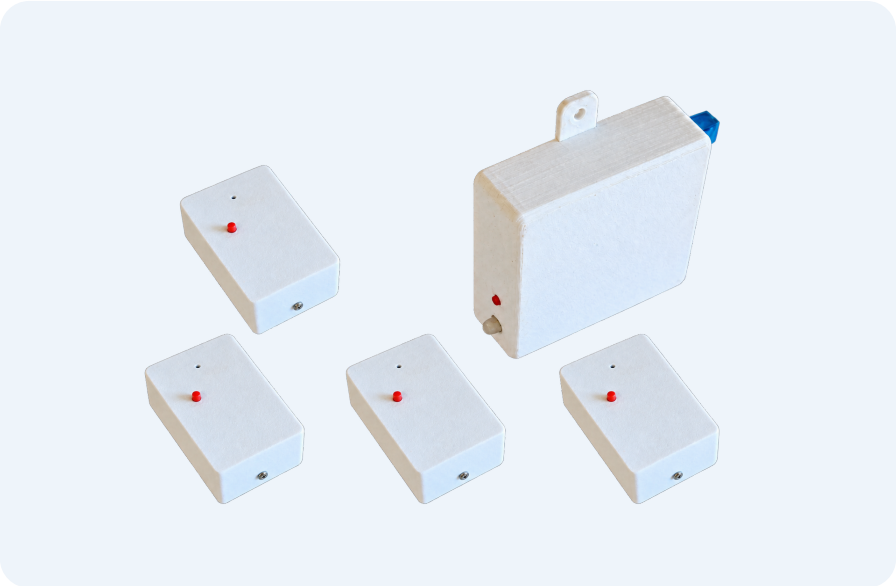
RADIOCONTROLLO · ROLLING CODE · HMAC-SHA-256

Trasmettitore-ricevitore 433 MHz rolling code SHA256-128bit

Sistema di radiocomando con autenticazione HMAC-SHA-256, tag a 128 bit, contatore rolling anti-replay e gestione selettiva fino a 1024 telecomandi (512 consigliati).



FREQUENZA
433 MHz
radiocomando

MEMORIA
512 consigliati
1024 limite assoluto

USCITA
5-15 VDC / 3 A
commutata

CHIAVI SEPARATE PER TELECOMANDO

Ogni TX contiene la propria chiave dispositivo; la master key non è memorizzata nei telecomandi.

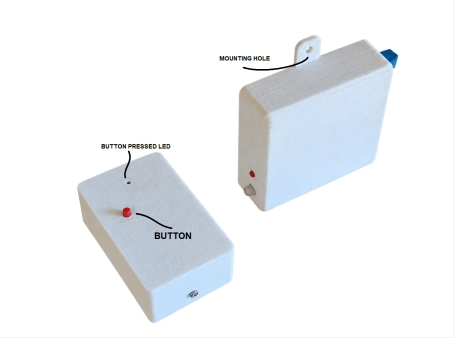
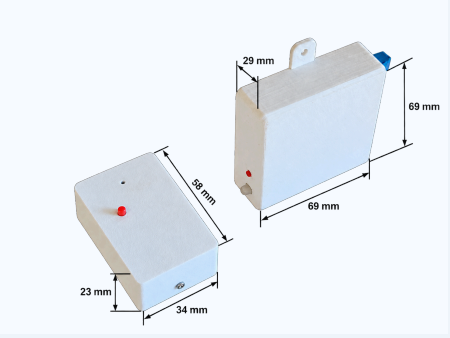
DATI TECNICI ESSENZIALI

Specifiche, sicurezza e gestione

Frequenza radio	433 MHz
Ingresso ricevitore	5 - 15 VDC
Uscita commutata	5 - 15 VDC / 3 A max
Telecomando	1 batteria AAA 1,5 V
Capacità memoria	512 consigliati / 1024 max
Autenticazione	HMAC-SHA-256; tag troncato a 128 bit
Anti-replay	contatore rolling crescente
Memoria	non volatile sul ricevitore

PROCEDURA LEARN / REMOVE

- LEARN + pressione del telecomando: il nuovo seriale viene memorizzato.
- Conferma aggiunta: 3 lampeggi lenti del LED sul ricevitore.
- Se il seriale è già presente, la stessa procedura rimuove solo quel telecomando.
- Conferma rimozione: 10 lampeggi veloci. Gli altri telecomandi restano abilitati.
- RESET memoria: pressione prolungata del comando dedicato cancella tutti i telecomandi.

SICUREZZA DEL PROTOCOLLO

Il ricevitore deriva una chiave dispositivo per ciascun seriale tramite HMAC-SHA-256. Nel firmware di produzione del trasmettitore è memorizzata solo la propria K_DEVICE, non la master key. I frame sono autenticati con HMAC-SHA-256 e tag di 128 bit. Il ricevitore memorizza il contatore accettato e respinge valori uguali o precedenti, contrastando il replay. La compromissione di un singolo trasmettitore non fornisce direttamente la master key né le chiavi degli altri trasmettitori.