INSTRUCTIONS
OPERATION
RETRANSLATOR
Keyless Go – Keyless Entry

«AKS Pro» 5.1 version

Description of the Keyless Go / Keyless Entry system itself:

Keyless Go / Keyless Entry is a system without key (comfortable) access to unlock the car without actively using a simple key with a sting and start, simply by pressing the start button. This is made possible by the key that the driver of the vehicle carries with him. Keyless Go / Kole ant isregistered name. Similar solutions are available under different brands from How it works

LF 125 or 130 kHz (Audi and Mercedes-Benz 20 kHz) is emitted from several antennas distributed throughout the vehicle. The on-board system then goes into UHF receive mode (Europe: 433, 434, 868 MHz, Japan and USA: 315 MHz) and waits for confirmation. If the RFID transponder dongle is in range, it receives a 125 kHz signal, decodes it and actively sends it out on battery power with a new UHF encoding. In turn, it decodes the control unit in the vehicle. Since the Keyless Go control unit knows both coding tables, it can compare its own original output with the signal it just received. If there is no correct answer within a certain time, nothing happens and the system switches back to standby mode. Pulling on the door handle has no effect because the state of the door lock has not been changed by the Keyless Go system. However, if both codes match, at this time the user is authorized, the on-board system unlocks the lock, and pulling the handl шое unlocks the door. In addition, the car can also be opened using the remote control. In addition, there is a mechanical emergency key with which you can open at least the driver's doors. Thus, the Keyless Go car key consists of a mechanical key, a battery powered remote control, an RFID chip and a battery. In modern vehicles, the electronic key is designed both as a remote control and as a transponder, the mechanical emergency key only serves as an attachment to the key fob.

The engine start process is essentially the same as the door release process, except that the engine start / stop button is pressed here. A decisive factor for the function is that the keyless control unit recognizes the transponder as located in the vehicle. At the developmental stage, delimiting the inside and outside is one of the most difficult endeavors. This should allow the end user to store the key anywhere in the vehicle, with the key being recognized internally at all times. In addition, care must be taken to ensure that the key outside the vehicle is recognized everywhere as external and that the range does not increase too much.

If the owner so wishes, the car is locked automatically as soon as the transponder goes out of a certain range. In accordance with the conditions specified in the vehicle for size, position, power consumption of antennas and electronics, as well as allowable transmission energy, the ranges achieved are short. This effect is clearly desirable for security reasons. This scenario is the most controversial feature in keyless systems; therefore, automatic interlocking may be switchable or not offered by many manufacturers.

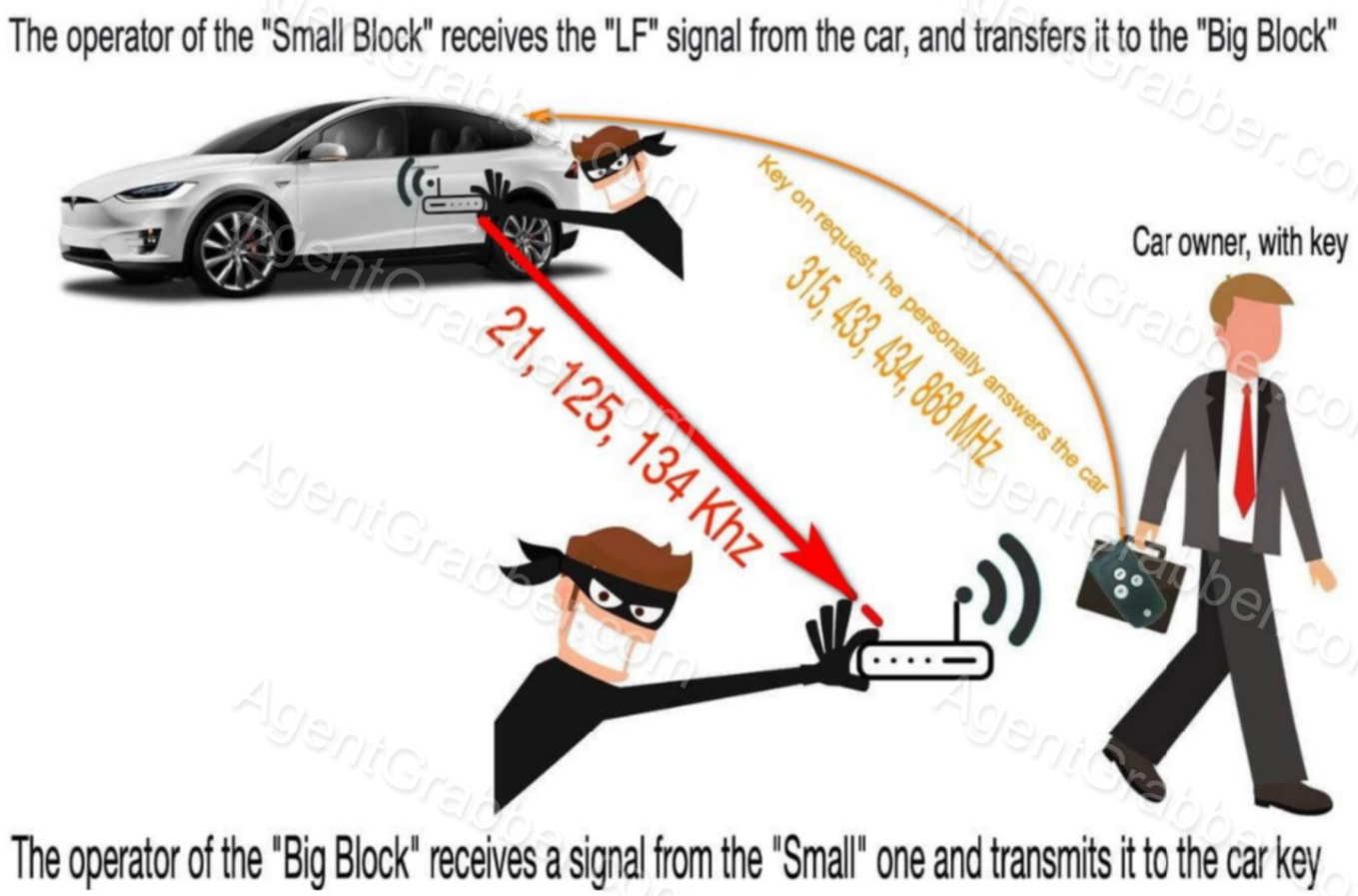
For many vehicles (for example, Mercedes-Benz S-Class, Toyota Prius, Toyota Yaris HSD, VW Phaeton) the door handle is equipped with a volume sensor, touch sensor, or just a tact button, which are located on the outside of the door handle, must be pressed to lock / unlock the vehicle.

Inside the passenger compartment, in most cases, a large clock button is used to start the engine.

It is located on the car console with the inscription "Start | Stop", some brands use a swivel mechanism in the steering column area (such car brands as Nissan, Porsche). The turn signal confirms the locking process with manual start as in the conventional locking system.

Description of the functionality of the "AKS Pro" repeater, when carrying out the relay, referred to as "Relay Attack"

An illustrative example of working with a repeater



In the picture above, the system, using the essence of the attack on 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 in close proximity to 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 own frequency (315, 433, 434, 868 MHz).

After that, the car receives the correct answer from the key, authorizes the user, in other words, removes the car from the

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

Thus, you need to understand several facts to conduct an attack:

1. To the operator of the "Small block" - The presence of indication of the received signal from the car, this is the indication of the blue LED when it is located in the immediate vicinity of the place where the "LF" antenna of the car is installed (near the car door handle, inside the car interior)
2. To the operator of the "Big Block" - located in close proximity to the key from the car (5-10 meters to the internal antenna)

If this algorithm is followed, everything happens automatically, which is signaled by the LED indication on the "Big block" during communication between the blocks and the authorization itself.

Functional features and characteristics

Description	Value
The minimum distance from the large block to the key (internal antenna)	1 meter
Average distance from large block to key (internal antenna)	3-10 meter
Maximum distance from large unit to key (internal antenna)	12 meter
Average distance from large block to key (External (optional) antenna)	10-17 meter
Maximum distance from large unit to key (External (optional)antenna)	25 meter
Guaranteed communication distance between units (1 *)	350 meters (in any reception conditions)
Maximum comunication distance between units (1*)	600м (open field)
Distance from the car to the key which it is possible to authorise (open the car door, start the engine) (2 *)	250 meters On average up to 150 meters

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 in urban conditions, the presence of reinforced concrete and metal structures in conditions of signal retransmission.
2 * - This is the distance at which, during the attack of the attack, we have a one-way process of relaying the low-frequency signal from the car to the key.
In turn, after receiving a signal from the "Big Block", he himself responds to the car and authorizes. So at what distance from the car the key can reach the car itself - this will be the maximum distance at which we can open the car and start. The distance at which the key works with the car depends on many factors, for example: it depends on the make and model of the car, on what frequency the key itself works (315 433 434.868 MHz), the battery charge in the key, etc. On average, if we generalize the statistics, then this distance is about 70-150 meters. In practice, there are several brands and models of cars that work even up to 250 meters. You also need to work on the factor that the higher the key is, the further it will be.
Key search function in the first mode:
In the first mode, immediately after turning on the power, a continuous search for TOYOTA / LEXSUS keys begins in the working area of the "Big block".
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.
Car brands supported by the repeater:

- Audi All model < 2020
- Mercedes All model < 2020
- BMW All models E-series, F-series, G
- series < 2020

• Mazda All model < 2020
Honda All model < 2020
10006
Toyota All models <2020
Lexus All models < 2020

- Subaru All models < 2020
- Nissan All models < 2020
- Infinity All model < 2020
- Hyundai All models < 2020
- Kia All models < 2020
- Porsche All models
- Citroen All models <2020
- Peugeot All models <2020
- Renault All < 2020
- TESLA Electric Car All <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 and 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)

abber

Subaru All Model Happy (2008-2020)

o 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)

7. 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 and 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)
o 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)
7. Mode for working with cars of the Nissan brand - Infinity from 2017 o 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 connecte
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 remembered with which mode it worked before turning off, and they 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 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 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 - Mode 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", select the operating mode you need. Then, being in close proximity to 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, or 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".

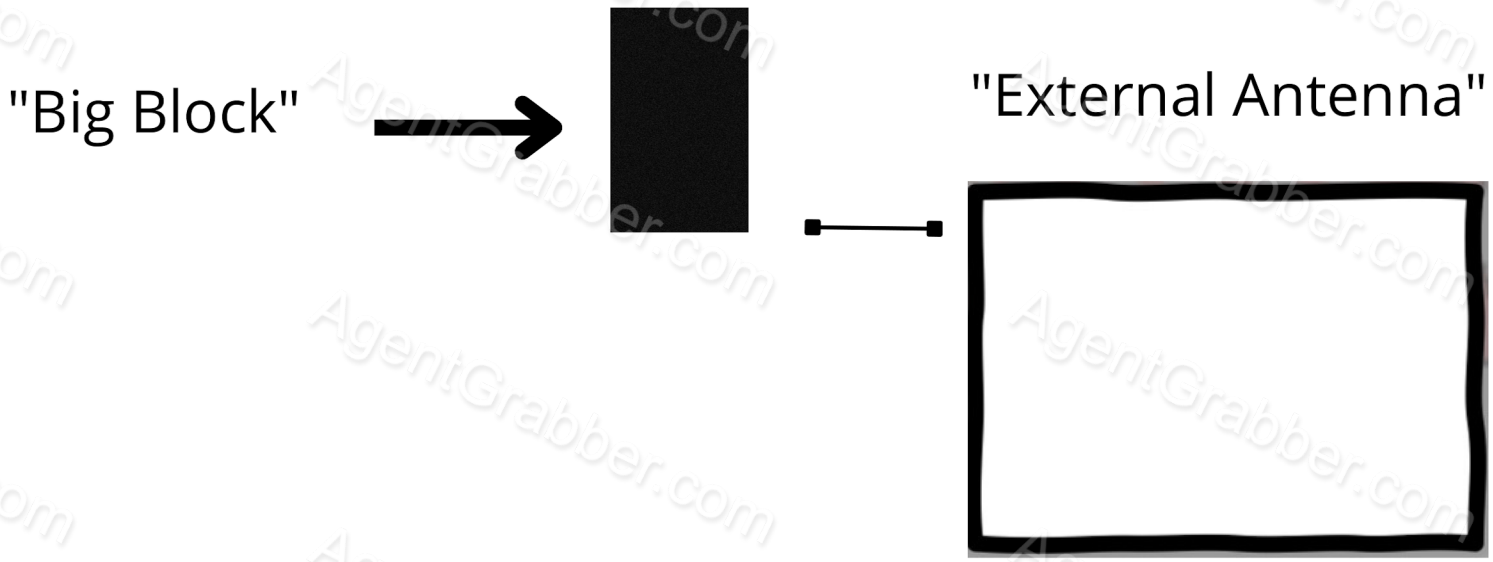
Connected - when the device is OFF, into the connector located on the side of the device (it is also a connector for charging the internal battery).

Disabled - after power 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 use it as directed.
3. Turn OFF the device, 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: Warranty for each set of the device is 5 years of 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 are 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, 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 antenna (Option)	1 piece (option)