



SECURECOM

SC-GPRS M2

2G (GPRS) alarm monitoring communicator, for Contact ID reports forwarding in SIA DC-09 (IP) format

Installation manual v2.0

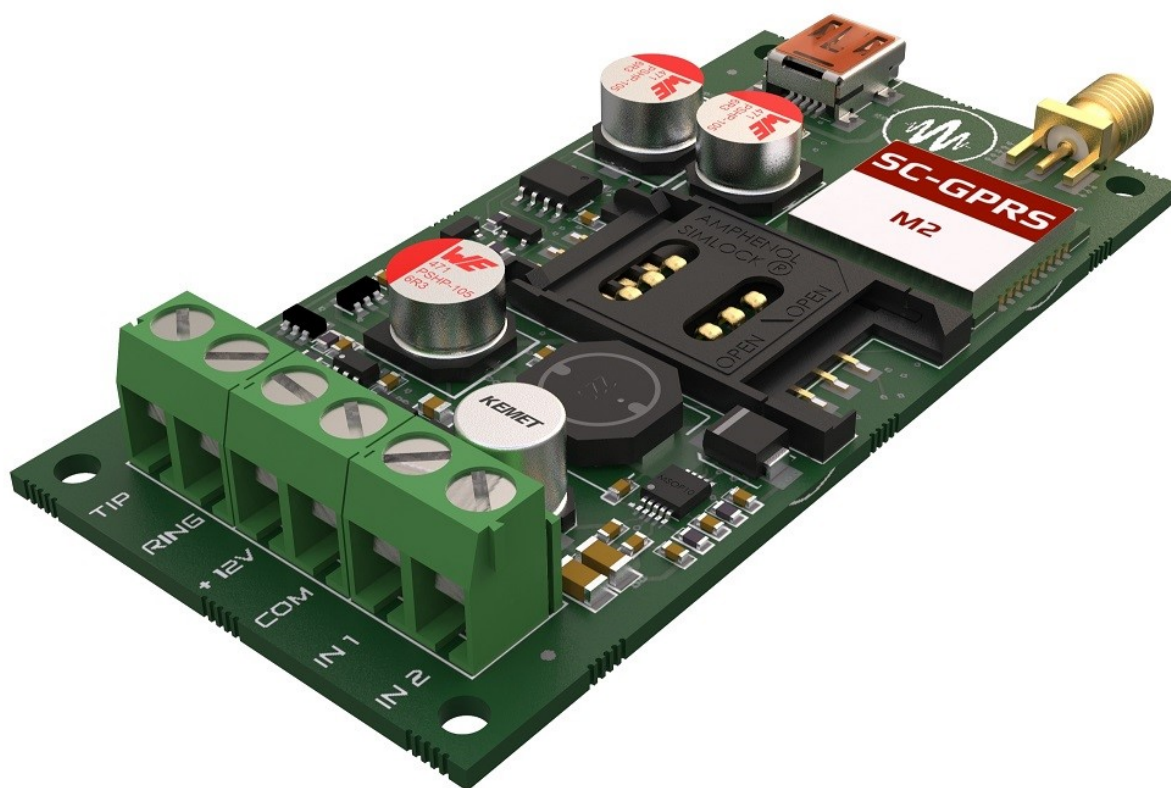


Table of content

1	General information.....	3
1.1	Main features.....	3
2	Device hardware.....	3
3	Required setting of alarm panel.....	4
4	Status signals.....	5
5	Settings.....	5
5.1	Setting the connection to mobile network (REQUIRED INITIAL SETTING).....	6
5.2	Monitoring station connection settings.....	6
5.3	Inputs events setting.....	8
5.4	Device's own events.....	8
5.5	Module Status panel.....	8
5.6	Remote management features.....	9
5.7	Latest Events window.....	9
5.8	Administrative window.....	10
6	Technical data.....	11
7	Device package content.....	11

1 General information

The SC-GPRS M2 device is a modern security communication device operating in GPRS channel of 2G mobile network. It converts the Contact ID signals from alarm panel (transmitted on phone line, TIP/RING terminals) to SIA IP format and sends it to a given IP monitoring receivers. The communication is performed on GPRS system, using TCP or UDP package format.

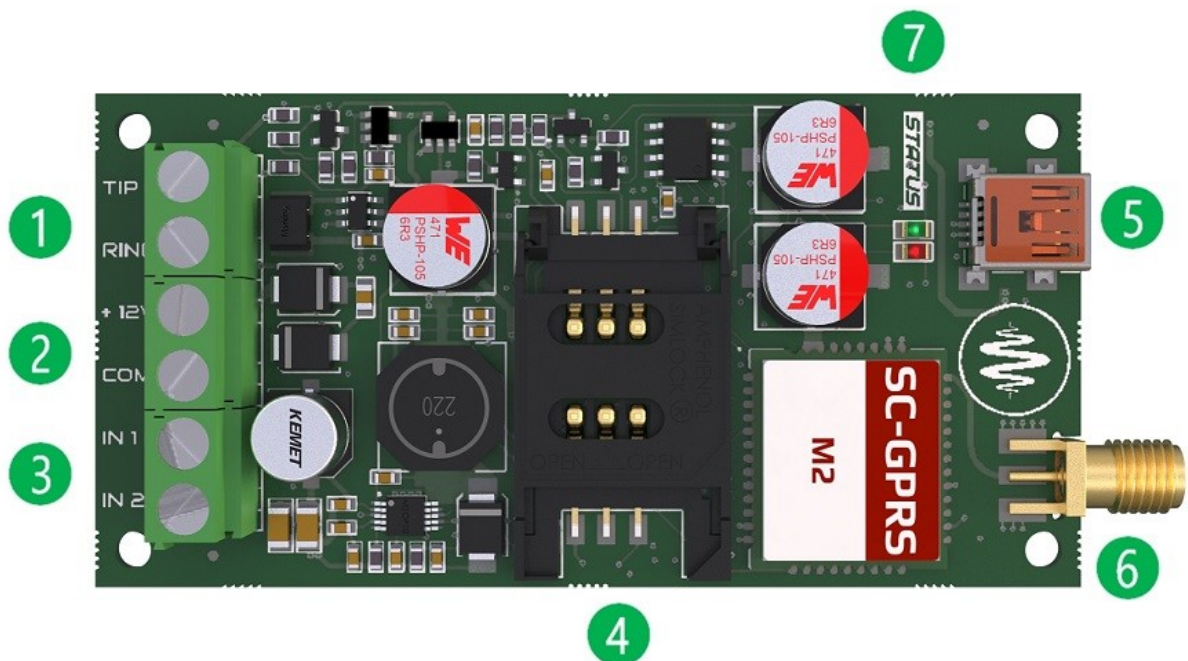
Operation of device: it generates a simulated PSTN line for alarm panel, and accepts Contact ID reports sent on it by alarm panel dialler. After receiving, device forwards the report through GPRS network, (using TCP or UDP protocol, depending on the setting) toward one of two pre-set IP receivers, in accordance to SIA DC 09 standard. The device will acknowledge the reporting to alarm panel only when the acknowledge signal is received back from the IP receiver, thus ensuring the 100% delivery rate for all reports! Also, contact signals applied to the two inputs are reported to monitoring station with programmed codes.

Device is equipped with an independent watchdog circuitry that prevents the device „freezing” phenomenon, caused by network deviations in most communication devices. When a communication error is detected, this circuitry cuts the device power supply for 5 seconds and after re-applying of power the device restarts, assuring that it connects again to mobile network.

1.1 Main features

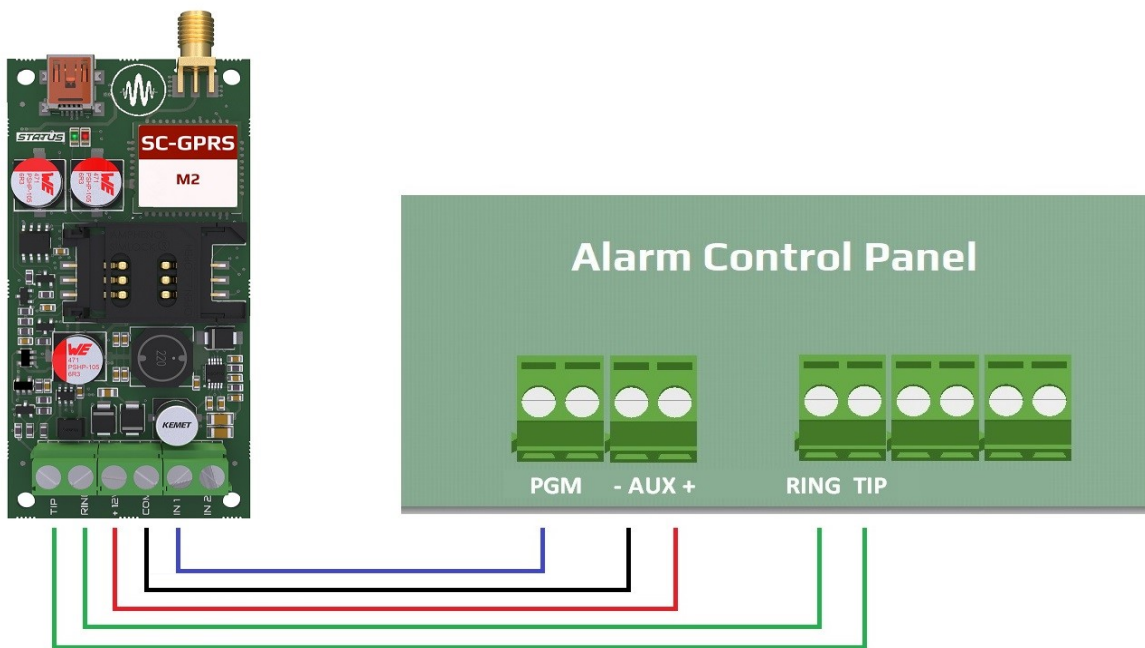
- Phone line simulation for alarm panels
- 2 contact inputs with independent signalling
- Handling 2 independent alarm monitoring receivers
- IP connection with UDP or TCP protocols
- Configuration with PC software, connecting with USB cable

2 Device hardware



- 1 **TIP/RING Communication terminals, generated phone line output**
Simulated PSTN line for connection to TIP/RING alarm panel input terminals
- 2 **Power supply terminals**
Required supply DC 9-30V / 300mA
- 3 **Inputs, triggered with dry contact**
- 4 **SIM card holder, for cards set for DATA connection**
Type: 2FF/mini SIM
- 5 **USB mini B connector for programming**
- 6 **GSM antenna connector, SMA type**
- 7 **Status signalling LED**

Connection diagram



3 Required setting of alarm panel

Connected alarm panel must have following settings:

- Phone communication should be enabled in the alarm centre
- DTMF (Tone) dialling should be selected
- A minimum 4 digit phone number should be set for dialling (anything is acceptable, e.g. 1111)
- Object identifier should be set
- Contact ID (Full) should be selected

The device will accept the Contact ID reports from alarm panel as a monitoring receiver, and forward them to IP monitoring receiver. Only after the reporting was acknowledged by monitoring station, the acknowledge signal will be transmitted to alarm panel.

4 Status signals

With the status LED **7**, device can display these basic statuses.

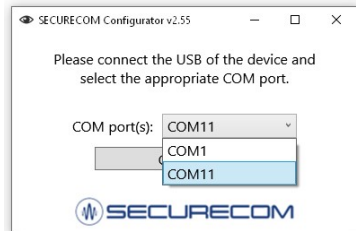
Continuous red	APN setting or SIM card missing
Blinking red	Connecting
Blinking green	Idle state (Device is ready, waiting for report from alarm panel)
Continuous green	Communication with alarm panel in progress

5 Settings

To set up the device install the SECURECOM CONFIGURATOR software. The installation file (securecomconfiguratorsetup.exe) is available on Securecom web site. Run the installer, it will make the software available from the start menu.



After running the program, connect the USB port of the device to the PC, and select the appropriate serial port, then push the “Connect” button. For example:



Once connected, device settings can be found on the following interface.

SECURECOM Configurator v2.60

TYPE: SC-GPRS
FIRMWARE: v2.3.569
Device ID: 3c606e9a46219769

EN DE HU

LATEST EVENTS

11:34:58: Phone initialization completed but still waiting for internet connection...

11:34:59: Phone connected to the internet!

11:34:59: Phone IP: 10.130.192.157

11:35:00: Send NULL test to MS1 (modem)

11:35:01: MS1 NULL test response (modem): ACK

11:35:01: Send event to MS1 (modem)

11:35:02: MS1 event response (modem): ACK

11:35:44: OFFHOOK


WARNING! Remote programming of the security system during USB connection is not allowed!

MODULE STATUS		MONITORING STATION 1 SETTINGS		MONITORING STATION 2 SETTINGS	
Mobile network:	EDGE (2G) T-Mobile Hungary	IP address:	siatest.securecom.eu	IP address:	
Network signal (%):	100%	Port:	9998	Port:	9998
Monitoring station 1:	OK	Protocol:	UDP	Protocol:	UDP
Monitoring station 2:		SIA prefix:		SIA prefix:	
Dial capture:	ONHOOK	Object identifier:	1632	Object identifier:	0000
Input 1:	INACTIVE	Replace obtained identifier:	YES	Replace obtained identifier:	YES
Input 2:	INACTIVE	Dialed number by alarm system:		Dialed number by alarm system:	
Supply voltage:	-	Link test period:	3 mins	Link test period:	3 mins
		Link test code:		Link test code:	

MODEM AND GPRS SETTINGS		COMM. EVENT CODES		INPUT 1 SETTINGS		INPUT 2 SETTINGS	
PIN code:		Battery low:	314	Sensitivity:	0.3 sec	Sensitivity:	0.3 sec
GPRS APN:	iot.truphone.com	Setup changed:	306	Contact type:	NO	Contact type:	NO
User:				Event code:	130	Event code:	130
Password:				Partition:	01	Partition:	01
				Zone:	001	Zone:	002

If a password was set for device, after connecting the window will be blurred and only the module status and Latest events panels will be visible. A dialog will appear in the middle, where the password should be entered. After entering the correct password, the blur will disappear.

Attention: To validate the changes, settings must be downloaded into the device!

Downloading of settings is performed with  icon. The latest events panel will show the changes. When any parameter value is changed in software, the background color of the icon becomes red, showing that the displayed values are not the valid ones (in the device), so they should be downloaded.

5.1 Setting the connection to mobile network (REQUIRED INITIAL SETTING)

Attention: These are the only parameters that **MUST** be set through USB connection. All other values can be changed through the web site, after the device becomes online on the server.

Appropriate SIM card must be inserted in the SIM holder **4**. These data are required about it:

- SIM must have assigned data plan
- SIM must be in active state
- Exact APN parameters must be available
- PIN code should be available or PIN request on start must be deactivated

If the PIN request is not disabled, it must be entered in the **SIM PIN** field. The APN name is always required for data connection, while the username and password are not required for most APN settings (SIM provider defines the APN settings for each SIM card).

MODEM AND GPRS SETTINGS	
PIN code:	
GPRS APN:	m2m.sim.com
User:	
Password:	

After downloading of settings the device will restart and after 30-60 seconds it will connect to network. The status LED **7** will start blinking green. The successful connection will be also shown as an event in the Last events panel of software.

5.2 Monitoring station connection settings

For connection to a SIA DC-09 monitoring receiver (e.g. IPR-5000) following parameters are required:

MONITORING STATION 1 SETTINGS	
IP address:	siatest.securecom.eu
Port:	9998
Protocol:	UDP ▾
SIA prefix:	
Object identifier:	6667
Replace obtained identifier:	YES ▾
Dialed number by alarm system:	
Link test period:	3 mins ▾
Link test code:	603

IP address	IP address or domain name of the monitoring station
Port	Receiving port number of the monitoring station's IP address (public port, forwarded in router to internal receiving port and address of receiver)
Protocol	Selectable communication IP protocol: TCP, UDP

SIA prefix	2 characters long SIA prefix, it is used if the monitoring station requires identifier with 6 characters (while the identifier in CID is only 4 characters).
Object identifier	Identifier used when reporting of personal events (e.g. test report, settings change, power error). This identifier is used for ALL reports (even for those coming from alarm panel) if the „replace identifier“ is set to value YES
Replace object identifier	When this value is set to „enabled“, all account numbers (customer ID) in CID reports coming from the alarm panel will be replaced with the identifier set in the “Object identifier“ field
Dialed number by alarm system	For default functionality (Report to MS1 and backup to MS2 leave the fields empty (for both MS1 and MS2 settings). Alarm panel can dial any number Value in this field is the number which must be dialled by alarm system if the to forward the reports from that call to corresponding IP receiver (MS1 or MS2).
Link test period	The test report will be sent to MS in intervals that are set in this field. If the selected value is „None“, the device will not send test reports to the monitoring station!
Link test code	The CID code that is sent as test report. If the value is empty, the test reports will be created as „nulltest“ (an empty code) - as it is defined by the SIA protocol.

The device can maintain the communication with up to 2 Monitoring Receivers. Connections are maintained by acknowledged periodic test report, and this is handled separately to the two receivers. For default reporting logic, the fields „Dialed number by alarm system“ should stay empty. Then the Monitoring station 1 is the primary, so all reports will be sent to it. In case when a report (Test report or some CID from alarm panel) to MS1 is not acknowledged after several attempts and alarm panels finishes the call, the device will determine that connection as bad, and next report from alarm panel (after next dialling) will be forwarded to the backup receiver, MS2. If both connections are bad (presented with status „error“), the device will not provide a „free line signal“ to alarm panel at all, so it should not try to send reports at all. Even while the reporting is directed to MS2, test reports are regularly sent to MS1 and as soon as the test report is sent successfully (the acknowledge is received back), the reports sending will be redirected to MS1 again.

When you want to use the two receives with routed reports, you must separate the desired report groups with two different phone numbers in alarm panel. Same numbers must be set in the „Dialed number by alarm system“ fields as well. So if alarm panel dials the number that is set in the MS2 settings, events reported after dialling will be sent to MS2.

If **"Replace object identifier"** is enabled, it will replace the client ID code in all reports from the alarm panel with the new ID set in the communicator and the modified reports will be send to the IP receiver.

This feature allows you to connect old alarm systems to the remote monitoring without changing the alarm panel settings.

5.3 Inputs events setting

Device provides 2 contact inputs, selectable for NO or NC type. The inputs are triggered with contact to **DC** – terminal. Triggering the inputs generates an event that is reported with a set ContactID code:

INPUT 1 SETTINGS		INPUT 2 SETTINGS	
Sensitivity:	0.3 sec	Sensitivity:	0.3 sec
Contact type:	NO	Contact type:	NO
Event code:	130	Event code:	130
Partition:	01	Partition:	01
Zone:	001	Zone:	002

The user account ID in the report is value of **Object identifier** field. The „event” or „restore” depends if the zone was opened or closed (depending on zone type setting NO or NC). The event code, partition and zone values will be as set in appropriate fields, for the triggered zone. Sensitivity is the minimum length of input status change (connected or disconnected) that will be detected.

5.4 Device’s own events

Device continuously monitors it’s supply voltage, and generates an event if it drops below 11V. This supervision is very important because the low supply voltage ruins the stability of communication. The generated event is also reported to monitoring station with the set report code. When the Voltage rises above 12V, the restore event is generated and reported with same event code. The account (user ID) in these reports is always the one that was set in the **Object Identifier** field, the partition number is always 00 and the zone number is 000.

Another supervised feature is the settings change. If the device settings are changed (through USB or through Puloware server), a „setup changed” event is generated and reported to the monitoring station with set report code. For this report, the partition and zone values are also always 00/000.

COMM. EVENT CODES	
Battery low:	314
Setup changed:	306

5.5 Module Status panel

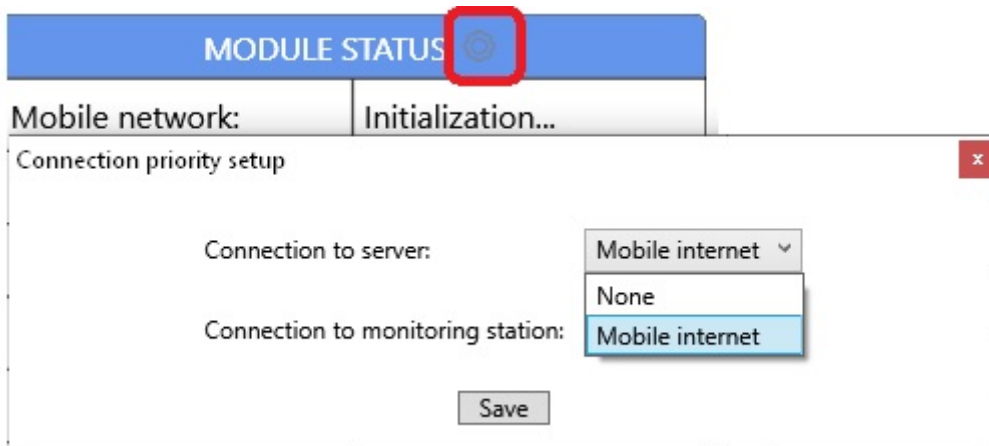
The „module status” panel shows the momentary values of the listed parameters.

MODULE STATUS	
Mobile network:	EDGE (2G) Vodafone
Network signal (%):	67%
Monitoring station 1:	OK
Monitoring station 2:	OK
Dial capture:	INACTIVE
Input 1:	INACTIVE
Input 2:	INACTIVE
Supply voltage:	11.66

- Status of SIM card and the provider name
- Mobile Network signal level (0-100)
- Status of connection to MONITORING STATION 1
- Status of connection to MONITORING STATION 2
- Status of alarm panel dialer (TIP/RING)
- **IN1** input status
- **IN2** input status
- Supply voltage value



5.6 Remote management features

The „gear button” in the header of MODULE STATUS panel opens a dialogue with option to enable and disable the connection to Puloware IoT server.



When the connection is enabled, the device becomes remotely manageable using the web platform of the Puloware server. The public Puloware server is available at www.puloware.com

Create an account on the server, and add the device to it, using the Device ID number. This number is visible when the device is connected to SecurecomConfigurator software.

When a device is assigned to account it's Device ID and the assigned device name is added to Devices list, on the left side of screen. „Online” status of device is shown in this list, with a  sign next to the Device ID. You can select desired device and a screen similar to SecurecomConfigurator will be displayed on the right side, showing valid values of all parameters. (left side of the screen) With this service, you can remotely check the status of device, change settings, see the live and stored events of devices. Also, device firmware can be updated, using the  mark presented after the version number. If there is a next to version, device runs with the latest available version.

Warning: The remote management function generates roughly 6-8Mbyte of traffic per month on the SIM card! Every firmware update generates approximately 1MByte data traffic consumption. Please note the usage data provided!

5.7 Latest Events window

In this field, you can watch all events displayed in text format, as well as the communication and status changes that are not stored, but might be useful.








5.8 Administrative window

This panel contains the most important information about the connected device (type, version, device ID for remote management), as well as the control buttons (icons) for available functions.



- Device type
- Device Firmware version
- Unique device ID This ID is used
- Icons for starting an available function
- Language selector

These functions are available:

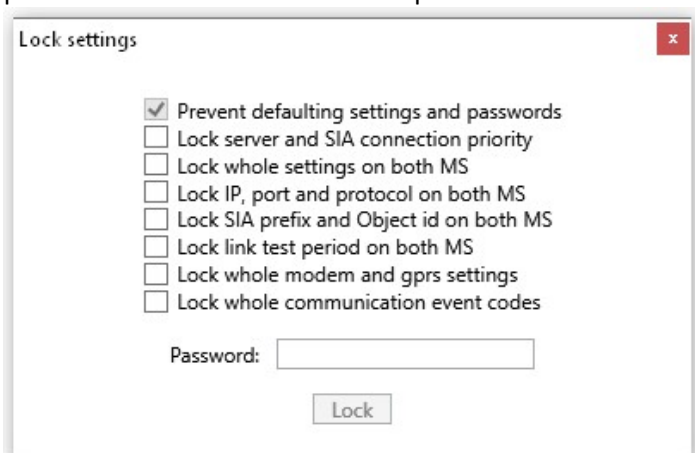
-  Module restart
-  Load saved settings to screen
-  Save current settings to file
-  Download the modified or loaded settings
-  Change device password

Current device password must be also provided to accept the new password. To remove password from device, provide the current password, leave the „new password” field empty and confirm (OK).



Device locking feature

This icon opens a dialog box where you can prevent an unauthorized person from changing the parameters of the device to other parameters.



**WARNING: Unlocking cannot be done remotely, only locally via USB connection!
Use this function very carefully as a device locked with a lost password cannot be unlocked!**

6 Technical data

- Network connection GPRS (2G) GSM850MHz/EGSM900MHz/DCS1800MHz/PCS1900MHz
- Supply voltage: 9 V - 30 V DC
- Rated current 100 mA
- Maximum current 300 mA
- Operating temperature -20°C - +70 °C
- Dimensions 80x45x15 mm

7 Device package content

- SC-GPRS M2 communicator
- Antenna
- Plastic peg spacers
- Warranty