POLOCOM 2023 Keyless Repeater User Manual

Contents

POLOCOM SHOP

POLOCOM 2023 Keyless Repeater

Specifications

- **Emission Frequency:** 125 or 130 kHz (Audi and Mercedes-Benz: 20 kHz)
- **Reception Frequency:** Europe – 433, 434, 868 MHz; Japan and USA – 315 MHz

FAQs

- **What is a Relay Attack about Keyless Go?**
  - A Relay Attack involves transmitting data to allow unauthorized access to the vehicle. This can be done through radio keys being read from a distance, walls, or pockets, enabling the vehicle to be opened, started, and potentially moved unseen.

Introduction

- **Keyless Go** / **Keyless** Entry is a system that allows keyless unlocking and starting of the vehicle without actively using a physical key.

- **Functionality:** The user only needs to carry the key on them for the system to recognize their presence.

System Operation

Emission Frequency	Reception Frequency
125 or 130 kHz (Audi and Mercedes-Benz: 20 kHz)	Europe: 433, 434, 868 MHz; Japan and USA: 315 MHz

- Antennas placed around the vehicle emit a Low Frequency (LF) signal (125 or 130 kHz).
- The onboard system switches to UHF receive mode and waits for confirmation.
- **If the RFID transponder of the key is in the range:**
  - It receives the 125 kHz signal, decodes it, and sends a response via UHF.
  - The vehicle decodes this response and compares the codes.
  - **If the codes match:** the system unlocks the door.
  - **If there is no match:** the system returns to standby mode.

Door Unlocking

- **Unlocking Methods:**
  - **Automatic:** When the codes from the key and system match.
  - **Remote Control:** Using the remote control to unlock the doors.
  - **Mechanical Emergency Key:** For at least the driver's door, in case of emergency.

Keyless Go Key Components	Description
Mechanical Key	Usable in emergencies
Battery-powered Remote Control	For unlocking the vehicle remotely
RFID Chip	For identifying the driver
Integrated Battery	Powers the remote control

Engine Start

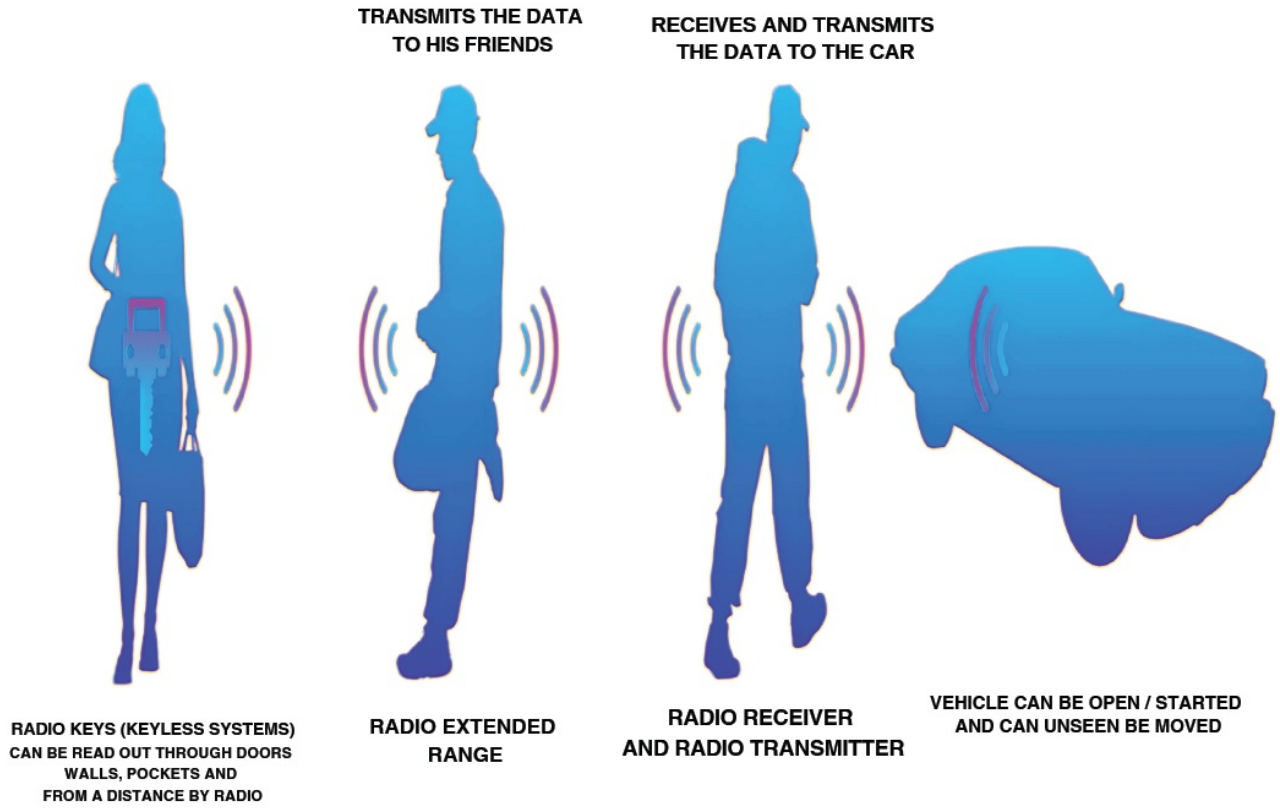
- **Process:** Similar to the door unlocking process, except that the start/stop button is pressed.
- **Key Position:** The keyless control unit must recognize the transponder as being within the vehicle.
- **System Challenges:** The system must consistently distinguish between the interior and exterior, ensuring the key is recognized internally when within the vehicle and as external when outside.

Additional Features

- **Automatic Locking:** The vehicle can automatically lock when the transponder moves out of range.
- Sensors on Door Handles (e.g., Mercedes-Benz S-Class, Toyota Prius, VW Phaeton):
- May include volume sensors, touch sensors, or tactile buttons on the exterior of the handle to lock/unlock the vehicle.

DESCRIPTION OF THE FUNCTIONALITY OF THE KEYLESS GO REPEATER, WHEN CARRYING OUT THE RELAY, REFERRED TO AS “RELAY ATTACK”

This is how a hacker attack works via radio/Relay Station Attack (RSA)



AN ILLUSTRATIVE EXAMPLE OF WORKING WITH A REPEATER

THE OPERATOR OF THE “SMALL BLOCK” RECEIVES THE “LF” SIGNAL FROM THE CAR, AND TRANSFERS IT TO THE “BIG BLOCK”

- THE OPERATOR OF THE “BIG BLOCK” RECEIVES A SIGNAL FROM THE “SMALL” ONE AND

TRANSMITS IT TO THE CAR KEY

- In the picture above, the system uses the essence of the attack without key access “Keyless Go / Keyless Entry” and how the signal is relayed with subsequent user authorization.

IN SIMPLE WORDS:

- “LF” ANTENNA OF THE CAR AND TRANSMITS IT TO THE LARGE BLOCK. OTERAN ANTS.16 MAGE BEL FION ME
- THE OPERATOR OF THE “BIG BLOCK” BEING NEAR THE KEY (5-10 METERS TO THE INTERNAL ANTENNA), RECEIVING AN INFORMATIVE REQUEST FROM THE “SMALL BLOCK”, ISSUES IT TO THE KEY. IMITATING THE PRESENCE OF THE KEY NEXT TO THE CAR
- THE KEY, HAVING RECEIVED A REQUEST FROM THE “BIG BLOCK”, RESPONDS TO THE CAR ON ITS FREQUENCY (315, 433, 434, 868 MHZ).

- AFTER THAT, THE CAR RECEIVES THE CORRECT ANSWER FROM THE KEY, AUTHORIZES THE USER, IN OTHER WORDS, REMOVE THE CAR FROM THE

Security Mode and Attack Process

Security mode makes it possible to open the door and, in other words, start the engine.

To execute this, here are some critical points:

1. **To the operator of the 'Small block' –** The blue LED indicates the signal from the car when located near the 'LF' antenna (near the car door handle, inside the car).
2. **To the operator of the 'Big Block' –** Positioned close to the car key (5-10 meters from the internal antenna).
    - Following this process, the system activates automatically, indicated by the LED on the 'Big Block' during communication between the blocks.

Functional Features and Characteristics

Description	Value
Minimum distance from large block to key (internal antenna)	1 meter
Average distance from large block to key (internal antenna)	3-10 meters
Maximum distance from large block to key (internal antenna)	12 meters
Average distance from large block to key (External optional antenna)	10-17 meters
Maximum distance from large block to key (External optional antenna)	25 meters
Guaranteed communication distance between units (1 *)	350 meters (any reception)
Maximum communication distance between units (1 *)	600 meters (open field)
Distance from car to key for authorization (2*)	250 meters, up to 150 meters

Distance and Signal Information

Distance and Signal Information and Supported Car Brands (<2023)

1. This is the distance at which you will have a stable connection between the blocks.
    - In other words, the signal will reach from a small block to a large one in building conditions, radio interference around urban areas, and the presence of reinforced concrete or metal structures in conditions of signal retransmission.
2. This is the distance at which, during the attack, there is a one-way process of relaying the low-frequency signal from the car to the key.
    - After receiving a signal from the "Big Block," it responds to the car and authorizes access. The maximum distance for car access depends on various factors, including car model, key frequency (315, 433, 434.868 MHz), and battery charge. This distance is typically between 70-150 meters, but certain models

can reach up to 250 meters.

Key Search Function

In the first mode, immediately after turning on the power, a continuous search for the TOYOTA / LEXUS keys begins within the “Big block” working area. When the key is found, the “Indication” LED will glow green; if there is a built-in vibrator, the “Big Block” body will begin to vibrate.

Supported Car Brands

Car Brand	Models Supported (<2023)
Audi	All models
Mercedes	All models
BMW	All E-series, F-series, G-series models
Mazda	All models
Honda	All models
Toyota	All models
Lexus	All models
Subaru	All models
Nissan	All models
Infinity	All models
Hyundai	All models
Kia	All models
Porsche	All models
Citroen	All models
Peugeot	All models
Renault	All models
TESLA Electric Car	All models (<2018)

Note: The list contains brands that have been personally verified. The device supports almost all brands equipped with the Keyless system, so the real list is much larger. By purchasing any version, you can activate new functions remotely. They will be reserved in the instrument. To do this, you will need to pay the specified amount for the desired function and receive a pin code to activate it. Naturally, buying additional functions will be more expensive than you would immediately buy the full version. But someone does not need all the functions so you can save on the price of the device, and it will be more affordable for you.

Available options:

1. Vibration upon detection of a key in the area of operation of the “Big block”
2. External antenna

Large Block – Modes of Operation:

1. Mode for working with vehicles equipped with Keyless Go system:
    - Toyota all model happy (2009-2020)
    - Lexus All Model Happy (2006-2020) rubber
    - Subaru All Model Happy (2008-2020)

2. “Multibrand” mode for working with cars equipped with Keyless Go or Keyless Entry systems of all other brands (BMW All models E-series, F-series, G – series, Mazda, Honda, Acura, Nissan, Infinity, Hyundai, Kia, Porsche, Citroen, Peugeot, Renault) inclusive until 2017-2020 (Audi up to 2011, Mercedes-Benz up to 2013).
3. Mode for working with cars equipped with the FBS4 system, Audi until 2020 and Mercedes-Benz until 2018 opening and starting, 2018-2020 only starting the car.
4. “Multibrand 868” mode for working with cars equipped with a Keyless Go or Keyless Entry system in which the key works at a frequency of 868 Mhz, in particular, it is BMW Eseries (BMW F – Series only where the keys are for 868) and some cars VAG – Group.
5. Mode for working with cars of the TESLA Electric Car brand until 2018. (up to plastic keys that look like a credit card)
6. Mode for working with cars of the Nissan brand – Infinity from 2017 to 2020.. After turning off, the large unit turns on in the same mode in which it was turned off earlier.
    - **Note:** The list contains brands that have been personally verified. The device supports almost all brands equipped with the Keyless system, so the real list is much larger.

By purchasing any version, you can activate new functions remotely. They will be reserved in the instrument. To do this, you will need to pay the specified amount for the desired. function, and receive a pin code to activate it. Naturally, buying additional functions will be more expensive than you would immediately buy the full version. But someone does not need all the functions so you can save on the price of the device, and it will be more affordable for you.

Available options:

1. Vibration upon detection of a key in the area of operation of the “Big block”
2. External antenna

Large Block Modes of Operation:

1. Mode for working with vehicles equipped with the Keyless
    - **Go system:**
        - Toyota all model happy (2009-2020)
        - Lexus All Model Happy (2006-2020)
        - Subaru All Model Happy (2008-2020)
2. “Multibrand” mode for working with cars equipped with Keyless Go or Keyless Entry systems of all other brands (BMW All models E-series, F-series, G – series, Mazda, Honda, Acura, Nissan, Infinity, Hyundai, Kia, Porsche, Citroen, Peugeot, Renault) inclusive until 2017 – 2020 (Audi up to 2011, Mercedes-Benz up to 2013).
3. Mode for working with cars equipped with the FBS4 system, Audi until 2020 and Mercedes-Benz until 2018 opening and starting, 2018-2020 only starting the car.
4. “Multibrand 868” mode for working with cars equipped with a Keyless Go or Keyless Entry system in which the key works at a frequency of 868 Mhz, in particular, it is BMW E – series (BMW F – Series only where the keys are for 868) and some cars VAG – Group.
5. Mode for working with cars of the TESLA Electric Car brand until 2018. (up to plastic keys that look like a credit card)
6. Mode for working with cars of the Nissan brand – Infinity from 2017 to 2020 After turning off, the large unit turns on in the same mode in which it was turned off earlier.


Indication LED «Battery charge»
Connector for charging or an external antenna
Indication of "Active session and LF reception"
Indication LED «On\Off»
Micro usb - charging connecto
Button «On\Off»
LEDs for indication of operating modes:
Mode No.2 - two LEDs are off
Mode No.3 - yellow LED is on
Mode No.4 - green LED is on
Indication LED «Selected mode, session status, and other indications»
Button «Function»
Button «On\Off»

BIG BLOCK

The Big Block can be turned on in two ways:

- **simply by turning on the power button,** the device will start in the last selected mode before turning off. (in other words, the device remembers with which mode it worked before turning off, and it will switch to it automatically when the power is turned on)
- **Mode selection:** to do this, first of all, hold down the “Function” button, without releasing it, turn on the device with the power button. At the same time, watch the LED indication. How many times will he blink this mode with you and turn it on? To select the mode you need, on the number of blinks which mode is needed for operation, the “Function” button must be released to activate it.

To turn it off, switch the “On / Off” button to the “O” position Example: YOU NEED TO TURN ON MODE No. 3 to do this, you need to do the following – first hold down the “Function” button (and do not release it), turn on the device with the power button, wait three times for the LED to turn green, and at this time release the “Function” button. After that, as confirmation, the indication LED will blink 3 times in blue (confirmation of the selected mode) and will turn on mode No. 3 accordingly.

Status LED indication colors

Function name	LED color	Action
When selecting a mode	Green	- when selecting a mode
When confirming the mode selection	Blue	- after selecting the mode
Mode No. 7 (Nissan \ Infinity 2017-2020)	Blinking Yellow Blue	- ready for work - active session
Mode No. 2 (Multi-brand)	Blinking Green Blue	- ready for work -active session
Mode No. 3 (Audi - Mercedes)	Pink yellow blue	-ready for work -active session -active session
Mode No. 4 Mode No. 2 (Multibrand 868 MHz)	Green-red blue	-ready for work -active session
Mode No. 5 (Tesla)	Blinking white blue	-ready for work -active session

SMALL BLOCK

- **Switching on –** long press on the “on / off” tact button until the “Red on / off indication LED” blinks, then release the button. Confirmation that the device has been turned on will be permanently lit “Red LED” above the button.
- **Switching off –** long press on the “on / off”‘ tact button until the “red on / off indication LED” goes out, then release the button. The confirmation that the device has been turned on will be the absence of the “Red LED” above the button.
- **Selecting the operating mode –** after the switch-on procedure, each short press on the “on / off” tact button will correspond to the number of the operating mode. Example: two short presses – Mode
  - **No. 2** (both mode indication LEDs are OFF), three short presses –
  - **Model No. 3** (only the Yellow LED is on), four short presses – Mode
  - **No. 4** (Only the Green LED mode indication is on)
- **The process of working with the device –** to get started, we need to turn on the “Small block”, and select the operating mode you need. Then, being near the car, bring the device to the location of the “LF” antenna *. The fact that the process of receiving the “LF” signal from the car has begun, and its subsequent retransmission to the “Big block” will be the turning on of the LED indicating the “Active session” in BLUE color.
- **Then:** to open the car door, you need to insert your hand into the car door handle if it is equipped with a volume sensor in the handle, slide your finger along a special mark on the car handle, or if there is a button on the car handle, press it. to start the engine, it is necessary, with automatic transmission, to make sure that the gear

lever is in the “P” or “N” position, depress the brake pedal, and start the engine with the “Star/ Stop” button. (With a manual transmission, make sure the gear lever is in neutral. depress the clutch pedal and start the engine with the Star / Stop button.)

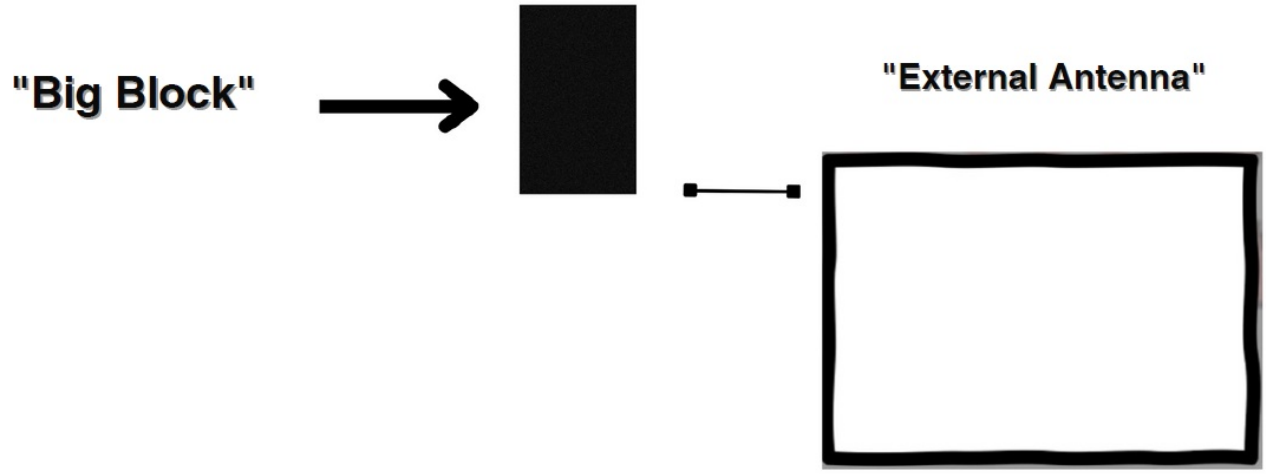
- *** LF ANTENNA LOCATION –** On the outside of the car – near the door handle (95% of cars), in some brands, it is a pillar between the front and rear doors (Audi and Mercedes) or in the middle of the rear door panel BMW, Porsche. and some VAG-Group models)).

- Inside the car, this is any place in the car where the BLUE LED indicator lights up.

- The internal rechargeable battery is charged through the Micro USB connector located in the lower part of the case; during charging, the “White” LED will light up, and when fully charged, it will turn off. Charging is done with any standard charger from a mobile phone, for a fixed network, or a car.
- AFTER SHUTDOWN, “BIG BLOCK” AND “SMALL BLOCK” ARE TURNED ON IN THE SAME MODE AS THEY WERE TURNED OFF EARLIER.
- External low-frequency antenna – used to increase the range to the key when working with the “Big block”.
- Connected when the device is OFF, into the connector located on the side of the device (it is also a connector for charging the internal battery). Disabled after powering off the device.

Usage algorithm:

1. with the device OFF, connect the antenna to the connector, straighten it, and give it an approximate SQUARE shape.
2. We turned on the device and used it as directed.
3. Turn OFF the device, and disconnect the antenna.
    - **FEATURES:** when working with an external antenna, it must be straightened and shaped into a SQUARE / RECTANGLE for maximum efficiency.



- **Precautions:** Using and connecting an external Antenna to the device in a different order, and giving it a different shape may damage the device !!! (In this case, this will not be a warranty repair)

Warranty Commitment

- The warranty for each set of the device is 5 years from the day of purchase.
- To carry out warranty repairs, updates, and maintenance, it is necessary to have the integrity of the numbered seals on both blocks, as well as the model of the hardware version of the device applied to the surface of the back wall of each device.
- All possible damage to the decency of the above factors is guaranteed.

Disclaimer of warranty service:

- In the presence of broken numbered warranty seals, obvious traces of opening the device case, improper use of an external antenna, and deterioration of batteries.
- In all of the above cases, the manufacturer can refuse to repair, update, and maintain the device, any non-warranty repairs are made only at the expense of the buyer on an individual basis and time frame.

Equipment delivery set:

- **Big block** 1 piece
- **Small block** 1 piece
- **Charger for Big Block** 1 piece
- **Large block charging cable** 1 piece
- **Small unit charging cable** 1 piece
- **External optional antennal (Option)** 1 piece (option)

Documents / Resources

	**POLOCOM 2023 Keyless Repeater** [pdf] User Manual 2023 Keyless Repeater, 2023, Keyless, Keyless Repeater, Repeater

References

- **User Manual**