the demo application by double-clicking on the file "AccessControlDemo.exe".



Buttons

START	Establishes the USB connection to the reader.
STOP	Terminates the USB connection to the reader.
LED Color	Switches the LED color and activates the acoustic signal.
Clear	Emptying the top display area.
ReadData	Manual reading of the transponder data.
WriteData	Manual writing of the transponder data.

Option buttons / check boxes and drop-down list

USB	Operation via the USB interface
RS232	Operation via the RS232 interface (or via the USB interface with COM port emulation)
COM	Selection of the COM port used
Read SerNr	Read the serial number and the card type.
Read Data (auto)	Automatic reading of the transponder data depending on the specific card type configuration.

Read/Write (man.)	Manual reading/writing of the transponder data depending on the selected parameters.
Configcard	Transferring the configuration from the configuration card in the antenna field to the reader.
Reset2Factory	Resetting the reader to factory settings and deleting user-specific data.
Reverse UID	Reversing the byte sequence when the serial number is output.
Input boxes	
VHL file number	Input box for the ID of the VHL function Default = 255; if no configuration has been transferred to the reader. The corresponding VHL ID must be selected for a specific configuration.
address	Input box for the start address as of which the transponder data is to be read or written.
length	Input box for the data length of the transponder data to be read/written.

Figure 8-1 Example view of reading a serial number

The version number of the demo application is shown at the bottom right in the application.

2. Use the option buttons to select the interface via which the reader is operated ("USB" / "RS232 COM").
3. Click the "Start" button to set up the connection to the reader and start the selected action.

Option buttons	Description
Read SerNr	Read the serial number and the card type. The data is output in the top display area.
Read Data (auto)	Automatic, periodic reading of the transponder data depending on the card-type specific configuration. The data is output in the bottom display area. Requirement: Autoread configuration is stored on the reader.
Read/Write (man.)	Manual reading/writing of transponder data depending on the selected VHL function ("VHL file number"), as well as the start address and the data length ("address" and "length"). The read or write operation is initiated with the "Read Data" or "Write Data" buttons. The transponder data to be written or read are edited or output in the bottom input/display area.
Configcard	Transferring the configuration from the configuration card in the antenna field to the reader. Note that the connection is terminated after the transfer ("Stop") and must be reestablished ("Start").

4. To clear the display area, click on the "Clear" button.
5. Click the "Stop" button to disconnect the reader.

8.2 Creating a custom application

You can create custom applications for operation via USB or RS232 interface. The creation of some sample applications is described below.

Requirement

- The reader is connected.
- When programming via the USB interface:
  You have unzipped the file "RF1000R_Vxxx.exe" onto your PC (Windows).

You require Microsoft Visual Studio (Express) on your PC to edit the source code.

Note that the demo application is capable of running without Microsoft Visual Studio (Express) being installed. You can view and edit the source code using a text editor.

Create your own "Read serial number" application

Follow the steps below to create your own application for reading the serial number:

1. Establish the connection to the reader ("brp_open_usb_session" or "brp_open_serial_session").
2. Check cyclically whether a transponder is located in the read range of the reader ("vhl_select").
   There is transponder in the read range:
   - The transponder is recognized.
   - Read out the serial number ("vhl_get_snr").
   - The application reports that the transponder with the serial number "x" has been detected.

   The transponder is no longer within the read range:
   - The application signals that the transponder with the serial number "x" is no longer recognized.
3. Terminate the connection to the reader ("brp_close_session").

The source code of the demo application can serve as an example for your own application.

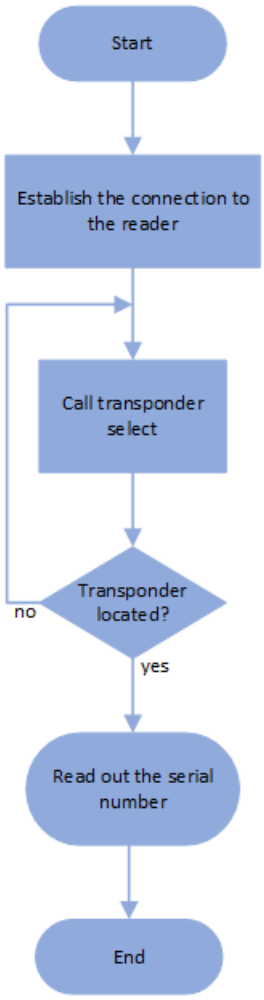


Figure 8-2 "Read serial number" flow diagram

Create your own "Autonomous reading" application

Requirements: A corresponding configuration is stored in the reader.

Follow the steps below to create your own application for autonomous reading of the transponder data:

1. Establish the connection to the reader ("brp_open_usb_session" or "brp_open_serial_session").
2. Switch on Autoread mode ("Autoread_SetMode" / "exec_command", devcode = 0x05, cmdcode = 0x00, param = 0x01 or 0x02)
   - The transponder is recognized automatically.
   - Read out the transponder data ("Autoread_GetMessage" / "exec_command", devcode = 0x05, cmdcode = 0x01)

The source code of the demo application can serve as an example for your own application.

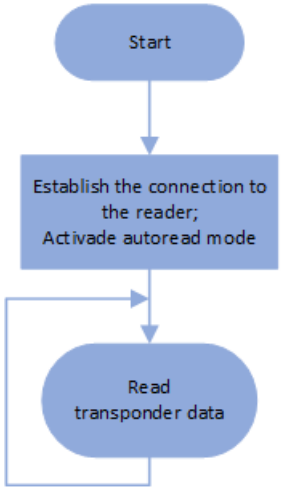


Figure 8-3 "Autonomous reading" flow diagram

Create your own "Read/write memory area" application

Follow the steps below to create your own application for reading or writing user data:

1. Establish the connection to the reader ("brp_open_usb_session" or "brp_open_serial_session").
2. Check cyclically whether a transponder is located in the read range of the reader ("vhl_select").
   When a transponder is located in the read range:
   - The transponder is recognized.
   - You can read data from the memory area with the "vhl_read" function.
   - You can write data to the memory area with the "vhl_write" function.
3. Terminate the connection to the reader ("brp_close_session").

The source code of the demo application can serve as an example for your own application.

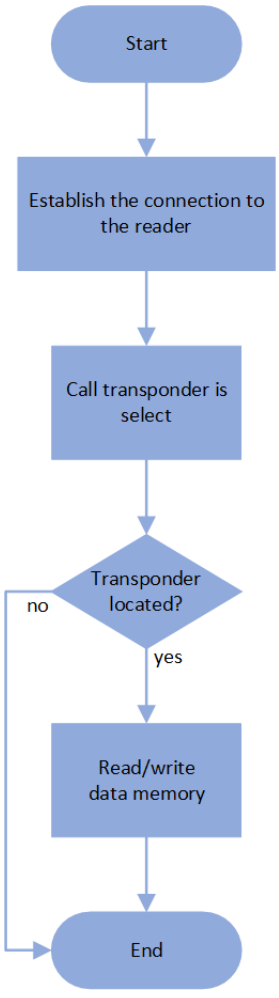


Figure 8-4 "Read/write memory area" flow diagram

Own application "Transfer reader configuration"

Requirement: A corresponding VHL configuration was created and transferred to a configuration card.

Follow the steps below to transfer a reader configuration using a configuration card:

1. Establish the connection to the reader ("brp_open_usb_session" or "brp_open_serial_session").
2. Check whether a configuration card is located in the read range of the reader ("vhl_select"; "AllowConfig = true").
   If a configuration card is located in the read range, the status code "CONFIG_READ" or "HF_ERR" is returned and the configuration is transferred to the reader. Parameterization is complete as soon as "vhl_select = STATUS_OK" is returned.
3. Terminate the connection to the reader ("brp_close_session").
4. Establish the connection to the reader again ("brp_open_usb_session").

The source code of the demo application can serve as an example for your own application.

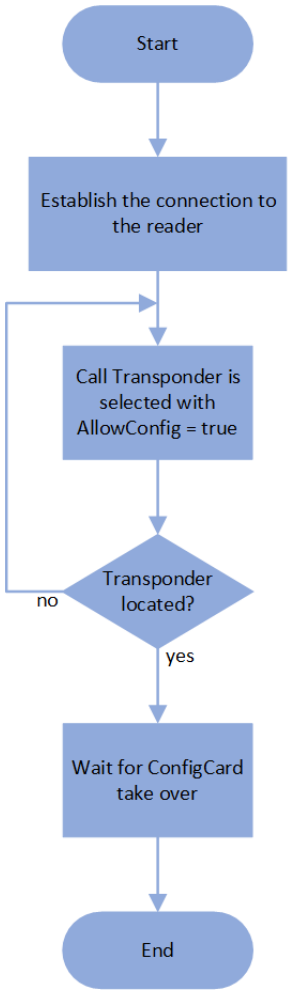


Figure 8-5 "Transfer reader configuration" flow diagram

Technical specifications

9

9.1 Technical specifications of SIMATIC RF1000

Table 9-1 Technical specifications of the SIMATIC RF1000 reader

		6GT2831-6xAx0 6GT2831-6BAx0-0AX0
Product type designation	SIMATIC RF1040R SIMATIC RF1060R SIMATIC RF1070R	
Radio frequency		
Operating frequency		
• RFID	• RF1040R: 125 kHz; 13.56 MHz • RF1060R: 13.56 MHz • RF1070R: 13.56 MHz	
• BLE	• 2.402 ... 2.48 GHz	
Protocol for wireless transmission	RF1040R, RF1060R, RF1070R: ISO 14443 A/B, ISO 15693, LEGIC advant, MIFARE Classic, MIFARE DESFire, MIFARE Plus, MIFARE Ultralight, HID iClass, NXP NTAG21x, FeliCa BLE for wireless communication RF1040R (in addition): EM4100/EM4102, EM4450/EM4550, HITAG 1, HITAG S, HITAG 2, Keri, SecuraKey, AWID, ioProxy RF1070R (in addition): LEGIC prime	
Electrical data		
Maximum transmission power	• RF1040R: – 125 kHz: < 50 mW – 13.56 MHz: 250 mW • RF1060R: 250 mW • RF1070R: 200 mW	
Maximum range	30 mm	
Mechanical specifications		
Housing		
• Material	• Lexan EXL5689	
• Color	• TI-Gray	

	6GT2831-6xAx0 **6GT2831-6BAx0-0AX0**
Interfaces	
Interface to the communications module	• USB 2.0, Type A (480 Mbps) • RS232 (115.2 kBd; no parity) [1]
RFID	Integrated antenna
BLE	Integrated antenna (default: deactivated)
Supply voltage, current consumption, power loss	
Power supply	4.6 to 5.25 V DC
Current consumption	• Typ. 150 mA • Max. 300 mA
Permitted ambient conditions	
Ambient temperature	
• During operation	• -25 ... +55 °C
• During transportation and storage	• -25 ... +55 °C
Minimum distance between two readers	15 cm [2]
Degree of protection according to EN 60529 (in installed state)	
• In-wall / cabinet installation	• Front: IP65 [3] Rear: IP20
• Surface/table installation	• Front: IP41 [3] Rear: IP20
Shock-resistant to EN 60721-3-7, Class 7 M2	300 m/s²
Vibration-resistant to EN 60721-3-7, Class 7 M2	50 m/s²
Design, dimensions and weights	
Dimensions (W × H × D)	
• Reader excl. card holder	• 90 × 62 × 23.5 mm
• Reader incl. card holder	• 99 × 62 × 34.6 mm
• Mounting opening	• 76.5 (± 0.3) × 48.5 (± 0.3) mm
Weight	approx. 120 g
Type of mounting	
• In-wall / cabinet installation	• 4 x stud screws (slotted screws) M4 x 20 • 4 x Torx screws (EJOT) T10 x 10; Tightening torque ≤ 1.5 Nm • Installation wall thickness 2-7 mm

	6GT2831-6xAx0 **6GT2831-6BAx0-0AX0**
• Surface/table installation	• 4 x Torx screws (EJOT) T10 x 10; Tightening torque ≤ 1.5 Nm • Surface installation: 4x screws M4 or 4 mm • Table installation: 4x rubber stoppers
Cable length reader ↔ communications module	USB connection cable: 1.8 m RS232 connection cable: 2 or 3 m
Display elements	• LED, 3 colors • Acoustic sensor [4]
Approvals	CE / FCC / IC
MTBF	28 years

[1] Only in conjunction with the SIMATIC RF1040R reader as of product version "AS: A" and SIMATIC RF1070R as of product version "AS: B", and SIMATIC RF1070R OEM as of product version "AS: A".

[2] The minimum distance can be lowered if, from an application point of view, it is permissible that a transponder can also be read by an adjacent reader.

[3] IP67 or IP65 in connection with the cleanroom cover and sealing of the table/wall housing

[4] Only for the SIMATIC RF1040R and SIMATIC RF1070R readers

9.2 Technical specifications, RF1100T Configuration Card

Table 9-2 Technical specifications of the RF1100T configuration card

	6GT2300-0CC00-0AX0
Product type designation	SIMATIC RF1100T
Memory	
Memory configuration	
• UID	• 7 bytes
• User memory	• 8000 bytes EEPROM
Read cycles (at < 40 °C)	> 10^{12}
Write cycles (at < 40 °C)	> 10^{4}
Data retention time (at < 40 °C)	> 10 years
Write/read distance (S_g)	≤ 30 mm
Mechanical specifications	
Housing	
• Material	• PVC
• Color	• White
Printing	Writeable handwritten
Permitted ambient conditions	

	6GT2300-0CC00-0AX0
Ambient temperature	
• During write/read access	• -25 ... +60 °C
• Outside the read/write field	• -25 ... +60 °C
• During storage	• -25 ... +60 °C
Degree of protection according to EN 60529	IP67
Design, dimensions and weight	
Dimensions (D × W × H)	86 × 54 × 0.8 mm
Weight	6 g

9.3 Technical specifications of the license cards

Table 9-3 Technical specifications of the license cards

	6GT2300-0CC00-0AXx
Product type designation	HID license card for SIMATIC RF1000 and RF1100 BLE license card for SIMATIC RF1000
Mechanical specifications	
Housing	
• Material	• PVC
• Color	• White
Printing	Writeable handwritten
Permitted ambient conditions	
Ambient temperature	
• During write/read access	• -25 ... +60 °C
• Outside the read/write field	• -25 ... +60 °C
• During storage	• -25 ... +60 °C
Degree of protection according to EN 60529	IP67
Design, dimensions and weights	
Dimensions (D × W × H)	86 × 54 × 0.8 mm
Weight	6 g

9.4 Technical specifications of table/wall housing

Table 9-4 Technical specifications of table/wall housing for SIMATIC RF1000

	6GT2890-0CB00
Product type designation	Table/wall housing RF1000
Mechanical specifications	
Housing	
• Material	• Polycarbonate
• Color	• TI-Gray
Design, dimensions and weights	
Dimensions (W × H × D)	
• Table/wall housing	• 121 × 75.7 × 24.5 mm
• Table/wall housing incl. reader	
Weight	approx. 58 g

9.5 Technical specifications of cleanroom cover

Table 9-5 Technical specifications of the cleanroom covers for RF1000

	6GT2890-0Cx00
Product type designations	Cleanroom cover
Mechanical specifications	
Housing	
• Material	• Polycarbonate [1]
• Color	• Transparent
Design, dimensions and weight	
Dimensions (W × H × D)	
• Cabinet installation	• 95.9 × 66 × 8 mm
• Surface installation	• 124.2 × 78.2 × 29.2 mm
Weight	
• Cabinet installation	• approx. 15 g
• Surface installation	• Approx. 26 g

[1] UV-resistant, food-safe

Dimension drawings

10

All dimensions in mm

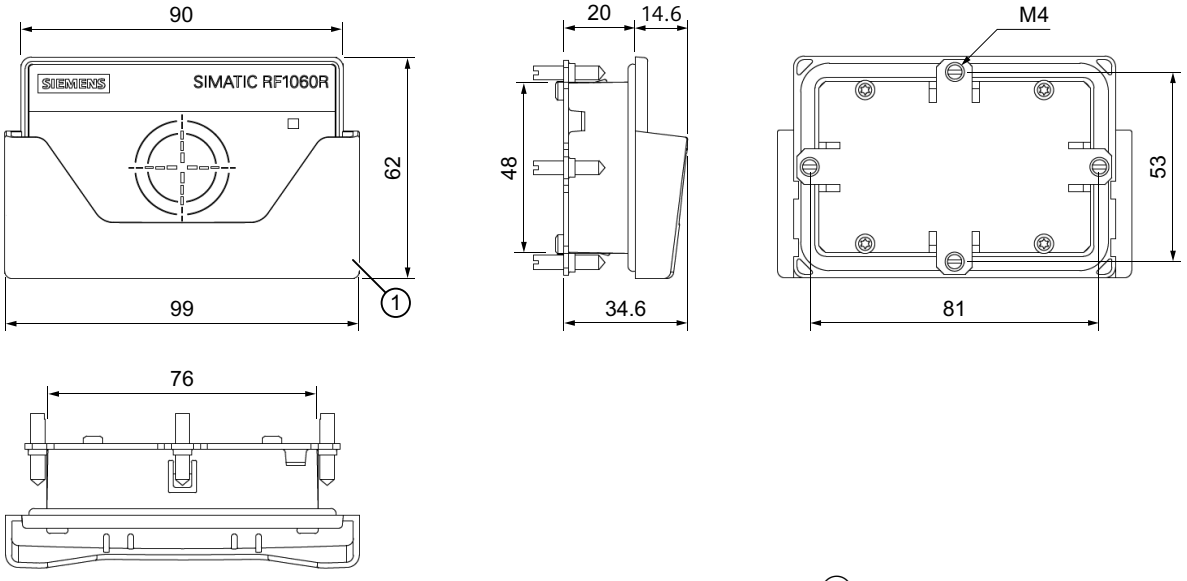


Figure 10-1 Dimension drawing SIMATIC RF1000 with optional card holder (1)

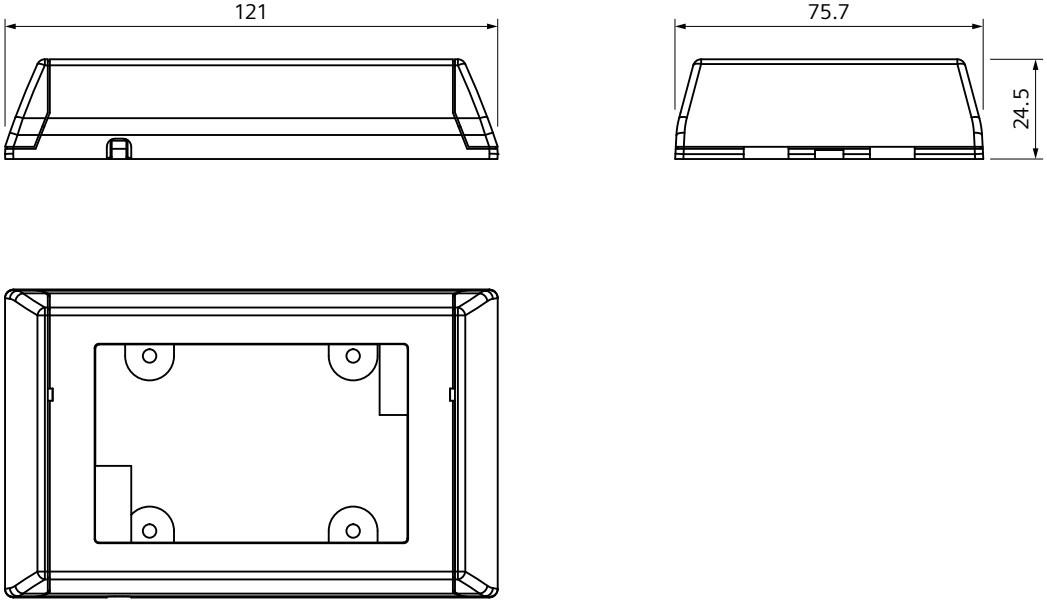


Figure 10-2 Dimension drawing of the table/wall housing

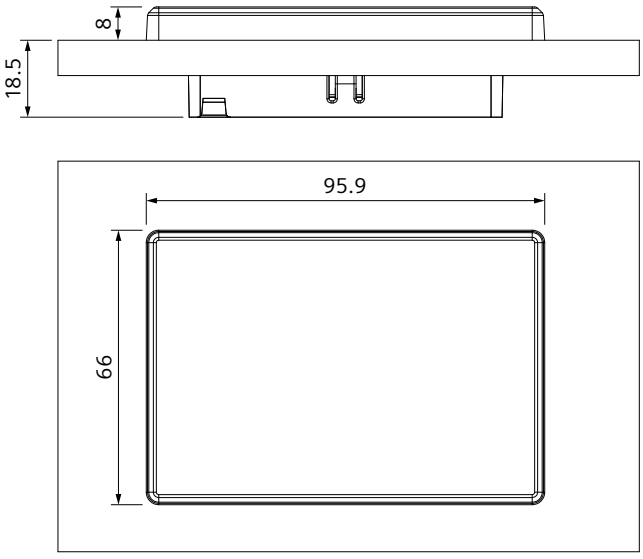


Figure 10-3 Dimension drawing of SIMATIC RF1000 with the cleanroom cover "Cabinet installation"

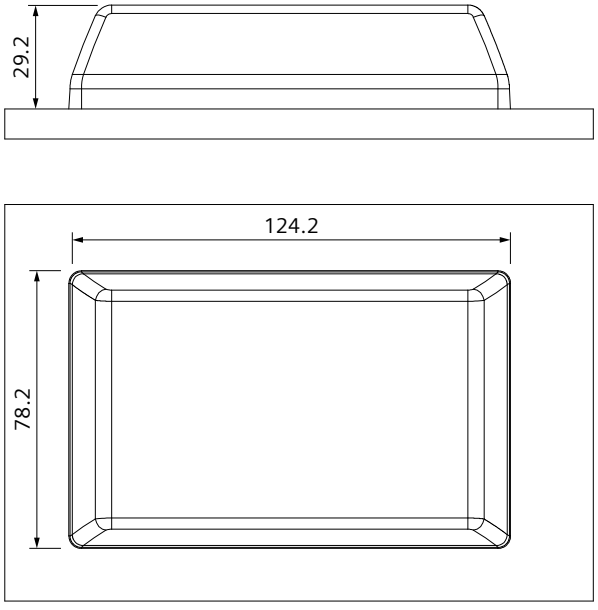


Figure 10-4 Dimension drawing of SIMATIC RF1000 with the cleanroom cover "Surface installation"

Appendix

A

A.1 Certificates & approvals

If a device has one of the following marks, the corresponding approval has been obtained.

Table A-1 Country-specific approvals

Marking	Description
CE	CE according to RED directive 2014/53/EU CE according to RoHS directive 2011/65/EU
FC Federal Communications Commission	1) Part 15 Clause 15.105: "Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: • Reorient or relocate the receiving antenna. • Increase the separation between the equipment and receiver. • Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. • Consult the dealer or an experienced radio/TV technician for help." 2) Statement for Part 15 Clause 15.21: "Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment." 3) Statement for FCC Part 15.19: "This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: • (1) This device may not cause harmful interference, and • (2) this device must accept any interference received, including interference that may cause undesired operation."

Marking	Description
Industry Canada Radio Standards Specifications	CAN ICES-3 (B)/NMB-3(B) This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions: • 1) This device may not cause interference; and • 2) This device must accept any interference, including interference that may cause undesired operation of the device. Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : • 1) l'appareil ne doit pas produire de brouillage; • 2) l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
UK CA	Importer UK: Siemens plc, Sir William Siemens House, Princess Road, Manchester M20 2UR
ANATEL 05695-22-04794 ANATEL 00860-17-04794	Brazil (ANATEL) Certificado de Homologação REPÚBLICA FEDERATIVA DO BRASIL AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados. Para maiores informações, consulte o site da ANATEL (www.anatel.gov.br). ANATEL IDs: • SIMATIC RF1040R (6GT2831-6CA50): 05695-22-04794 • SIMATIC RF1060R (6GT2831-6AA50): 05695-22-04794 • SIMATIC RF1070R (6GT2831-6BA50): 07881-18-04794 Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.
Mexico (IFETEL)	Mexico (IFETEL) Instituto Federal de Telecomunicaciones • SIMATIC RF1040R (6GT2831-6CA50): RCPSIRF20-0917 • SIMATIC RF1060R (6GT2831-6AA50): RCPSIRF16-2053 • SIMATIC RF1070R (6GT2831-6BA50): RCPSIRF18-2240

Marking	Description
	South Korea (KCC) Korea Communications Commission Certificate of Broadcasting and Communication Equipments Republic of Korea • SIMATIC RF1040R (6GT2831-6CA50): R-R-RF5-RF1040R • SIMATIC RF1060R (6GT2831-6AA50): MSP-CRM-RF5-RF1060R • SIMATIC RF1070R (6GT2831-6BA50): R-C-RF5-RF1070R
Thailand	Marking requirements: Following statement may be displayed on packaging or additional page or on user's manual. For Sdoc, it is optional to display this wording. **"เครื่องโทรคมนาคมและอุปกรณ์นี้มีความสอดคล้องตามมาตรฐานหรือข้อกำหนดทางเทคนิคของ กสทช."** This telecommunication equipment conforms to the technical standards or requirements of NBTC.

A.2 Connection via Remote Desktop Protocol (RDP)

Using the Remote Desktop Protocol (RDP), you can use a reader that is physically connected to the RDP client (e.g. Industrial Thin Client) on an RDP server. To establish a connection, you need to edit the group policies for the USB redirection on both the RDP server and the RDP client.

The following procedure only works for the virtual COM port of the reader. Note that the USB-HID interface cannot be used via RDP.

Editing RDP client group policies

Follow these steps to edit the group policies of the RDP client:

1. Open the Local Group Policy Editor on the RDP client.
   To do this, enter "gpedit" in the Windows search field.
2. Navigate to the menu "Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Connection Client > RemoteFX USB Device Redirection".
3. Double-click the entry "Allow RDP redirection of other supported RemoteFX USB devices from this computer" and select the "Enabled" option box.
4. Select "Administrators and Users" in the drop-down list in the "Options" area.
5. Close the Local Group Policy Editor.
6. Open the command prompt.
   To do this, enter "cmd" in the Windows search field.
7. In the command prompt, enter "gpupdate /force" to update the group policies.
8. Restart the client computer for your changes to take effect.

Editing RDP server group policies

Follow these steps to edit the group policies of the RDP server:

1. Open the Local Group Policy Editor on the RDP server.
   To do this, enter "gpedit" in the Windows search field.
2. Navigate to the menu "Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection".
3. Double-click the entry "Do not allow supported Plug and Play device redirection" and select the "Disabled" option box.
4. Close the window.
5. Double-click the entry "Do not allow COM port redirection" and select the "Disabled" option box.
6. Close the Local Group Policy Editor.
7. Open the command prompt.
   To do this, enter "cmd" in the Windows search field.
8. In the command prompt, enter "gpupdate /force" to update the group policies.
9. Restart the host computer for your changes to take effect.

Establishing an RDP connection

To establish an RDP connection, follow these steps:

1. Connect the reader to the RDP client.
2. Open the remote desktop connection and click "Show Options".
3. In the "Local Resources" tab, click on "More..." under "Local Devices and Resources".
4. Select the "Ports" check box.
5. Select the "Other supported RemoteFX USB devices" check box and select the desired reader.
6. Click "OK".
7. Click "Connect".

The reader is now displayed as serial device on the RDP server.

A.3 Ordering data

Table A-2 Ordering data

Product	Article number
SIMATIC RF1040R (AS: E)	6GT2831-6CA50
SIMATIC RF1060R (AS: E)	6GT2831-6AA50
SIMATIC RF1070R (AS: H)	6GT2831-6BA50
SIMATIC RF1070R (AS: H) OEM variant with neutral front foil	6GT2831-6BA50-0AX0

Product	Article number
SIMATIC RF1040R (AS: A)	6GT2831-6CA60
SIMATIC RF1060R (AS: A)	6GT2831-6AA60
SIMATIC RF1070R (AS: A)	6GT2831-6BA60
SIMATIC RF1070R (AS: A) OEM variant with neutral front foil	6GT2831-6BA60-0AX0

Table A-3 Ordering data accessories

Product		Article number
Card holder for RF1000		6GT2890-0CA00
Table/wall housing RF1000		6GT2890-0CB00
Cleanroom cover cabinet installation for RF1000		6GT2890-0CD00
Cleanroom cover surface installation for RF1000		6GT2890-0CC00
Configuration card RF1100T (pack of 5)		6GT2300-0CC00-0AX0
HID license card for SIMATIC RF1000 and RF1100		6GT2300-0CC00-0AX1
BLE license card for SIMATIC RF1000		6GT2300-0CC00-0AX2
Power supply unit LOGO! Power 5 V / 3 A		6EP3310-6SB00-0AY0
Optional USB connecting cable	0.5 m	6GT2891-0UE50
RS232 connecting cable for connection to communication modules M12 ↔ PicoBlade	2.0 m	6GT2891-4UH20
RS232 connecting cable for connection to a serial device Open cable end ↔ PicoBlade	3.0 m	6GT2891-2UH30
RS232 connecting cable for connection to a PC D-sub/USB ↔ PicoBlade	1.8 m	6GT2891-7UH18

Service & Support

B

Industry Online Support

In addition to the product documentation, you are supported by the comprehensive online information platform of Siemens Industry Online Support at the following Internet address:
Link: (https://support.industry.siemens.com/cs/de/en/)

Apart from news, you will also find the following there:

- Project information: Manuals, FAQs, downloads, application examples etc.
- Contacts, Technical Forum
- The option to submit a support request:
  Link: (https://support.industry.siemens.com/My/ww/en/requests)
- Our service offer:
  Right across our products and systems, we provide numerous services that support you in every phase of the life of your machine or system - from planning and implementation to commissioning, through to maintenance and modernization.

You will find contact data on the Internet at the following address:
Link: (https://www.automation.siemens.com/aspa_app/?ci=yes&lang=en)

"Industrial Identification" homepage

You can find the latest general information about our identification systems on the Internet at our Homepage (www.siemens.com/ident).

Online catalog and ordering system

The online catalog and the online ordering system can also be found on the Industry Mall home page (https://mall.industry.siemens.com).

SITRAIN - Training for Industry

The training offer includes more than 300 courses on basic topics, extended knowledge and special knowledge as well as advanced training for individual sectors - available at more than 130 locations. Courses can also be organized individually and held locally at your location.

You will find detailed information on the training curriculum and how to contact our customer consultants at the following Internet address:

Link: (https://new.siemens.com/global/en/products/services/industry/sitrain.html)