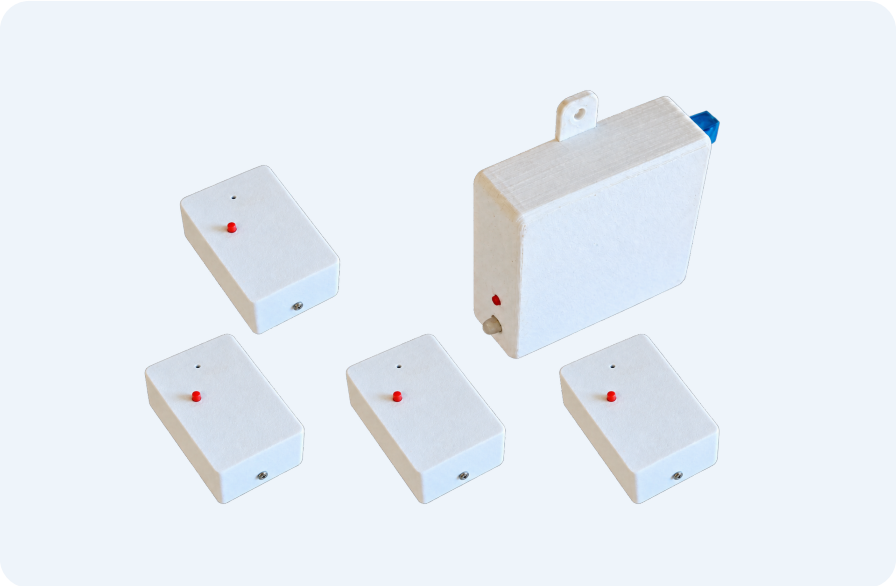
RADIO CONTROL · ROLLING CODE · HMAC-SHA-256

433 MHz transmitter-receiver rolling code SHA256-128bit

Radio-control system with HMAC-SHA-256 authentication, 128-bit tag, anti-replay rolling counter and selective management of up to 1024 remotes (512 recommended).



FREQUENCY
433 MHz
radio control

MEMORY
512 recommended
1024 absolute max

OUTPUT
5-15 VDC / 3 A
switched

SEPARATE KEY FOR EACH REMOTE

Each TX stores its own device key; the master key is not stored in the remotes.

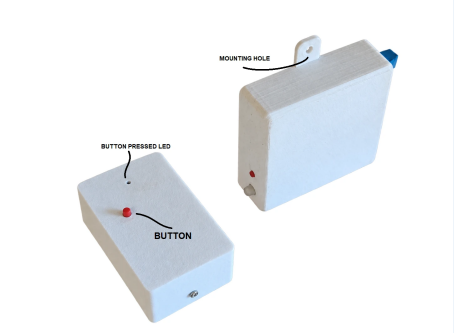
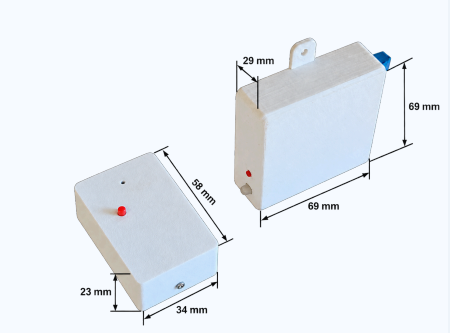
ESSENTIAL TECHNICAL DATA

Specifications, security and management

Radio frequency	433 MHz
Receiver input	5 - 15 VDC
Switched output	5 - 15 VDC / 3 A max
Remote supply	1 × AAA 1.5 V battery
Receiver capacity	512 recommended / 1024 max
Authentication	HMAC-SHA-256; 128-bit truncated tag
Anti-replay	monotonic rolling counter
Memory	non-volatile on receiver

LEARN / REMOVE PROCEDURE

- LEARN + remote button: the new serial number is stored.
- Successful addition: 3 slow LED flashes on the receiver.
- If the serial is already stored, repeating LEARN removes only that remote.
- Successful removal: 10 fast flashes. All other remotes remain enabled.
- Memory RESET: holding the dedicated control clears all stored remotes.

PROTOCOL SECURITY

The receiver derives a device key for each serial number using HMAC-SHA-256. In production transmitter firmware only the individual K_DEVICE is stored; the master key is not present. Frames are authenticated with HMAC-SHA-256 and a 128-bit tag. The receiver stores the accepted counter and rejects equal or older values, providing replay protection. Compromise of one transmitter does not directly disclose the master key or the device keys of other transmitters.