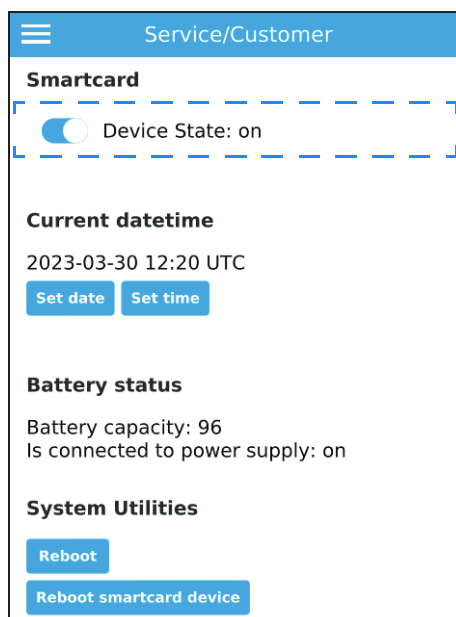


6.2.4.4 Smart Card Reader

The smart card reader can be switched on and off here.

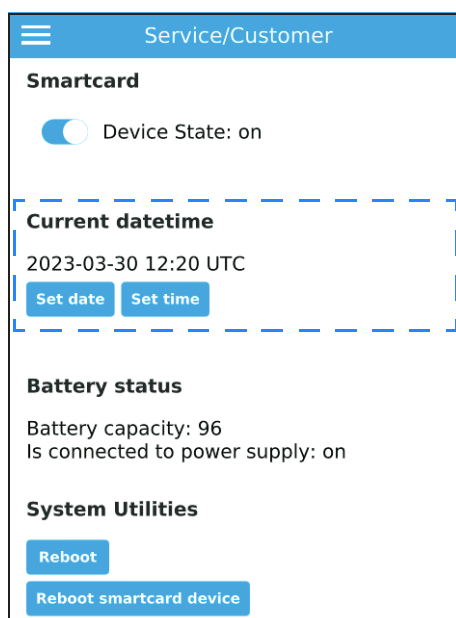


6.2.4.5 Current Time

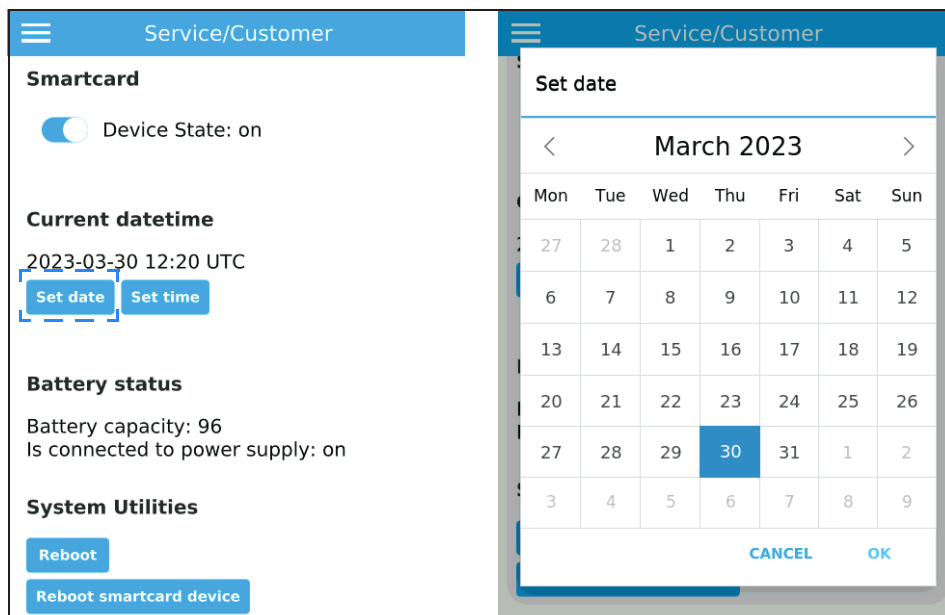
The current date and time are displayed here.

By tapping on the buttons "Set date" and "Set time", these can be changed.

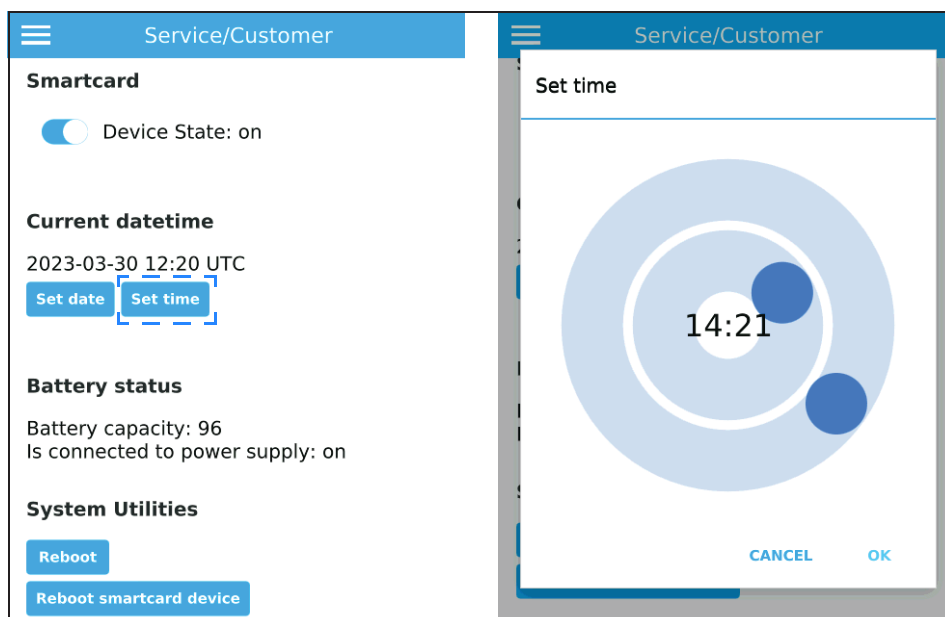
The date and time synchronise automatically when there is a network connection to the server. This overwrites the data that was manually changed here.



To set the date, tap the "Set date" button and select the desired date from the calendar view.

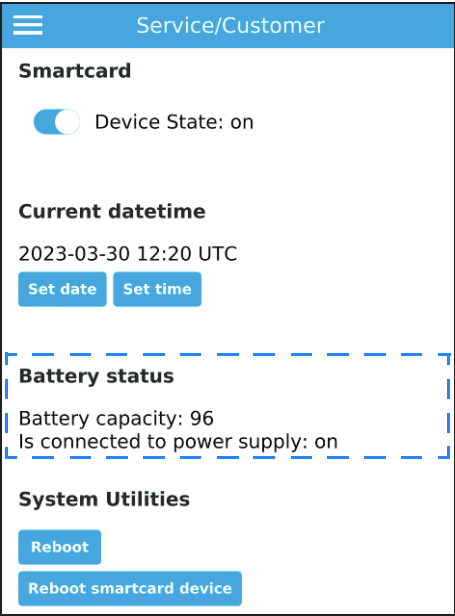


To set the time, tap the "Set time" button and select the desired time on the schematically displayed clock.



6.2.4.6 Battery Status

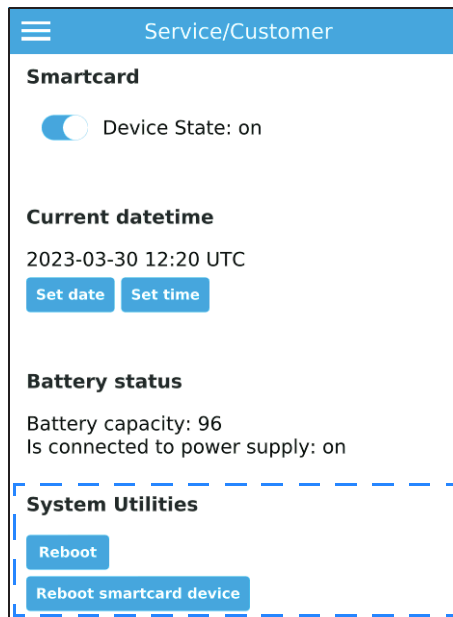
This shows the charge status of the battery and the status of the connection to the power supply.



6.2.4.7 System Utilities

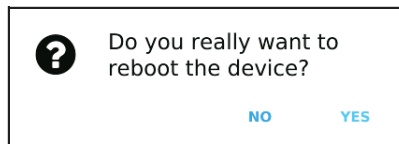
Two reset options are offered here.

- Reboot
- Reboot smart card device



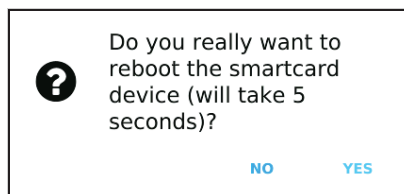
Pressing the "Reboot" button restarts the entire validator.

After pressing the "Reboot" button, the security question must be answered with "Yes" to restart the validator.



By pressing the button "Reboot smartcard device" only the smart card reader is restarted.

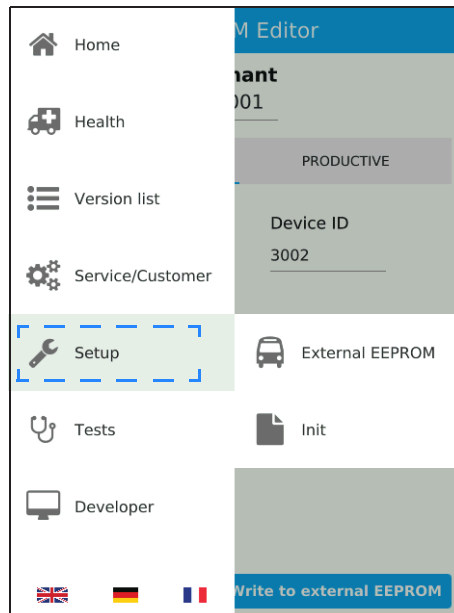
After pressing the "Reboot smartcard device" button, the security question must be answered with "Yes" to restart the smart card reader.



6.2.5 Setup

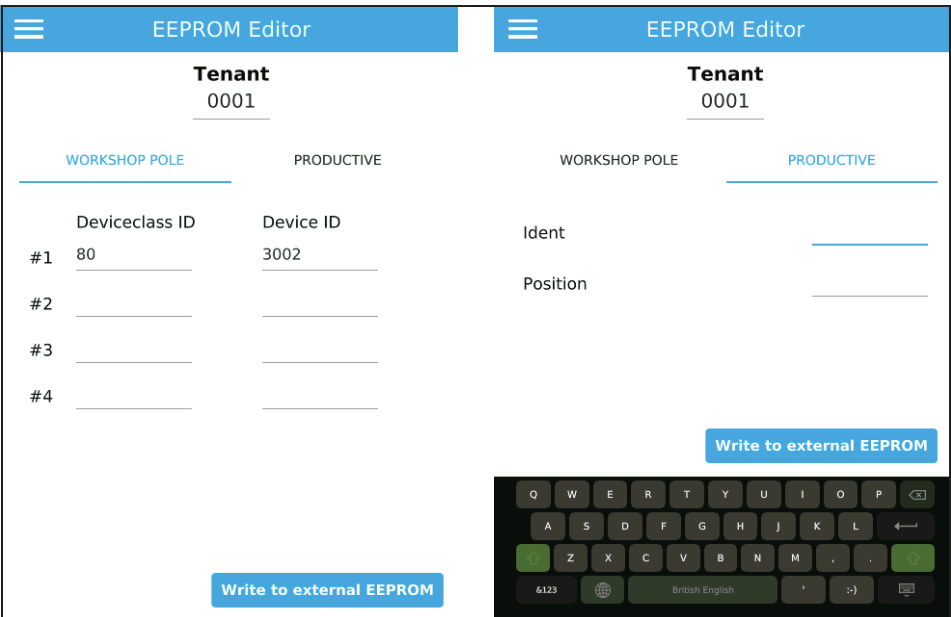
Under the menu item "Configuration" you will find functions for configuring the validator and the workshop and/or vehicle (productive) pole.

- EEPROM Editor (see **Chapter 6.2.5.1**)
- Init (see **Chapter 6.2.5.2**)



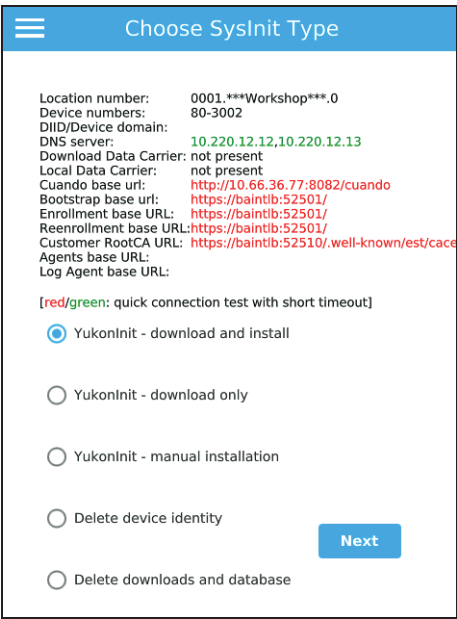
6.2.5.1 EEPROM Editor

This function is described in detail from **Chapter 4.3.1** Only the start screen of this function is shown here.



6.2.5.2 Init

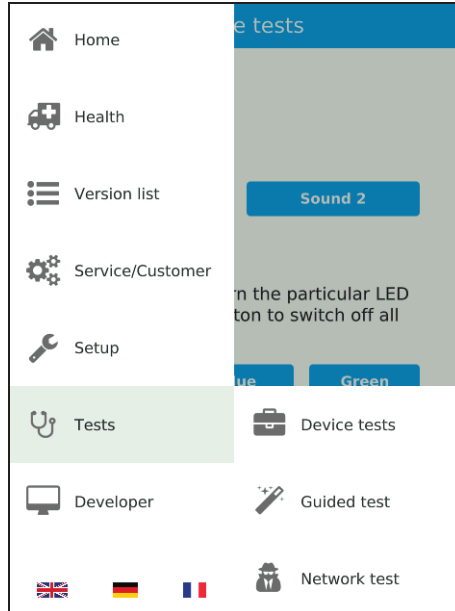
This function is described in detail from **Chapter 4.3.3** onwards. Only the start screen of this function is shown here.



6.2.6 Tests

Various software and hardware tests can be carried out in the "Tests" menu.

- Device tests (see **Chapter 6.2.6.1**)
- Guided test (see **Chapter 6.2.6.2**)
- Network test (see **Chapter 6.2.6.3**)



6.2.6.1 Device Tests

Various tests can be carried out in the “Device Tests” menu. The individual tests are self-explanatory or explained by a short text.

The following tests can be performed: ■ **Sound** ■ **LED's** ■ **Test Image**
 ■ **WLAN band preconfiguration** ■ **Tab simulations** ■ **WLAN-Client**
 ■ **WLAN-Access Point**.

Device tests

Sound

Plays test sounds.

Sound 1

Sound 2

LED's

Press a button to turn the particular LED on. Press the off button to switch off all LED's.

Red

Blue

Green

All Off

Test Image

Show chosen test image until the screen is touched. The image needs to be .png or .jpg and placed in file:///home/sbuser/

Show

WiFi band preconfigurations

Select one of the WiFi preconfigurations

uaputl.base.conf

Apply WiFi conf and reboot

Tap simulations

Simulates a tap signal from BarcodeHandler/SmartcardService

Tap Barcode ('barcode_id'=4711)

Tap smartcard ('uid'=4711)

Wifi Client

☒

Device State: on

For testing provide an access point with SSID='wifi_ssid' and PSK='secret123' before switching on

SSID WiFi client:

IP address wlan0:

MAC address wlan0:

Network WiFi Access Point

☐

Device State: off

SSID accesspoint: ERR:MRVLPRIVCMD is not su
ERR:Command sending failed!

IP address uap0:

MAC address wlan0:

6.2.6.2 Guided Tests

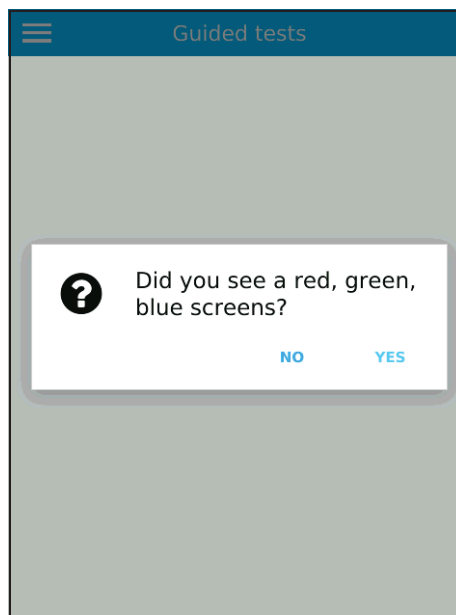
The guided test can be started via the start button or via the test barcode.

Step 1

Tap the start button to begin the guided test. Once the guided test has started, it cannot be interrupted. The test takes about 1 to 3 minutes.



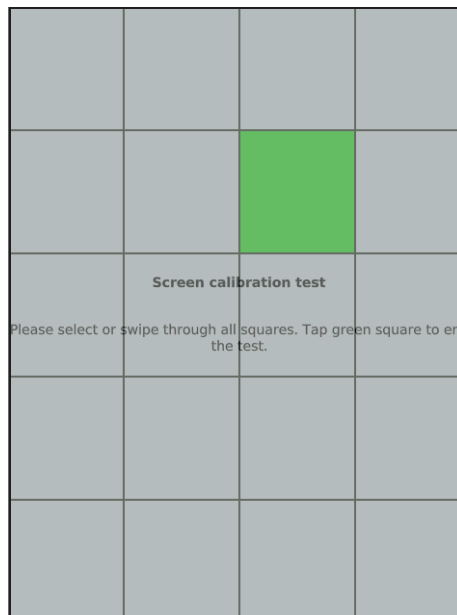
After the start, a red, a green and a blue screen appear one after the other. When you have seen these, confirm this with the "Yes" button.



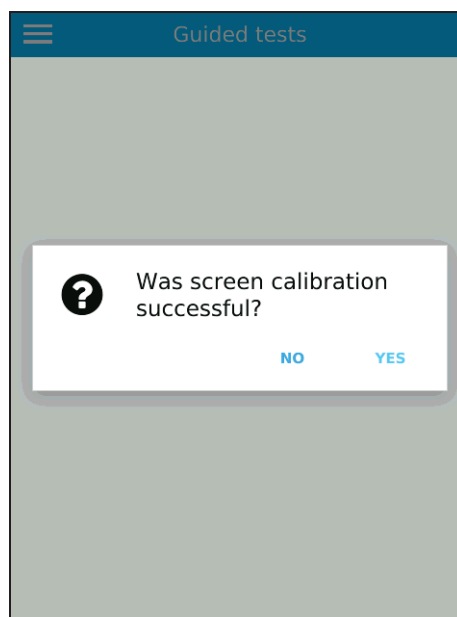
Step 2

Carry out the screen calibration test.

To do this, tap on each gray square on the screen. The color changes from gray to green.

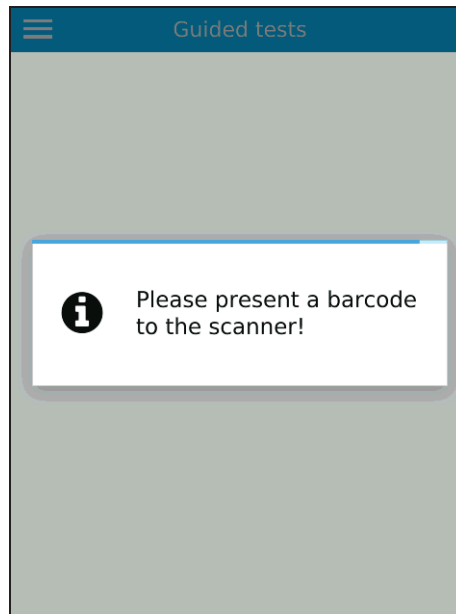


When all squares are green and the touch screen has responded satisfactorily, confirm this with the "Yes" button.



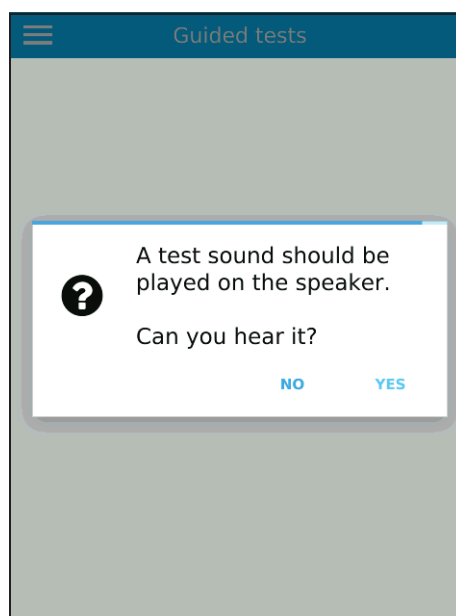
Step 3 Next, a barcode reader test is carried out.

To do this, hold any barcode in front of the barcode reader.



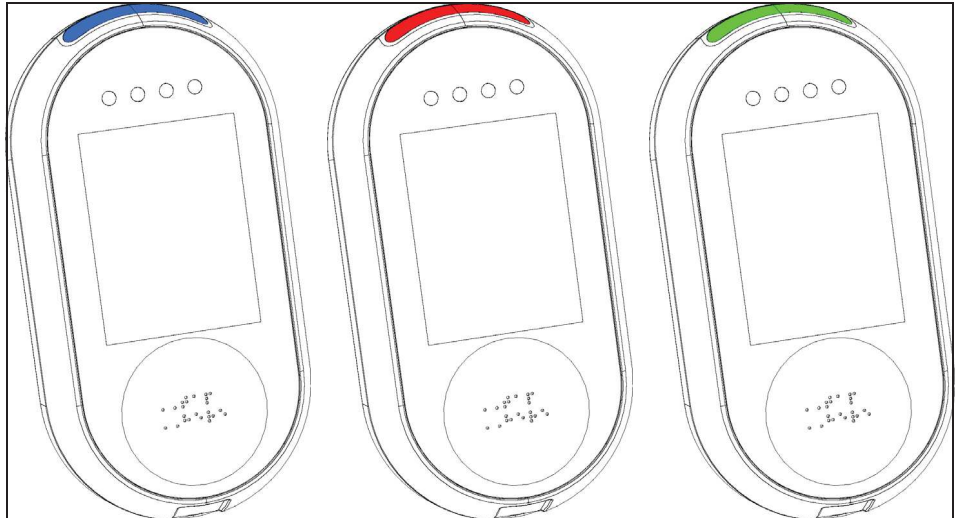
A blue bar above the displayed instruction shows how much time is left for this test before it is skipped.

- Step 4** The loudspeaker plays a signal tone. If this was heard, confirm this with the "Yes" button.



- Step 5** In the following test, the LEDs on the top edge of the validator are tested.

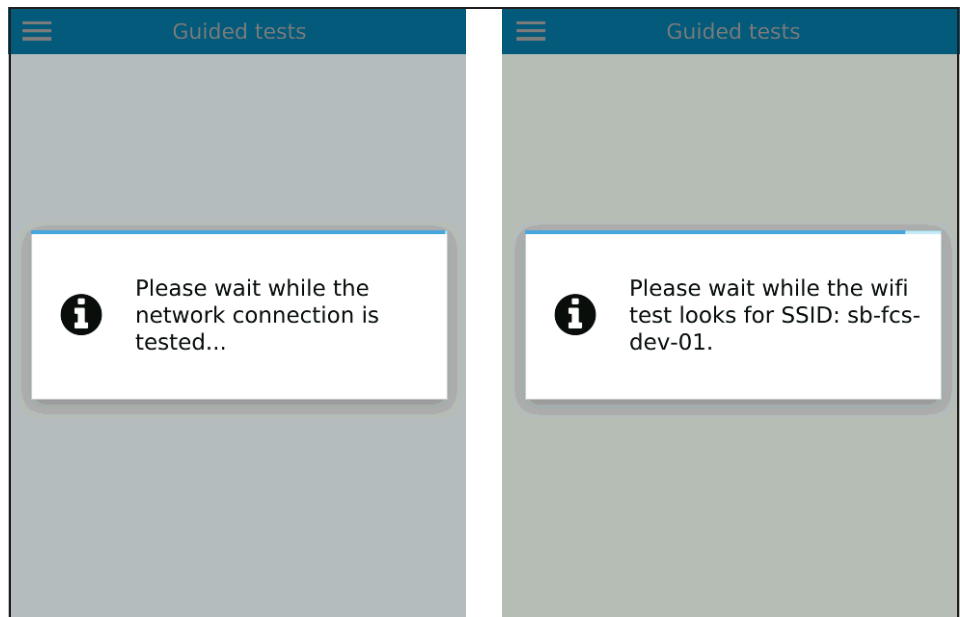
The blue LED, the red LED and the green LED are switched on one after the other.



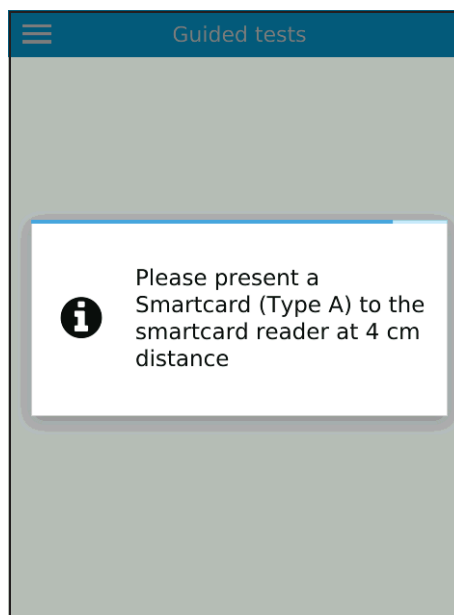
Confirm each individual colour with the "Yes" button when it is visible.



Step 6 Now the network connection is tested automatically. As a user, you have no influence on this test.



Step 7 Next, please have one type A smart card and one type B smart card ready and hold them at the indicated distance in front of the smart card reader when prompted.



Step 8 In the next test, an attempt is made to read SAM places 1 to 4. These reading attempts are carried out automatically.



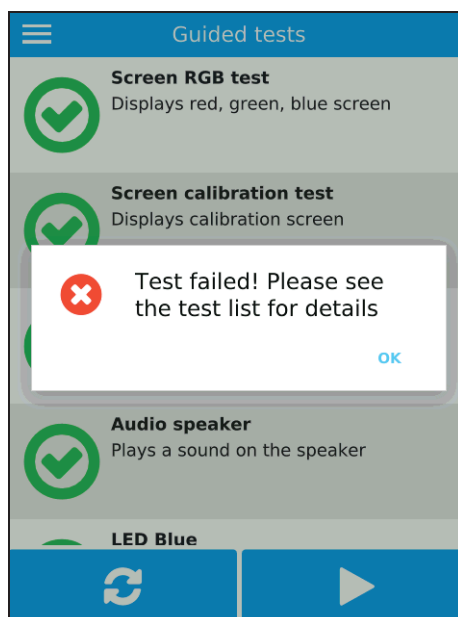
The next tests are carried out automatically and cannot be influenced by the operator.

The next tests are:

- Step 9** Write and read the **Mainboard-EEPROMS**
- Step 10** Write and read the **Pole-EEPROMS**
- Step 11** Check the **primary drive**

At the end of all tests, a listing of the individual test results is displayed.

If any of the tests have not been completed properly, an error message will be displayed.



The list of results can be scrolled through with your finger.

Guided tests


Screen RGB test
 Displays red, green, blue screen


Screen calibration test
 Displays calibration screen


Barcode
 Reads any barcode from the barcode reader


Audio speaker
 Plays a sound on the speaker


LED Blue
 Turns on the blue LED


LED Red
 Turns on the red LED


LED Green
 Turns on the green LED


Networking LAN
 Tries to send an icmp ping to address: 10.56.24.1


Networking Wifi
 Tries to find SSID: sb-fcs-dev-01
Maximum timeout: 30000 ms reached.


Smartcard serial number 021820063
 Check if smartcard serial number is not zero


Smartcard A 0cm
 Read (Type A) card at 0 cm distance


Smartcard A 4cm
 Read (Type A) card at 4 cm distance


Smartcard B 0cm
 Read (Type B) card at 0 cm distance


Smartcard B 4cm
 Read (Type B) card at 4 cm distance


SAM slot 1
 Checks communication with an arbitrary SAM in slot 1
SAM Communication failed.


SAM slot 2
 Checks communication with an arbitrary SAM in slot 2
SAM Communication failed.


SAM slot 3
 Checks communication with an arbitrary SAM in slot 3
SAM Communication failed.


SAM slot 4
 Checks communication with an arbitrary SAM in slot 4
SAM Communication failed.


Eeprom Board
 Checks correct writing and reading bytes of the main board EEPROM


Eeprom Pole
 Checks correct writing and reading bytes of the pole EEPROM


Main disk drive
 Checks main drive free capacity and health parameters


Backup disk drive
 Checks backup drive free capacity and health parameters

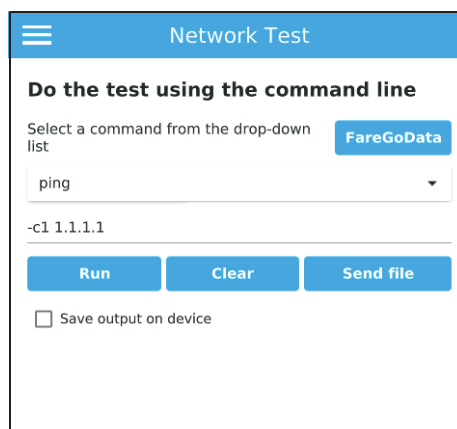

Eeprom read
 Checks correct reading bytes of the pole EEPROM




6.2.6.3 Network Tests

The following functions are available in the "Network Tests" area:

1. FareGo Data - Connection test (see Point 1.)
2. Command line commands for the network test (see Point 2.)

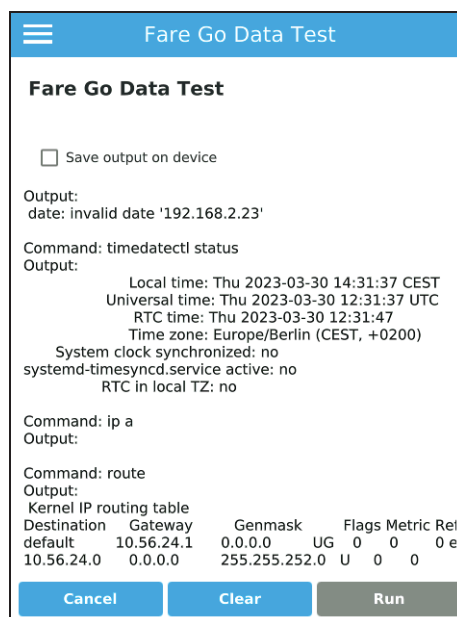


1. Test FareGo Data connection:

Step 1 Tap the <FareGo Data> button.

Step 2 If the output is to be saved on the device, activate the option "Save output on device" and enter a file name for saving.

Step 3 Start the test with the <Run> button.



The test runs automatically and is logged on the screen. Error messages may appear in red letters.

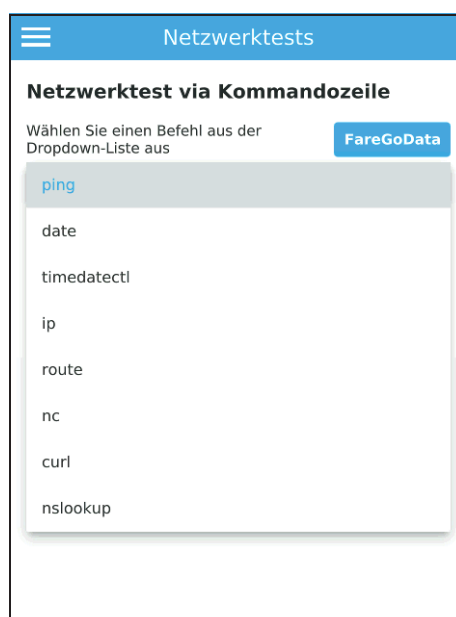
With <Cancel> you can end a running test prematurely. With <Clear> remove the test protocol from the display.

2. Execute command line commands:

The following commands are available:

- ping (Check a network connection via IP-Address)
- date (Change the system date)
- timedatectl (Control the date, time and timezone)
- ip
- route (Change the network routing table)
- nc
- curl (Get or send data using URL syntax)
- nslookup (Finding IP addresses/domains of a specific computer using DNS)

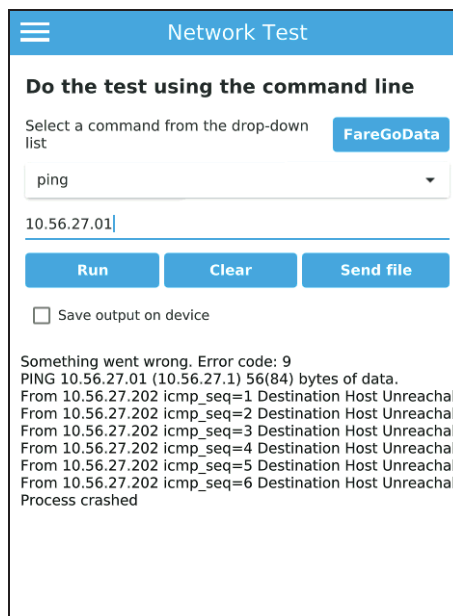
Step 1 Select the desired command from the drop-down list.



Step 2 Enter the associated parameters in the line below the selection field. When you tap the line, the screen displays a keyboard for input.

Step 3 If the output is to be saved on the device, activate the option "Save output on device" and enter a file name for saving.

Step 4 Tap <Execute>.

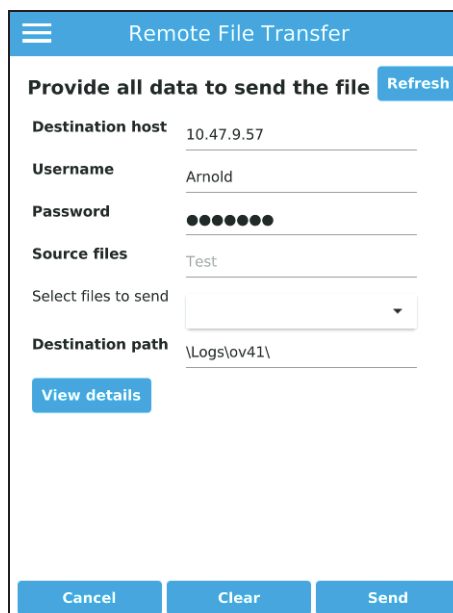


With <Stop> you can cancel the execution if necessary, with <Clear> you can remove the data output from the screen.

3. Send files to a destination host:

Step 1

Tap the <Send file> button.



Step 2 Enter the destination host and access data.

Step 3 Select the files to be sent from the drop-down list.

Step 4 Indicate the storage path under "Destination path".

Step 5 Use the "View details" button to show detailed information about the data output. Close the info window with "OK".

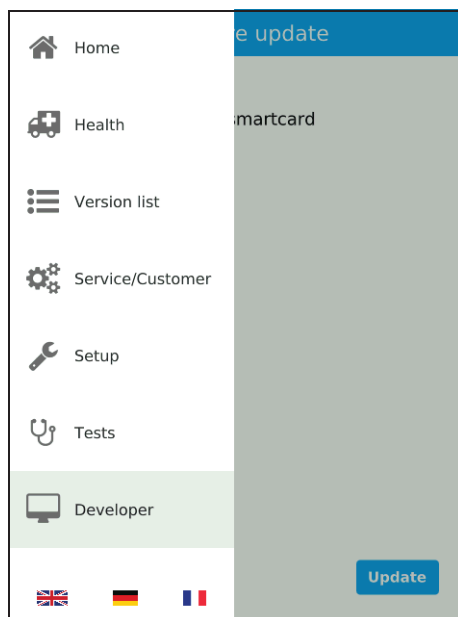
Step 6 Tap the "Send" button.

With <Clear> you can delete all entries in the window if necessary, with <Cancel> cancel the function.

6.2.7 Developer

The following functions are available in the "Developer" area:

- SCR Update (see **Chapter 6.2.7.1**)
- Settings (see **Chapter 6.2.7.2**)

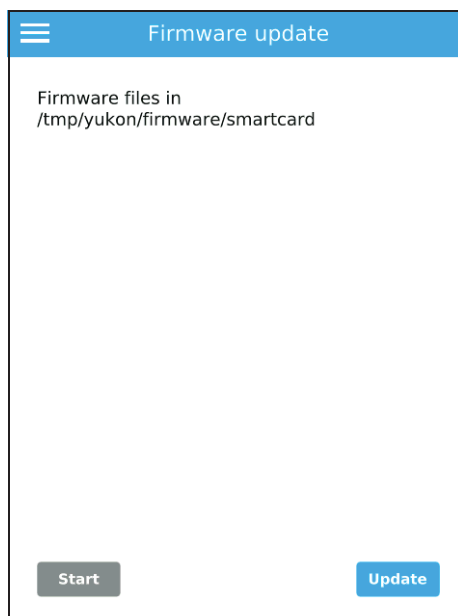


6.2.7.1 SCR Update

This function updates the firmware of the smart card reader.

Step 1

Tap the <SCR Update> button in the "Developer" area.



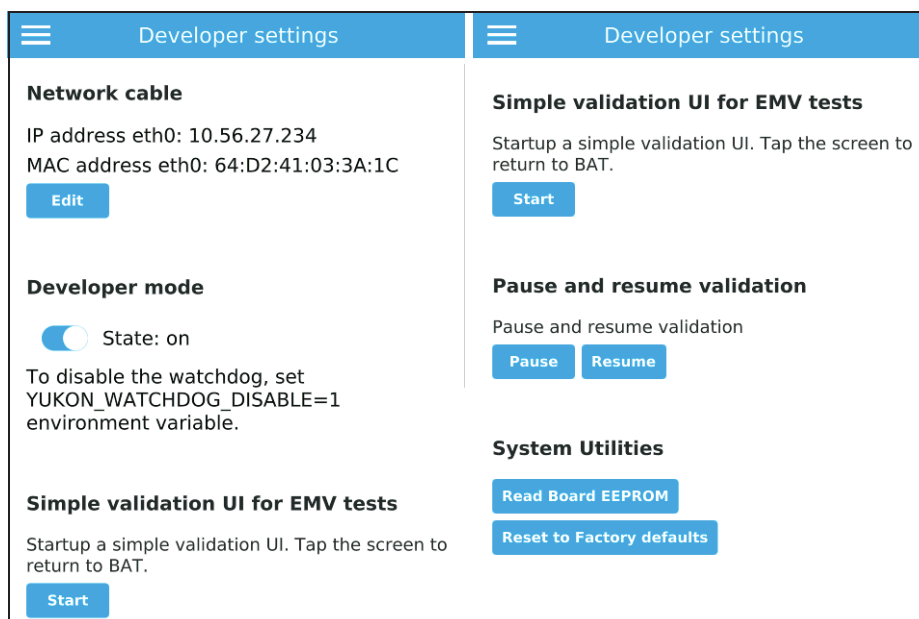
Step 2

Start the update by tapping the <Update> button.

6.2.7.2 Developer Settings

Under “Developer settings” you can make the following developer settings:

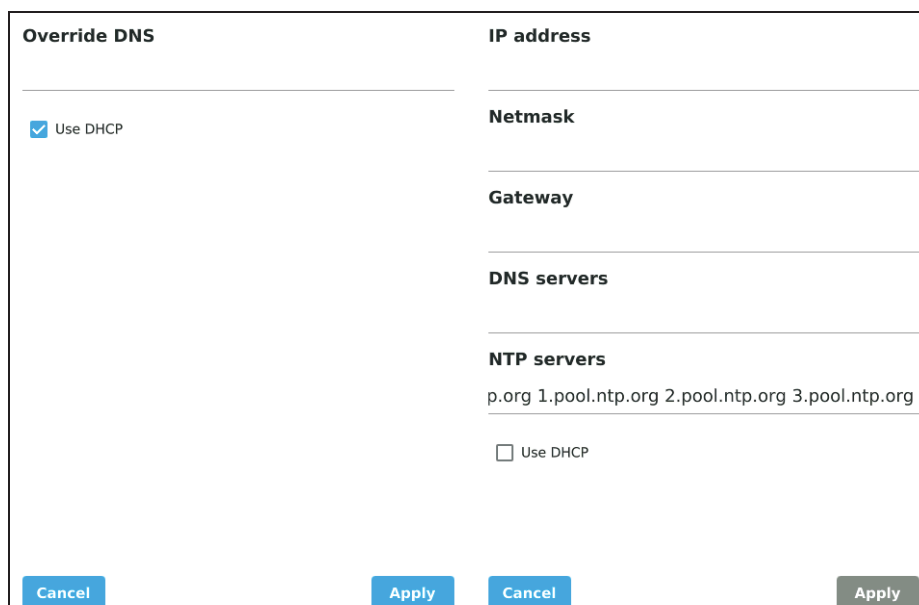
1. View and edit network information (see Point 1.)
2. Switch developer mode on or off (see Point 2.)
3. Validation UI for EMC tests (see Point 3.)
4. Pause and continue validation (see Point 4.)
5. Read out the EEPROM of the unit (System Utilises) (see Point 5.)
6. Reset to Factory defaults (System Utilises) (see Point 6.)



The screenshot shows the 'Developer settings' menu. It is divided into two columns. The left column contains: 'Network cable' with IP and MAC addresses and an 'Edit' button; 'Developer mode' with a toggle switch set to 'on' and a description about disabling the watchdog; 'Simple validation UI for EMV tests' with a 'Start' button. The right column contains: 'Simple validation UI for EMV tests' with a 'Start' button; 'Pause and resume validation' with 'Pause' and 'Resume' buttons; and 'System Utilities' with 'Read Board EEPROM' and 'Reset to Factory defaults' buttons.

1. Network information

In this area you can see the IP address and the MAC address of the Ethernet interface. You can make changes via the <Edit> button.



The screenshot shows a network configuration dialog. It has two main sections: 'Override DNS' on the left and 'IP address' on the right. The 'Override DNS' section has a 'Use DHCP' checkbox which is checked. The 'IP address' section has fields for 'IP address', 'Netmask', 'Gateway', 'DNS servers', and 'NTP servers'. The 'NTP servers' field contains the text 'p.org 1.pool.ntp.org 2.pool.ntp.org 3.pool.ntp.org'. At the bottom, there are 'Cancel' and 'Apply' buttons on both sides.

In the default setting, "Use DHCP" is activated. If deactivated, the following network information can be recorded manually:

- IP Adresse
- Netmask
- Gateway
- DNS server
- NTP server

2. Switch developer mode on or off

Developer mode allows SSH access to the unit.

Before initialisation, the developer mode must be switched on.

You can switch the developer mode on or off in the developer settings. Before switching over, a confirmation prompt is displayed.

To the Watchdog to deactivate must the environment variable YUKON_WATCHDOG_DISABLE=1 must be set.

3. Validation UI for EMC tests

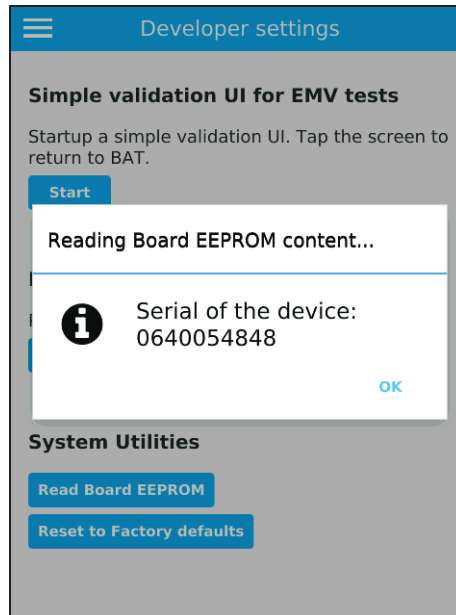
Use the <Start> button to open a simple validation environment for EMC tests. The screen shows the detection of EMV cards in colour. To return to the BAT, tap the screen.

4. Pause and resume validation

With the <Pause> button you switch the barcode reader and the smart card reader inactive so that the validation pauses. With <Resume> you switch the barcode reader and smart card reader active again.

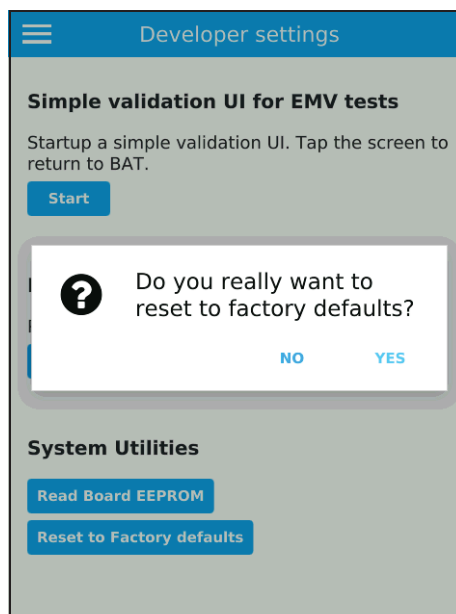
5. Read out the EEPROM of the unit

Use the <read out the unit's EEPROM> button to display the serial number stored on the EEPROM.



6. Restore factory settings

Use the <Restore factory settings> button to reset the unit to factory settings. Before resetting, a confirmation prompt is displayed.



Chapter 7 Revenue Services

- 7.1 This chapter is
not required for
this device type

Chapter 8 Preventive Maintenance

8.1 General Maintenance and Cleaning

The following general preventive maintenance schedules and cross references are for the overall maintenance and cleaning of the FareGo Val OV|41. The schedules should be followed by the customer. Cross references direct the customer to the procedures for specific items, including testing and validating the equipment to ensure proper operation.

Chapter 4, General Description, identifies the locations of the modules discussed in this chapter.

Maintenance on validator equipment subject to outdoor environmental conditions should be performed **ONLY** if the following conditions are met:

- Temperature of the validator does not fall below -30 °C (-22 °F).
- Humidity must be between 5 % and 95 %, non-condensing.
- Rain and snow ingress during maintenance must be prevented.

These restrictions are necessary because exposure to severe environmental conditions such as cold temperatures, rain, snow, and wind, can cause serious and permanent damage to the equipment. PCBs (Printed Circuit Board) may malfunction and cease operation at temperatures below -30 °C (-22 °F). Exposure to rain or snow may lead to short circuits and resulting equipment damage.

Failure to follow these guidelines can lead to damages that will not be covered under the warranty.

From a technical point of view, no Preventive Maintenance activities are needed for the Validators to ensure their functionality and availability.

S&B recommends that the customer inspects the Validators visually at regular intervals in order to detect defects and vandalism damages as soon as possible. This inspection should also focus on optical disturbance factors that limit the device functionality, e.g. graffiti on the Patron Display.

For the best possible user experience, S&B recommends to clean the devices in regular intervals. These intervals depend on the operating environment of the Validators and may need to be adapted if the devices are subject to heavy use or extreme environmental conditions, such as air pollution, dust, or other environmental factors, such as a construction work or high traffic density. For more details on the cleaning procedure, please refer to the corresponding S&B Service Manual of the Validator.

S&B Smart Card Reader - Safety instruction

With every service activity it needs to be checked:

- ✓ The validator housing does not have signs of tampering, opening by force, physical damage etc.
- ✓ The validator identification (serial number) is correct and matches company records. In other words it needs to be checked if the validator number XXXXXXXX is supposed to be installed in bus number YYYYYYYY.
- ✓ There are no unauthorized devices connected to the validator, especially around the landing plane of S&B Smart Card Reader antenna. Please note that such devices can be well hidden, so their presence might only be indicated by i.e. increased thickness of some parts.
- ✓ There are no extra wires or devices soldered or connected to the S&B Smart Card Reader.

Annually it needs to be checked:

- ✓ The S&B Smart Card Reader Version 3 identification (serial number) is correct and matches company records – is the S&B Smart Card Reader number ZZZZZZZZ supposed to be installed in validator number XXXXXXXX.
- ✓ The SAM card identification (serial number) is correct and matches company records – is the SAM reader number AAAAAAAA supposed to be installed in reader number ZZZZZZZZ?

For more information see “SBSCRx_SecurityGuidance_LifeCycle” document.

8.2 Initial Check

Complete the following checklist before turning on the validator:

- ✓ Verify that all screws have been tightened firmly.
- ✓ Ensure that the equipment is properly grounded.
- ✓ Ensure that power supply is installed and is working correctly.
- ✓ Check the state of the fuses (power supply side).
- ✓ Verify that all wires are firmly connected.
- ✓ Verify that you have not forgotten anything inside the validator Mounting Unit.
- ✓ Remove any foreign body from the inside of the validator (scraps, etc.), and clean.

8.2.1 Power On the Validator

When the power supply (Power Box or Power Switch Box) receives an ignition signal, the validators are supplied with voltage.

The base unit can be removed from the mounting unit under voltage. (Hot swapping).

As soon as the base unit is disconnected from the power supply, the base unit shuts down under controlled conditions.

8.2.2 Returning the Validator to Service

As soon as the base unit is connected to the power supply, the base unit goes automatically in service.

8.3 Maintenance Overviews

This table gives a quick overview of the general maintenance and cleaning cycles. This table complements **Table 8-1**, which provides a summary of the Preventive Maintenance schedule.

General Maintenance and cleaning	1 MONTH	3 MONTHS	6 MONTHS	12 MONTHS	AS NEEDED
Cleaning and Visual Inspection of the Exterior	X				X

Table 8-1 General Maintenance and Cleaning

When the recommended preventive maintenance intervals have both a time period and a receipt usage maximum, then preventive maintenance must take place when either the time or the usage maximum is reached. These are maximum maintenance intervals, which may have to be reduced, and they assume average usage in a moderate environment. If certain devices are heavily used or exposed to atypical environmental conditions, such as extreme temperature fluctuations or nearby construction work, then preventive maintenance must be undertaken more frequently in order to reduce the amount and frequency of field maintenance. Operation and maintenance histories should be consulted and preventive maintenance procedures undertaken for those devices and locations where experience shows more frequent preventive maintenance will reduce field maintenance.

8.3.1 Materials

Table 8-2 provides a complete list of the materials required to perform exterior cleaning. Please note the manufacturer's safety instructions on the products.

ITEM	PART NUMBER/ Description	WHERE USED
Heavy Duty Shop Cloths	Lint-free, soft	Miscellaneous Use
Katun Foam Cleaner	Aerosol Cleaner for plastic, glass, and metal	Plastic, glass, and non -stainless steel metal

Table 8-2 Cleaning Materials

For routine maintenance, follow these steps. For recommended cycles see **Table 8-1**, but some validator may need to be cleaned "as needed."

Step 1 Using Katun Foam Cleaner, clean the plastic and glass of the validator. Do not use the Katun Foam Cleaner on the stainless steel surfaces.

Chapter 9 Troubleshooting

9.1 Overview

This chapter provides information about FareGo Val OV|41 error and failure identification. The first indication of a problem is usually a message displayed on the LCD screen. Responding to an error involves identifying the nature of the error and taking appropriate action to finish the transaction. Responding to a failure involves identifying the nature of the failure and taking appropriate action to restore the FareGo Val OV|41 to service. When service cannot be restored, the module needs to be replaced with an operational one.

Maintenance on validator equipment subject to outdoor environmental conditions should be performed ONLY if the following conditions are met:

- Temperature of the validator does not fall below -30 °C (-22 °F).
- Humidity must be between 5 % and 95 %, non-condensing.
- Rain and snow ingress during maintenance must be prevented.

These restrictions are necessary because exposure to severe environmental conditions such as cold temperatures, rain, snow, and wind, can cause serious and permanent damage to the equipment. PCBs (Printed Circuit Board) may malfunction and cease operation at temperatures below -30 °C (-22 °F). Exposure to rain or snow may lead to short circuits and resulting equipment damage. Failure to follow these guidelines can lead to damages that will not be covered under the warranty.

To reiterate what is said in the preceding paragraph, a maintenance technician should troubleshoot FareGo Val OV|41 errors by:

- Making sure the FareGo Val OV|41 can power on.
- Making sure the correct software versions are on the FareGo Val OV|41.

9.2 Verifying Software Versions

When troubleshooting, a maintenance technician should compare the software versions of the device with the expected versions. If the versions are different, the technician should ask the backend system operator to confirm that the current software versions are linked to the device. If this is the case, the device software can be updated via the backend system's maintenance of jobs.

9.3 Error Messages on Patron Display

The presentation of error messages in this chapter is exemplary. The error messages displayed on your device may look slightly different.

9.3.1 Out of Service

Shown in **Figure 9-1**, the 'Out of Service' screen is displayed when the FareGo Val OV|41 is in 'Out of Service' mode. The device will not read or write to any Farecards.



Figure 9-1 Out of Service' Screen

When a critical alarm is detected, the FareGo Val OV|41 switches to Out-of-Service mode. Possible causes include:

- MicroSD card access failure
- Card reader failure
- No currently active business configuration data or other software versions

The solution is to remove and replace the FareGo Val OV|41. If the failure persists, contacting the Helpdesk is the appropriate action.

9.4 Error Identification

When an error occurs, an indication of the error appears **on the LCD**. This is the first place to look for messages such as **Already Tapped** (see **Figure 9-2**). Errors interrupt one type of fare transaction.

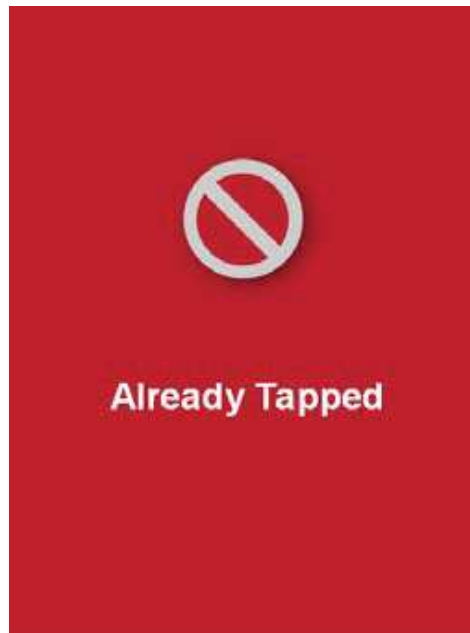


Figure 9-2 Already Tapped

9.4.1 Cash Supplement Required

A cardholder may invoke the screen shown in **Figure 9-3** if a farecard/stored value card with a period pass or a transfer product is tapped and cash supplement is required.

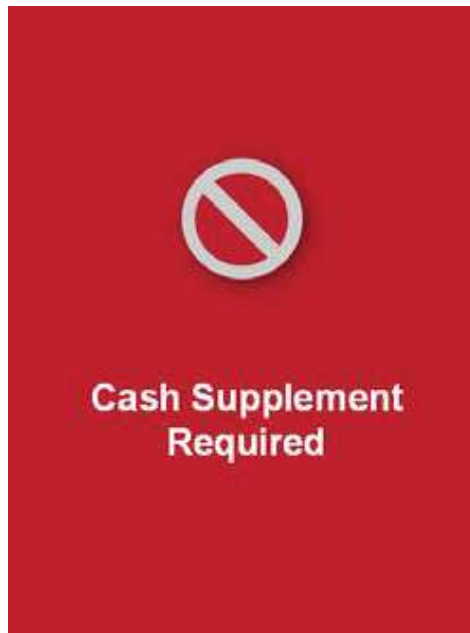


Figure 9-3 Cash Supplement

9.4.2 Cash Fare Required

When a cardholder taps a stored value card with an expired Transfer product and no Period Pass product, the screen in **Figure 9-4** appears.

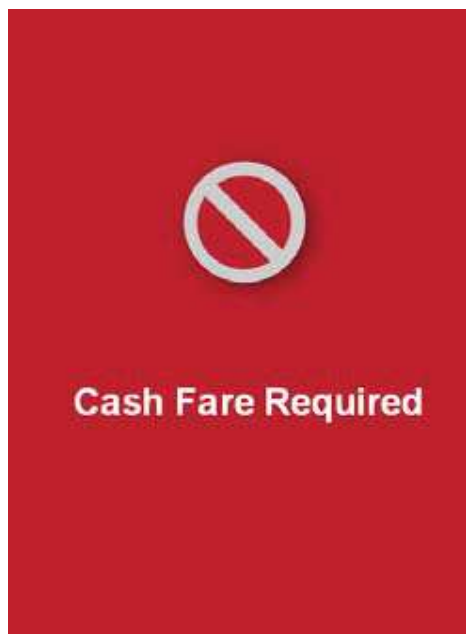


Figure 9-4 Cash Fare Required

9.4.3 Not Enough Funds, Reload Required

There are three circumstances when a cardholder may invoke the screen shown in **Figure 9-5**. These are:

- Tapping a registered Farecard with a negative e-Purse,
- Tapping an anonymous Farecard with a zero e-Purse,
- Tapping an anonymous Farecard with a positive e-Purse that is less than the fare.



Figure 9-5 Funds Lacking

9.4.4 Card Read Error A card read error will cause the screen shown in **Figure 9-6** to appear.

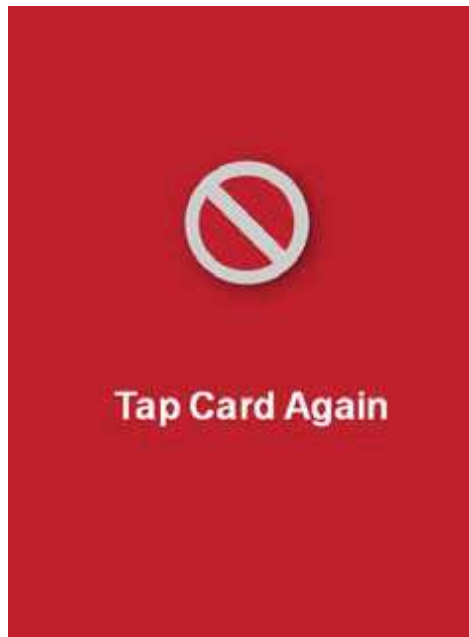


Figure 9-6 Farecard Read Error

9.5 Failure Identification

When a failure occurs, an indication of the failure appears on the LCD. This is the first place to look for messages such as **Blocked Card**.

9.5.1 Blocked Card

A failure occurs when a Farecard tap on fails. The issue may be one of the following:

- Blocked Farecard,
- A Farecard that has not been activated, or
- A card read/write error.

When a cardholder taps a blocked card or a hot listed farecard or stored value card on the FareGo Val OV|41, the screen in **Figure 9-7** appears.

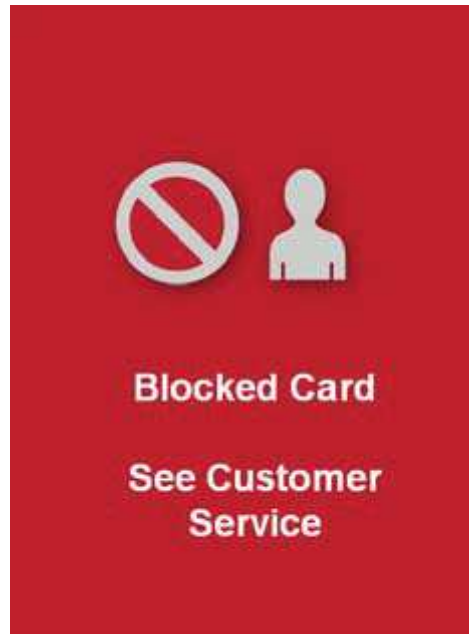


Figure 9-7 Blocked Card

9.5.2 Card Inactive

When a cardholder taps a not activated Farecard on the FareGo Val OV|41, the screen shown in **Figure 9-8** appears.



Figure 9-8 Card Inactive

9.5.3 Card Error

When a cardholder taps an invalid Farecard, the screen in **Figure 9-9** appears.

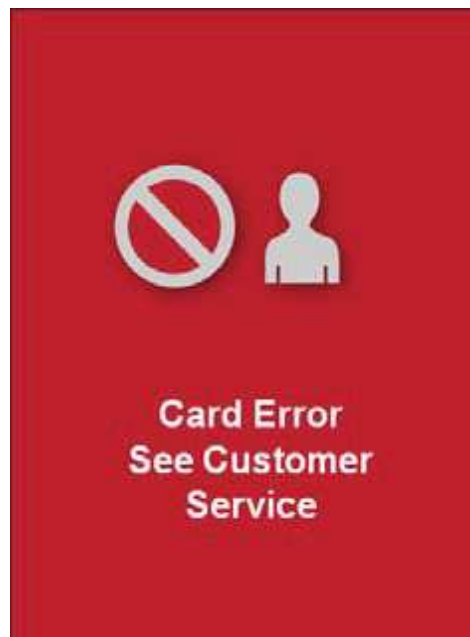


Figure 9-9 Card Error

9.5.4 Reversal Not Possible

When a cardholder tries to reverse a fare payment via the FareGo Val OV|41 where fare reversal is not processed, the screen in **Figure 9-10** appears.

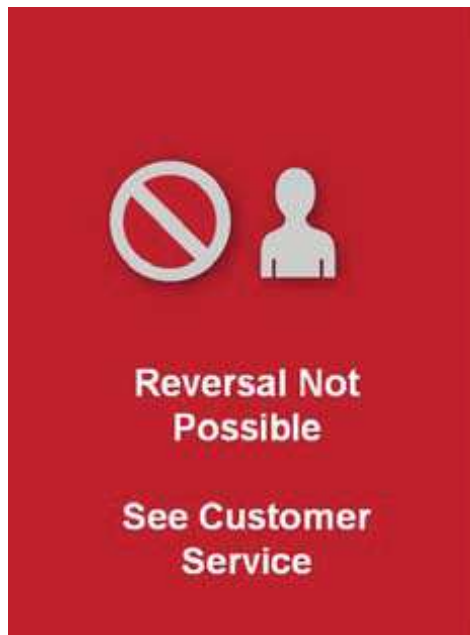


Figure 9-10 Reversal Error

9.6 Module Removal This section discusses how to remove and replace components.

Turn off power at the main facility breaker before proceeding.

As soon as the power supply of the device is stopped, it saves the open files and automatically switches off, according to the built in switch off logic.

9.6.1 Tools and Consumables

Device or Component Name	Part Number
OV 41 Base Unit (incl. Mounting Unit)	00349630
OV 41 Mounting Unit (Wall Mounting)	81 327030
Lock	81 325140
Key	81 325150
System MicroSD Card (including base image)	07 347840
Backup MicroSD Card	51 812770

Table 9-1 Part Numbers

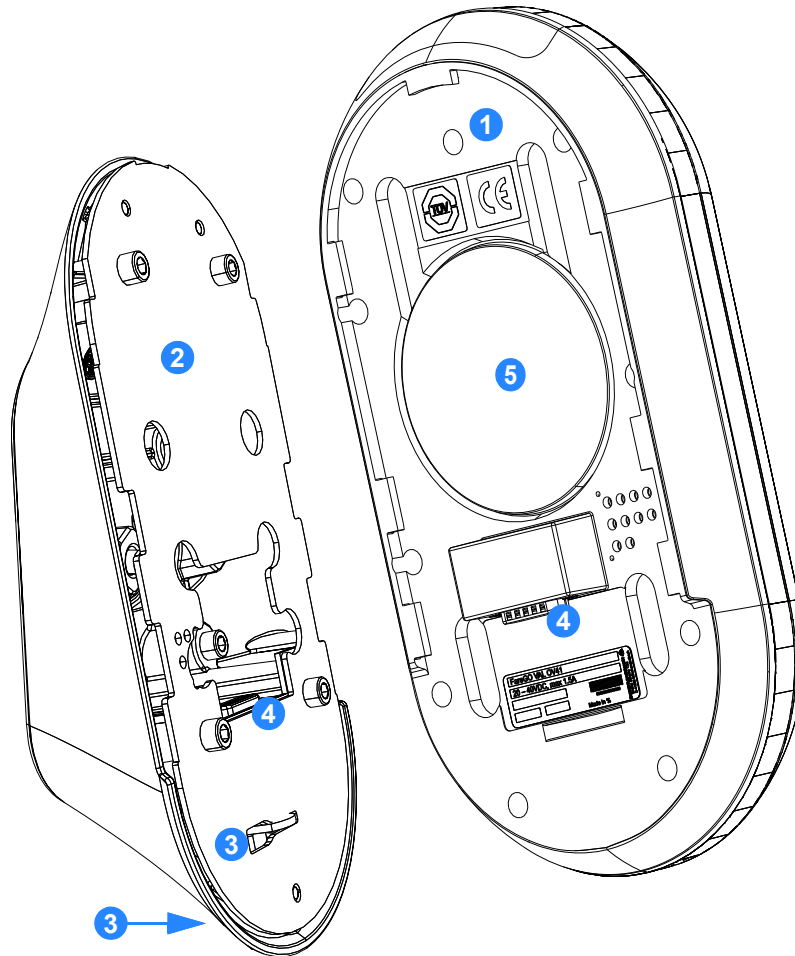
9.6.2 Base Unit Removal

The drawing in **Figure 9-11** illustrates how to unlock the FareGo Val OV|41 Base Unit and remove it for field replacement.

Step 1 Use the key to unlock the device.

Step 2 Push the base unit upward so that the FareGo Val OV|41 can be taken away from the mounting unit.

At no time should the service provider open the device to troubleshoot, repair, or replace FareGo Val OV|41 components in the field.

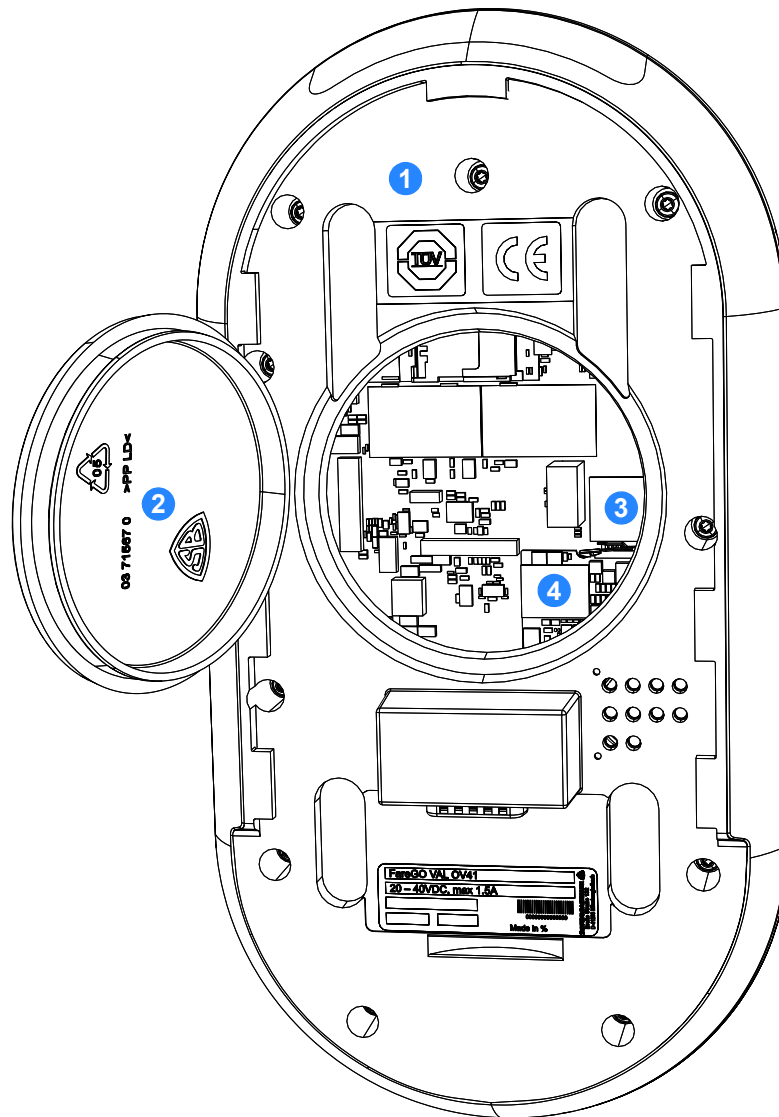


- 1 Base Unit
- 2 Mounting Unit
- 3 Key/Lock
- 4 Connector
- 5 Service Cover

Figure 9-11 Module Removal - Base Unit (Example: Wall Installation)

As a backup to the online data transmission, a second, pre-configured MicroSD card may be inserted into the FareGo Val OV|41 (different from the backup module MicroSD card). This second, pre-configured card may be used if the FareGo Val OV|41 is not online or cannot connect to the back end. Transaction data is also stored in the non-volatile system memory (flash memory).

- Step 3** Open the service cover.
- Step 4** Remove the Backup microSD card as shown in **Figure 9-12**.
- Step 5** Insert the microSD card in the replacement FareGo Val OV|41.
- Step 6** Set the base unit on the mounting unit and push it down.
- Step 7** Lock the base unit by turning the key shown in **Figure 9-11**.



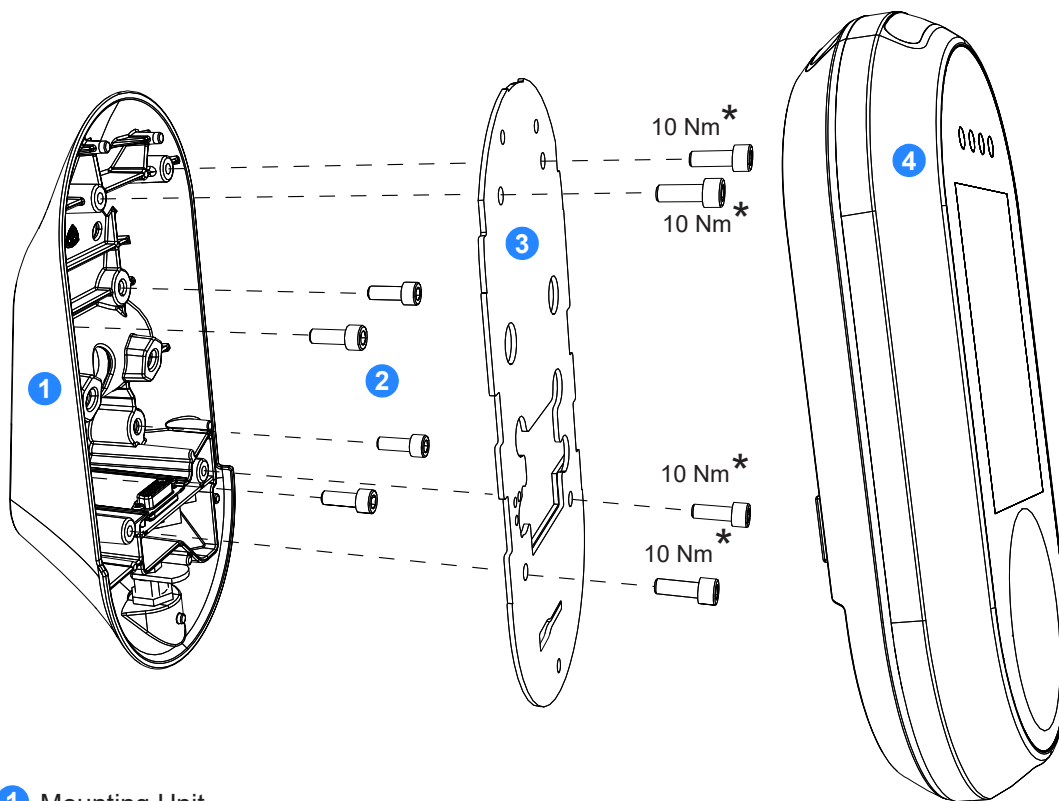
- 1 Base Unit
- 2 Service Cover
- 3 Backup MicroSD Card
- 4 CPU Module MicroSD Card

Figure 9-12 Service Cover - open

9.6.3 Mounting Unit Removal

The drawing in **Figure 9-13** illustrates how remove the FareGo Val OV|41 mounting unit from the assembly site (fastening elements on the wall side are not shown). For removal from a pole see **Figure 9-14** and **Figure 9-15**.

- Step 1** Remove the base unit from the mounting unit as described in **Section 9.6.2** (step 1 and 2).
- Step 2** Cut the cable tie and remove the power/network cable as shown in **Figure 9-16**.
- Step 3** Remove the four screws which fix the mounting plate to the mounting unit front part and remove the mounting plate.
- Step 4** Remove the four screws which fix the mounting unit rear part to the mounting unit front part and remove the mounting unit parts from the mounting bar.
Be careful when removing the mounting unit front part. When you push the Front part up or down you can damage the Power/network cable.



- 1 Mounting Unit
- 2 Screws for Wall Mounting, not included in Scope of Delivery
(Secure Fastening is the Responsibility of the Operator)
- 3 Mounting Plate
- 4 Base Unit

* Secure with Loctite 243

Figure 9-13 Module Removal - Mounting Unit (Wall Installation)

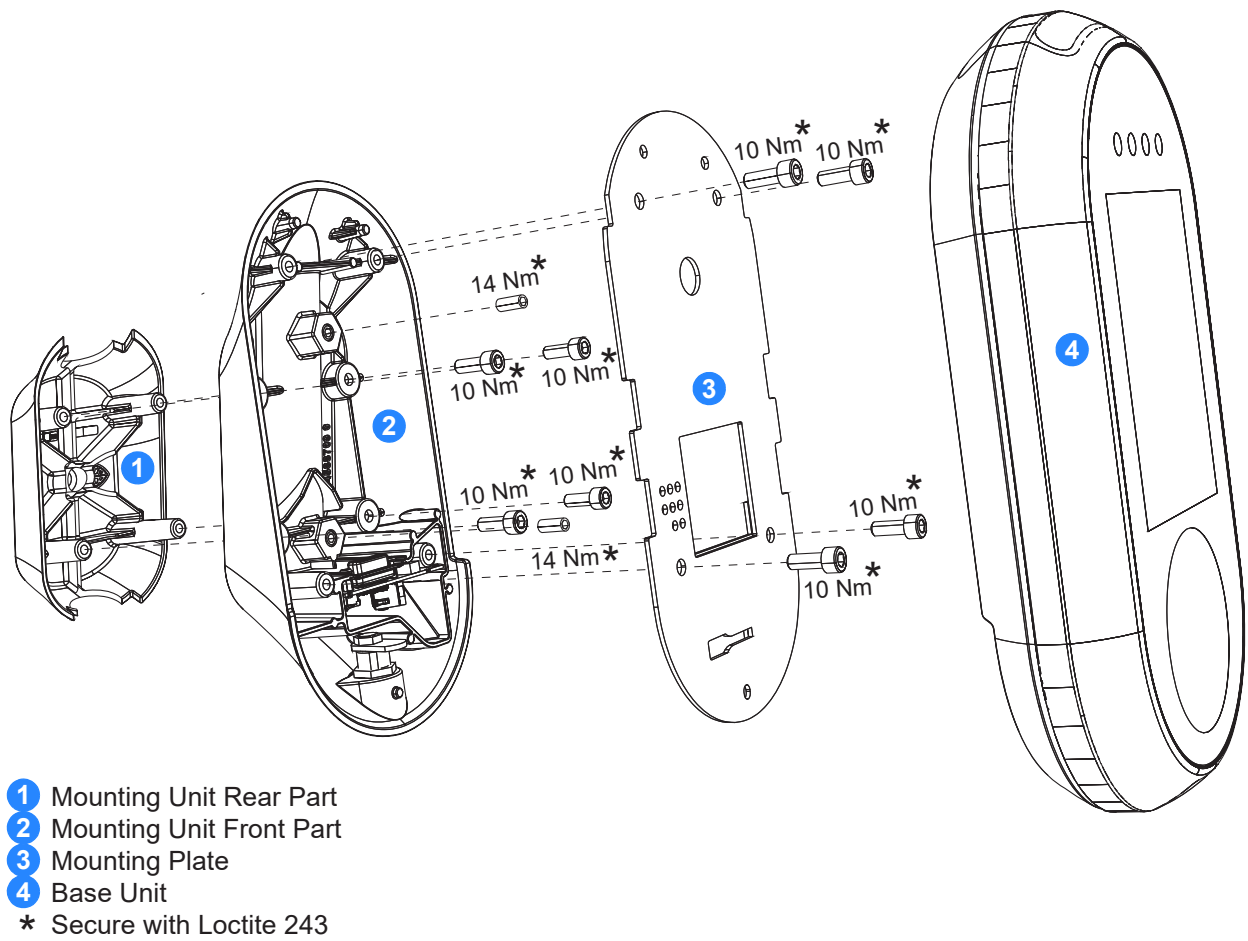
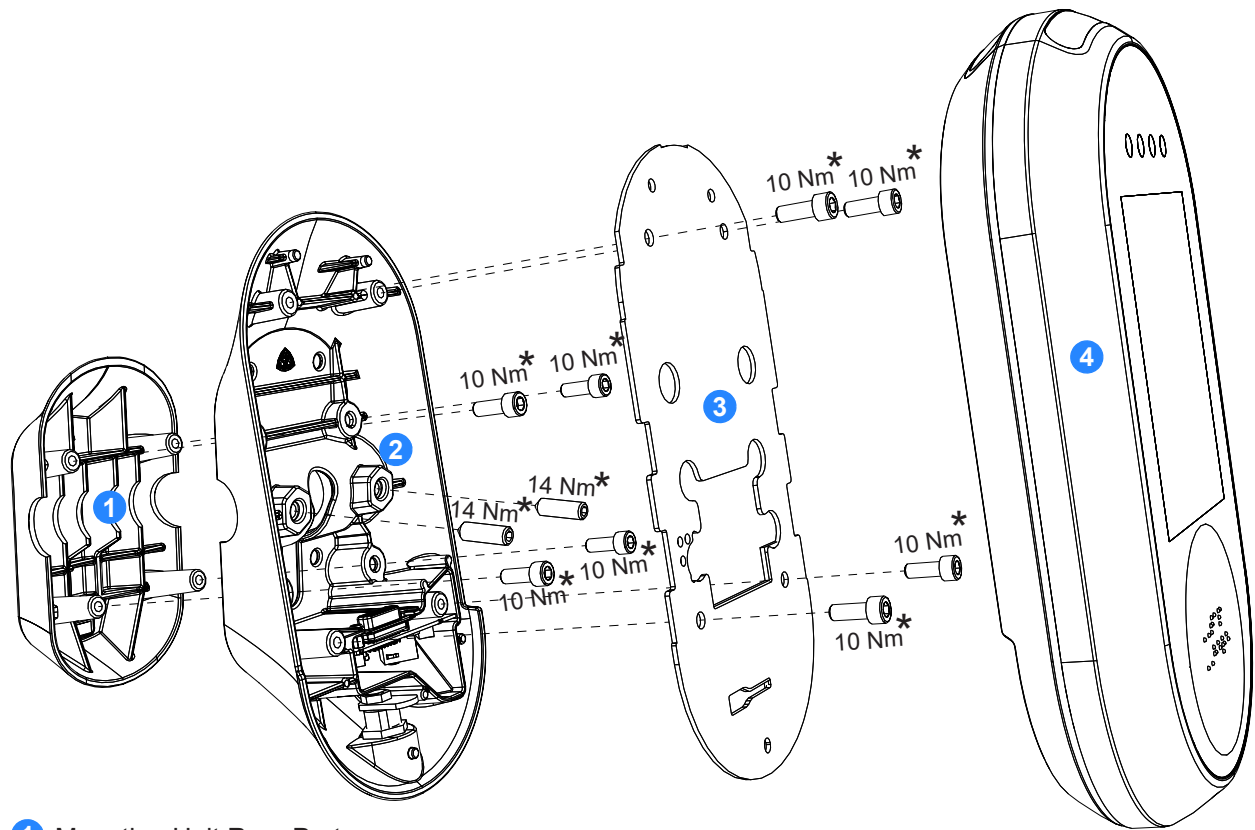


Figure 9-14 Module Removal - Mounting Unit (Option: Vertical Installation)



- 1 Mounting Unit Rear Part
- 2 Mounting Unit Front Part
- 3 Mounting Plate
- 4 Base Unit
- * Secure with Loctite 243

Figure 9-15 Module Removal - Mounting Unit (Option: Horizontal Installation)

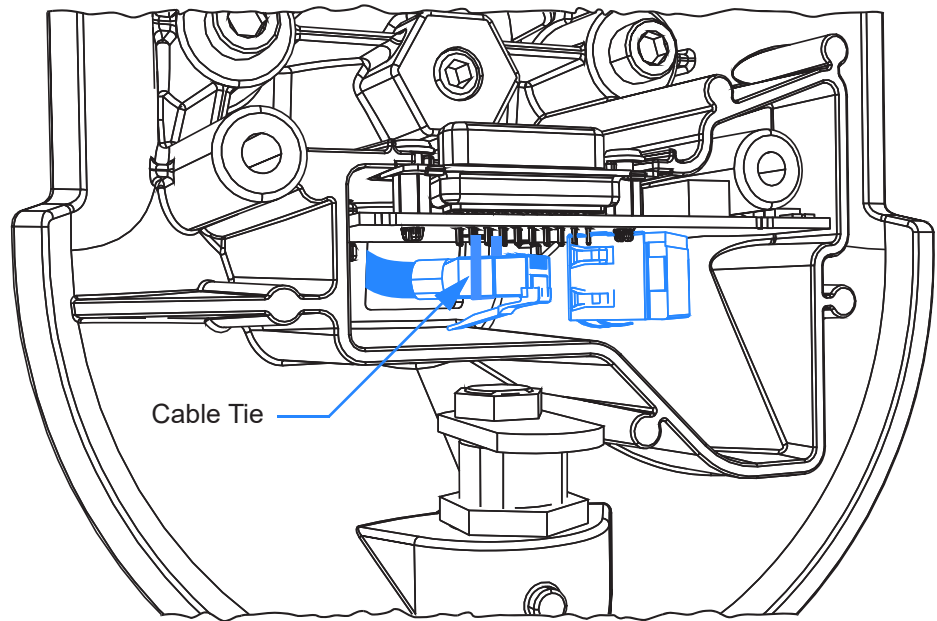


Figure 9-16 Wiring Connections

- Step 5** Place a new FareGo Val OV|41 mounting unit near the proper mounting position and connect the power/network cable as shown in **Figure 9-16**.
- Step 6** Secure the plug to the circuit board by a cable tie
- Step 7** Put the FareGo Val OV|41 in the proper mounting position on the mounting post as shown in **Figure 9-17**.

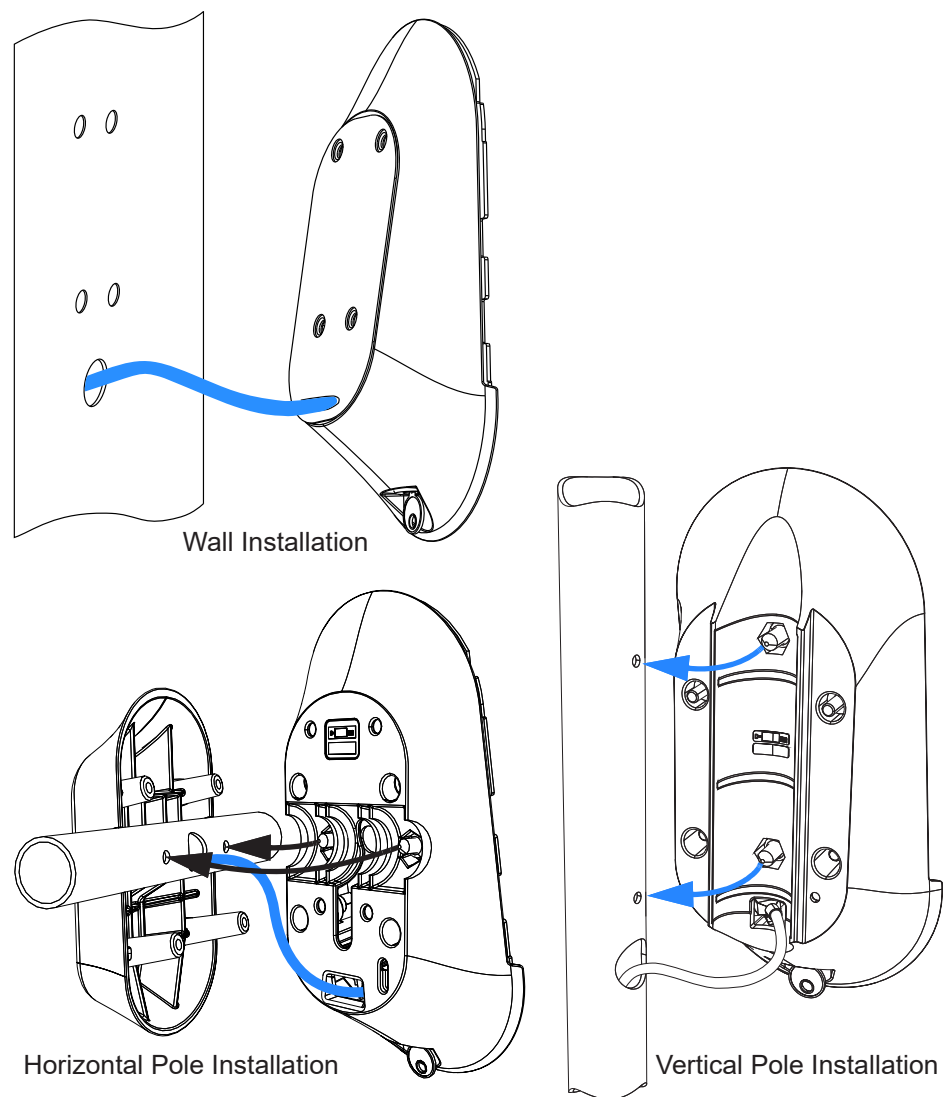


Figure 9-17 Wiring Connections

- Step 8** Set the mounting unit rear part on the mounting unit front part and fix it with the four screws shown in **Figure 9-14**. (Secure the screws with Loctite 243)
- Step 9** Set the mounting plate on the mounting unit front part and fix it with the four screws shown in **Figure 9-14**. (Secure the screws with Loctite 243)
- Step 10** Install the base unit as shown in Chapter **9.6**.

9.7 Returning the Validator to Service

9.7.1 System MicroSD Card

Replacement devices will be pre-initialized. The system provider is not responsible for either initialization or creation of system microSD cards (system initialization modules).

9.7.2 Import Backup

If a backup microSD card is used, you can transfer the data from the backup microSD card of the old device to the replacement device. The backup module holds the last shift data and the device ID only.

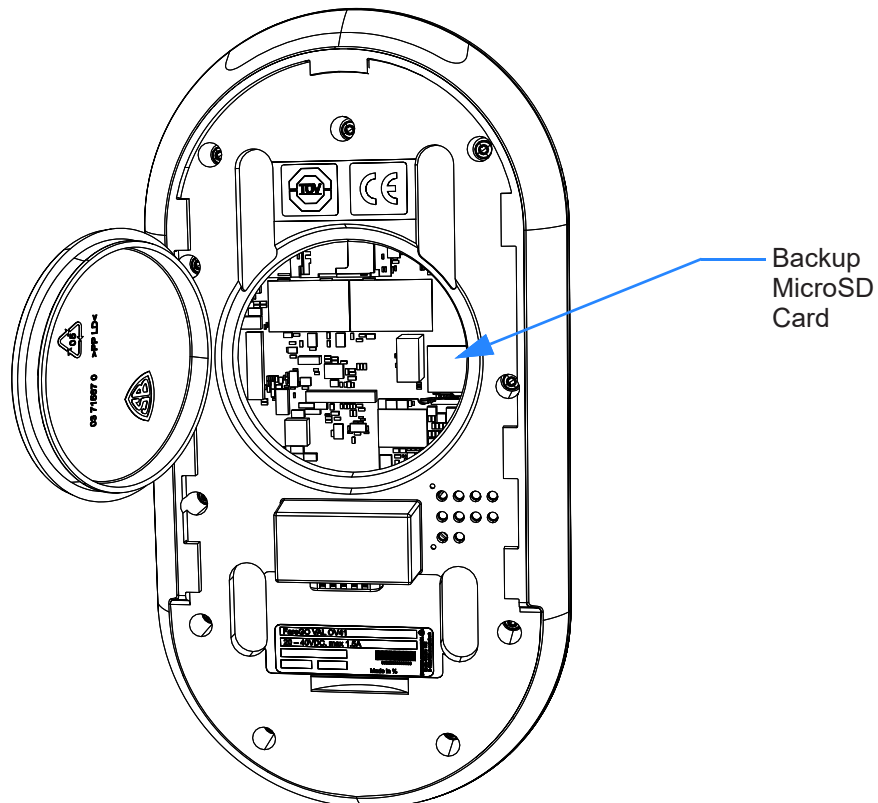


Figure 9-18 Backup MicroSD Card

Step 1

If the device is faulty, transfer its backup microSD card to the new device.

When powered on (see **Section 9.7.6**), the device initialization through the backup microSD card will be completed with a synchronization. There will be no loss of device data.

Avoid using an empty backup card. Only use an empty card during a device swap if the original backup module is lost, defective, or the entire device/backup combination is not available.

Maintenance staff should be careful not to damage or lose backup modules when swapping faulty devices, because all backed up data will be lost. Users may determine if a device backup module is faulty by checking the backend system.

9.7.3 New Backup MicroSD Card

Only if no backup is available, use a new backup microSD card. No configuration is needed for the initialization of the new backup microSD card (backup module).

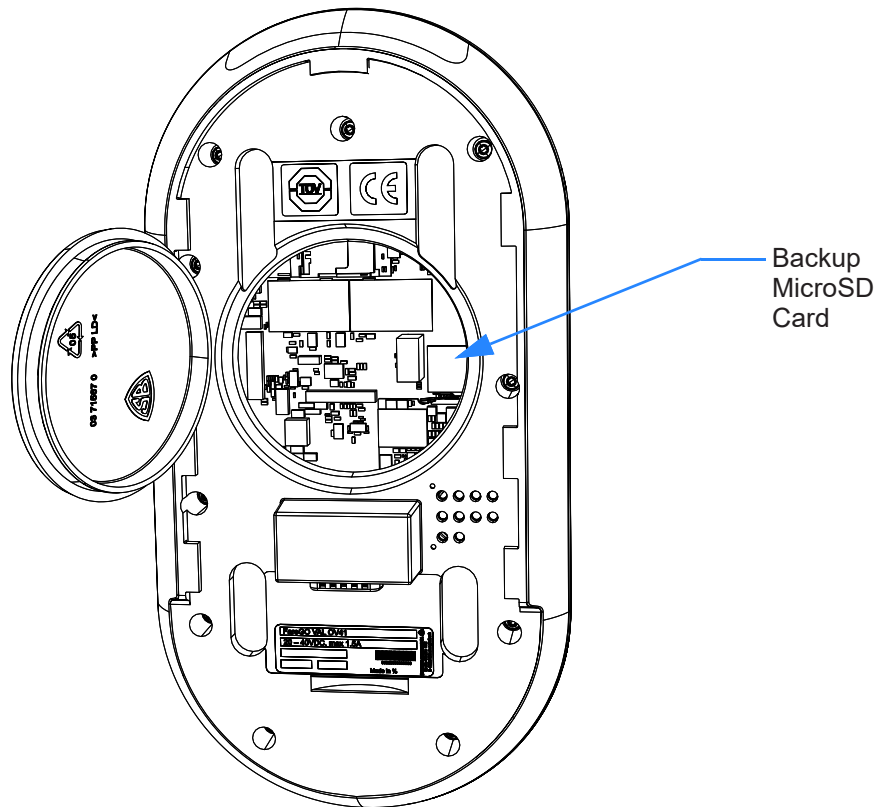


Figure 9-19 Backup MicroSD Card

- Step 1** Insert the empty microSD card in the corresponding backup microSD card slot.
- When powered on (see **Section 9.7.6**), the device will recognize the empty microSD card and will initialize it automatically. If the device detects a non-empty microSD card, the device will reject the microSD card and remain out of service.
- Spare backup microSD cards will be provided with each spare device. The service provider is responsible for providing additional spare backup modules.

9.7.4 Recovery Scenarios

If the FareGo Val OV|41 is faulty but the backup microSD card is still intact, follow Recovery Scenario 1. If the microSD card is lost, damaged, or defective but the FareGo Val OV|41 is functional, follow Recovery Scenario 2. If both the FareGo Val OV|41 and the backup microSD card are damaged (a double failure), follow Recovery Scenario 3.

The following description needs to be updated.

9.7.4.1 Recovery Scenario 1

If the FareGo Val OV|41 is faulty but the backup microSD card is still intact, follow these steps.

- Step 1** Remove faulty FareGo Val OV|41 from the bus (unplug data/power cable - remove from the pole).
- Step 2** Remove the backup microSD card from the malfunctioning FareGo Val OV|41 (spring loaded, pressing it down will pop it up for removal). It is a small module; be careful handling it.
- Step 3** Install a new FareGo Val OV|41 on the bus (following the standard installation process).
- Step 4** Insert the working backup microSD card from the faulty FareGo Val OV|41 into the new FareGo Val OV|41 (left slot).
- Step 5** Turn on the FareGo Val OV|41 (hook up data and power cables and re-attach to pole).
- Step 6** FareGo Val OV|41 goes through a recovery process (configures IP, data, transactions, etc.).
- Step 7** FareGo Val OV|41 will reboot after the recovery process. At this point the device is identical to the failed one.
- Step 8** Turn on the device and sync to backend system (to receive updated lists / version data); make sure that the FareGo Val OV|41 is operational and communicating online.
- Step 9** DATA STATUS: NO data loss.

9.7.4.2 Recovery Scenario 2

If the backup microSD card is lost, damaged, or defective but the FareGo Val OV|41 is functional, follow these steps.

- Step 1** Open the FareGo Val OV|41 cover. If necessary, remove the faulty backup module.
- Step 2** Insert a formatted new microSD card. The device auto recovery function will copy the correct Backupmodul.ini file onto the new card (ini file is now also saved on device internal hard disk) and backup the data.
- Step 3** DATA STATUS: NO data loss - All transaction data will be retrieved from the working FareGo Val OV|41 and uploaded to the backend system.

- 9.7.4.3 Recovery Scenario 3** If both the FareGo Val OV|41 and the backup microSD card are damaged (a double failure), follow these steps.
- Step 1** Remove the damaged FareGo Val OV|41 from the bus; it needs to be replaced.
 - Step 2** Send FareGo Val OV|41 (along with its backup microSD card) to Central Repair Depot to attempt retrieval of the shift files (data recovery may not be possible depending on the extent of the damage).
 - Step 3** Install a new FareGo Val OV|41 on the bus.
 - Step 4** Insert new backup SD card which has the file Backupmodule.ini with the correct ID setting, see **Section 9.8**. The number will be the same as the one on the original backup module, and can also be seen under Extended Parameters in Device Maintenance. The FareGo Val OV|41 will configure itself and use the microSD card as backup module when it is powered on.
 - Step 5** DATA STATUS: Possible Loss. The transaction data generated since the last synchronization is at risk of being permanently lost in the case of the dual failures of both the FareGo Val OV|41 and Backup module. If the main logic board of the FareGo Val OV|41 is intact, or if the microSD card can still be read, then data recovery at the Central Repair Depot may be possible.
- 9.7.5 Initial Check** Complete the following checklist before turning on the validator:
- ✓ Verify that all screws have been tightened firmly.
 - ✓ Ensure that the equipment is properly grounded.
 - ✓ Ensure that power supply is installed and is working correctly.
 - ✓ Check the state of the fuses (power supply side).
 - ✓ Verify that all wires are firmly connected.
 - ✓ Verify that you have not forgotten anything inside the device.
- 9.7.6 Turn on Power** Turn on power at the main facility breaker. When the power supply is switched back on, the validator automatically returns to operation.
- 9.8 ID Number of Validator** The format for the ID number in the Backupmodule.INI file is as follows: AABBBBBBCC, where AA is the provider number, BBBBBB is the 6 digit device ID (such as 020001), and CC is the position in the bus of the FareGo Val OV|41 (00, 01, 02...). Thus, an example number would be 1202000103. This information is also available by opening the INI file in notepad, and is easily set.
- Here is an example:
 Backupmodul.ini Identifier=129999903
 Operator ID 12
 Device ID 999999
 4th FareGo Val OV|41 (Position number 03)

Chapter 10

Glossary

10.1 Glossary of Terms and Abbreviations

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

AFC	Automated Fare Collection
AWG	American Wire Gauge
Aztec Code	2D barcode designed by Andrew Longacre at Welch Allyn (now Honeywell Scanning and Mobility). Public domain. International Standard: ISO / IEC 24778.

B

Boot	Bootting is the process of starting a computer
-------------	--

C

CAD / AVL	CAD / AVL (Computer Aided Dispatch and Automatic Vehicle Location System) is the British and American counterpart of the RBL standard widely used in Germany. The objective of the system is to monitor the positions of buses and trains on their planned routes and be able to provide passenger information in buses and trains as well as at stops. In addition, there is also the possibility to control communication between the driver or CAD / AVL system and the control center. CAD / AVL is similar to the German RBL which has been superseded by ITCS.
Calypso	Calypso is an international electronic ticketing standard for microprocessor contactless smart cards, originally designed by a group of transit operators from 11 countries including Belgium, Germany, France, Italy, Latvia, Portugal, Canada and others.
CE	Communauté Européenne Communauté Européenne marking is a certification mark that indicates conformity with health, safety, and environmental protection standards for products sold within the European Economic Area (EEA).
CMOS	Complementary Metal-Oxide-semiconductor Structure Complementary Metal-Oxide-semiconductor Structure is a set of semiconductor technologies for building integrated circuits and the corresponding circuitry of microcircuits.
Codabar	1D Barcode. Codabar is a numeric code with some additional special characters (0..9 and - \$: / . +). There are four different start and stop signs defined.
Code 128	1D Barcode. Code 128 Auto can encode the complete ASCII-character set. This is done by switching between all 3 character sets of Code 128.

Code 39 1D Barcode. Code 39 is an alphanumeric code. Each character is built by 9 elements (5 lines and 4 spaces) where 3 are thick and 6 are thin. This allows the self-checking of code 39. Code 39 does not require a build-in check digit. The main advantage is the wider character set.

CSA Canadian Securities Administrators
CSA is a not for profit standards organization which develops a wide range of standards for Canadian industry including standards on energy, electrical, construction, quality management, health care, environment, and information technology.

D

Data Matrix 2D Barcode from Microscan Systems, formerly RVSI Acuity CiMatrix/Siemens. Public domain. Increasingly used throughout the United States. Single segment Data Matrix is also termed Semacode. - International Standard: ISO/IEC 16022.

E

E1 Part of an approval mark provided for by the Regulations annexed to the Agreement concerning the adoption of uniform technical prescriptions for wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles and the conditions for reciprocal recognition of approvals granted on the basis of these prescriptions (so-called UN/ECE Regulations) for fitting to equipment and parts. Here with the country code "1", which stands for Germany. In the case of a complete approval mark, the approval number and, where appropriate, the number of the international agreement containing the letter "R" and, where appropriate, additional symbols shall be affixed in the vicinity of this circle.

EAN-13 1D Barcode. The EAN barcode is primarily used in supermarkets to identify product at the point of sales. The products contain the EAN number or GTIN (Global Trade Item Number) to identify itself.

EAN-8 1D Barcode. EAN 8 is the short form of EAN-13. This code is only used if the article is too small for an EAN-13 code. The restrictions for this are very hard. An EAN-8 will only be granted if a EAN-13 will uses more than 25% of the front space of the article.

EMV Europay International, MasterCard und VISA
Europay International, MasterCard and VISA is a specification for payment cards equipped with a processor chip and the associated smart card devices.

ESD Electrostatic Discharge
Electrostatic discharge is the sudden flow of electricity between two electrically charged objects caused by contact, an electrical short, or dielectric breakdown. The ESD occurs when differently-charged objects are brought close together or when the dielectric between them breaks down, often creating a visible spark.

F

FareGo The FareGo product brand is a complete system solution offered by Scheidt & Bachmann for all fare management requirements of public transport systems.

Only for FGD CS:
The first-class solution portfolio is characterized by innovation strength and high quality requirement. FareGo consists of innovative hardware, modular software and customized services and covers all aspects of the ticketing sector. High user friendliness and modern design are significant features of our products.
The clearly-arranged structured brand architecture offers our customers guidance during the conception of their ticket management system. The individual products of the comprehensive portfolio were compiled into product lines:

- FareGo Sales: Sales systems
- FareGo Val: Validators
- FareGo Gate: Entry and exit control
- FareGo Move: Mobile terminals
- FareGo Data CS: Software
- FareGo Life: Lifecycle services

Whether a local operator or a bus line, supra-regional or operator of a multi-mode transport network or participant of a multi-operator system - FareGo supplies the right solution for ticketing in public transport systems!

FCC Federal Communications Commission
This is an independent agency of the United States government created to regulate interstate communications by radio, television, wire, satellite, and cable. The FCC maintains jurisdiction over the areas of broadband access, fair competition, radio frequency use, media responsibility, public safety, and homeland security.

FCS Fare Collection Systems, one of four business areas of Scheidt & Bachmann Fare Collection Systems GmbH

I

IBIS Integriertes Bordinformationssystem (german), which is the integrated on-board information system.

ID Identification Number

IEC International Electro-Technical Commission
The IEC is an international standards organization for standards in the field of electrical engineering and electronics with headquarters in Geneva.

Interleaved 2 of 5 1D Barcode. Code 25 Interleaved is a special type of Code 25 that is also a numeric code able to display digits from 0 to 9. The code is also known as Code 2 of 5 Interleaved.

ITSO ITSO is a national railcard system used in the United Kingdom

L

LCD Liquid Crystal Display

M

Maxicode 2D Barcode used by United Parcel Service. Now public domain.

MCL MasterCard contactless
MasterCard Contactless is compatible with EMV contactless payment technology. Based on the ISO / IEC 14443 standard, which provides MasterCard and Maestro card holders with a way to make a payment by touching a payment card or other payment tool, such as a smartphone to a reader on a payment terminal instead of swipe it through a read or insert it to the terminal.

MIFARE The brand name covers proprietary solutions based upon various levels of the ISO/IEC 14443 Type A 13.56 MHz contactless smart card standard.

MSHA Mine Safety and Health Administration
The Mine Safety and Health Administration is an agency of the United States Department of Labor which administers the provisions of the Federal Mine Safety and Health Act of 1977 (Mine Act) to enforce compliance with mandatory safety and health standards as a means to eliminate fatal accidents, to reduce the frequency and severity of nonfatal accidents, to minimize health hazards, and to promote improved safety and health conditions in the nation's mines.

MSI 1D Barcode. The MSI Plessey barcode has been designed by the Plessey Company, England in 1971. It has been used in libraries and stores.

N

NEC National Electrical Code
The National Electrical Code, or NFPA 70, is a regionally adoptable standard for the safe installation of electrical wiring and equipment in the United States.

NFC Near-field communication
Near-field communication is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (1,57 ") of each other.

NFPA 70	National Fire Protection Association NFPA 70 is a part of NEC directive. See NEC.
NRTL	Nationally Recognized Testing Laboratory Nationally Recognized Testing Laboratory is the term used by the United States Occupational Safety and Health Administration to identify third-party organizations that have the necessary qualifications to perform safety testing and certification of products covered within OSHA and each organization's scopes.
NWC	Network Controller A network controller is a computer hardware component that connects a computer to a computer network

O

OEM	Original Equipment Manufacturer An original equipment manufacturer is a company that produces parts and equipment that may be marketed by another manufacturer.
OSHA	Occupational Safety and Health Administration The Occupational Safety and Health Administration is an agency of the United States Department of Labor. This agency is responsible to "assure safe and healthy working conditions for working men and women by setting and enforcing standards and by providing training, outreach, education and assistance.

P

payWave	payWave (Visa) is a contactless payment technology feature that allows cardholders to wave their card in front of contactless payment terminals without the need to physically swipe or insert the card into a point-of-sale device.
PCB	Printed Circuit Board
PDF 417	2D Barcode originated by Symbol Technologies. Public domain. International standard: ISO/IEC 15438

Q

QR Code	2D Barcode initially developed, patented and owned by Denso Wave for automotive components management; they have chosen not to exercise their patent rights. Can encode Latin and Japanese Kanji and Kana characters, music, images, URLs, emails. De facto standard for Japanese cell phones. Used with BlackBerry Messenger to pick up contacts rather than using a PIN code. The most frequently used type of code to scan with smartphones. Public Domain. – International Standard: ISO/IEC 18004
----------------	--

R

RED Radio Equipment Directive
The Radio Equipment Directive deals with the placing on the market of radio-electric equipment. All product in scope of this directive and placed on the EU market must be compliant with this directive.

S

S&B Scheidt & Bachmann.

SAM Secure Access Module
A Secure Access Module (or Secure Application Module) is based on SmartCard Integrated circuits and is used to enhance the security and cryptography performance in devices, commonly in devices needing to perform secure transactions, such as payment terminals. It can be used for cryptographic computation and secure authentication against smart cards or contactless EMV cards.

SBC Compact Scheidt & Bachmann Computer Compact

SCR Smart Card Reader

T

TÜV Technischer Überwachungsverein
TÜV (Technical Inspection Association) are German businesses that provide inspection and product certification services.

U

UPC-A 1D Barcode. The UPC A code is the standard version of the UPC code and has 12 digits. It is also called UPC 12 and is very similar to the EAN code.

UPC-E 1D Barcode. The UPC E code is a short version with 8 digits, always starting with a zero.

V

Vicinity Vicinity is an card ISO standard for i.e. cards which can be read from a greater distance as compared with proximity cards. Such cards can normally be read out by a reader without being powered themselves, as the reader will supply the necessary power to the card over the air (wireless).

Chapter 11 Appendix

11.1 Additional Documents

This chapter shows all documents which are attached to the pdf version of this document.

You are able to find attached documents as shown in **Figure 11-1**

Click on the paperclip symbol on the left edge of the opened pdf document.

If this manual is printed from the PDF version, the attached files will not automatically be included.

If the attached files are needed in printed form, each attached file must be printed separately.

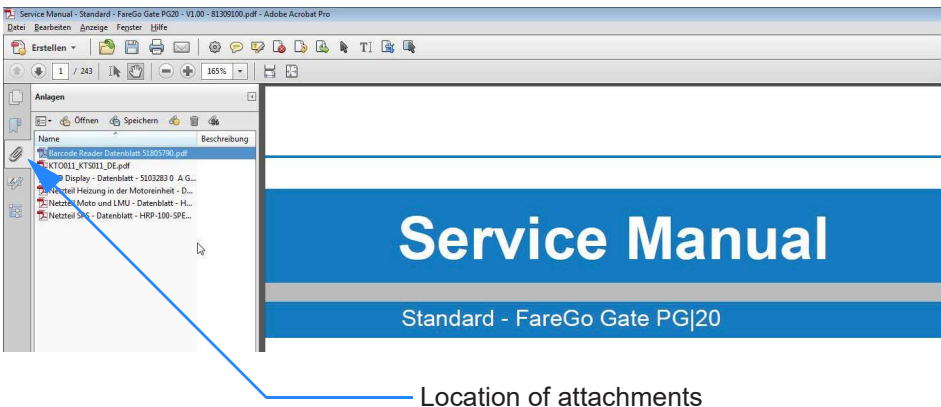


Figure 11-1 Location of attachments (this picture shows an example)

Drawing No.	Description
0375619 0 M_Mounting.pdf	Mounting Instructions Base Unit
0377129 0 E_Cable Plan.pdf	Cable-plan OV41
SBSCR2_SecurityGuidance_LifeCycle.pdf	Security Inspection Manual
51813140_Barcode Reader_Honeywell_N4680 2D.pdf	Barcode Reader Manual

Table 11-1 Appendix

