DarkMOSC

(Versione 1.5)

by jack70

Attenzione! Questo firmware è stato scritto esclusivamente per fini educativi personali e viene distribuito gratuitamente.
E' illegale usarlo nei paesi dove E' PREVISTO il pagamento per ottenere gli stessi scopi.
Qualsiasi utilizzo a fini commerciali è strettamente proibito e può essere perseguito per legge.
L' Autore declina ogni responsabilità derivante da qualsiasi utilizzo di questo firmware.
Chiunque non accetta integralmente quanto sopra DEVE distruggerlo immediatamente.

Questo firmware è concepito per hardware Evil (ideato dal Visiva Group) o Piccard 2.

E' composto da un solo file DarkMOSC.hex poiché sono implementate le routine di AutoDetect e di AutoFormat dell'eeprom esterna, l'eeprom esterna è necessaria anche se non deve essere programmata.

INIZIALIZZAZIONE

Al primo reset otterrete l'ATR di livello 3 e quindi lo status 90 00 che vi indicherà l'avvenuta formattazione della Card 1. Se entro pochi secondi non avete ottenuto lo status allora inviate un nuovo reset (è un problema che può nascere con alcuni programmi che non attendono la risposta della card).
Se ottenete lo status 65 01 significa che l'eeprom esterna non è collegata correttamente.
A questo punto potete iniziare la personalizzazione a livello 3 con l'INS 0C, nella card infatti non è inizialmente presente nessun provider e nessuna chiave (vedi Appendice 1).
La chiave di sistema della card è: 6A 61 63 6B 37 30 20 21

Terminato l'inserimento dell'UA, del provider 0 e della back-door, potete tornare a livello 1 sempre con l'INS 0C e continuare ad editare la card come una qualsiasi MOSC.

Al primo avvio viene sempre formattata la Card 1, le altre card potranno essere formattate successivamente, abilitandole e mandando un reset.

STRUTTURA MULTICARD

E' possibile gestire più di una card a seconda del tipo di eeprom utilizzata:

24C32	Una sola Card
24C64	Due Card
24C128 o superiore	Quattro Card

Per ciascuna card possono essere gestiti 16 provider e sono disponibili 250 records.
Il passaggio da una card all'altra può avvenire con due diverse modalità: attraverso il selettore BCD o attraverso l'inserimento di opportuni codici da telecomando.

SELETTORE BCD E CONTROLLO MULTICARD

Posizione	**Utilizzo**
0	Modalità mista (o uscita modalità configurazione attraverso il selettore BCD)
1	Card 1
2	Card 2
3	Card 3
4	Card 4
5	Card 1 in modalità speciale
6	Card 2 in modalità speciale
7	Card 3 in modalità speciale
8	Card 4 in modalità speciale
9	Ingresso modalità configurazione attraverso BCD

Nella modalità mista il Parental Control funziona come una card originale eccetto per il codice 9999, inserendo questo codice si può infatti selezionare la Card voluta attraverso il codice successivo che deve essere compreso tra 0001 e 0008.

Questa modalità è concepita per le piccard 2 che non hanno un selettore BCD. Per poter editare una Card diversa dalla 1 senza selettore bisogna quindi editare la Card 1, inserire la scheda nel decoder, abilitare la Card desiderata attraverso l'uso della modalità mista, togliere la scheda dal decoder e seguire gli stessi passi fatti per editare la Card 1.

Nella modalità speciale il parental control invece è utilizzato per modificare le impostazioni della Card associata.

IMPOSTAZIONI DA TELECOMANDO

Se il vostro decoder non supporta l'inserimento da telecomando leggete l'Appendice 2.
Questa modalità di cambio configurazione funziona solo in modalità speciale.

Accensione 8 LEDs

8195	Attivazione
8451	Disattivazione

Accensione LEDs da 1 a 4

8193	Attivazione
8449	Disattivazione

Accensione LEDs da 5 a 8

8194	Attivazione
8450	Disattivazione

Funzione LEDs da 5 a 8

8196	Indicazione ultimo errore riscontrato
8452	Indicazione della chiave in uso

Inversione stato dei LEDs

8200	Inverte lo stato dei LEDs
8456	Stato normale

Funzione AutoPMB

Quando vi posizionate su un canale fuori dal PBM quest'ultimo si aggiornerà e al prossimo passaggio il canale sarà disponibile

N.B. Il record del PBM deve essere presente, la funzione non lo crea. Inoltre non è consigliabile usare questa funzione per creare un PBM da zero, poiché si potrebbero verificare incroci non reali.

8208	Attiva
8464	Disattiva

Funzione AutoCWP

8224	Attivazione (avvenuta la cattura si disabilita automaticamente e si accende il LED 4)

Funzione AutoRegionalCode

8256	Attivazione (avvenuta la cattura si disabilita automaticamente e si accende il LED 4)

Creazione registro BX

Il provider a cui verrà aggiunto sarà quello dell'ultimo canale visto

Se non vengono inseriti tutti i parametri il decoder darà errore nel codice PIN

Primo byte Event ID	Secondo Byte Event ID	Numero visioni	
4096(*),0001-0255	4096(*),0001-0255	0001-0255	8800

(*) al posto di 0000 va inviato 4096

Trasformazione records AX in BX

Il provider a cui saranno aggiunti sarà quello dell'ultimo canale visto

Se non vengono inseriti tutti i parametri il decoder darà errore nel codice PIN

Numero visioni	
0001-0255	9000

Cancellazione di tutti i records BX
Il provider è quello dell'ultimo canale visto

9300

Azzeramento codice PIN

9500

MODALITA' CONFIGURAZIONE CON SELETTORE BCD

Per entrare nella modalità di configurazione si deve porre a 9 il selettore BCD e inviare un reset alla Card, a questo punto inizieranno a lampeggiare i LEDs (se attivi) corrispondenti alle opzioni attivate:


Accensione LEDs da 1 a 4 (Posizione 1)


Accensione LEDs da 5 a 8 (Posizione 2)


Se acceso i LEDs da 5 a 8 indicano l'ultimo errore verificatosi, se spento indicano la chiave in uso (Posizione 3)


Inversione LEDs attiva (Posizione 4)


AutoPBM attivo (Posizione 5)


AutoCWP attivo (Posizione 6)


AutoRegionalCode attivo (Posizione 7)

Per modificare un'opzione basta posizionare il selettore sul numero corrispondente all'opzione che si vuole modificare ed infine inviare un reset alla card.

Per uscire dalla modalità configurazione basta selezionare 0 e inviare un reset alla card, a questo punto lampeggeranno tutti i LEDs attivi e a partire dal prossimo reset tutto tornerà normale.

CHIAVE IN USO


Chiave 00


Chiave 04


Chiave 08


Chiave 0C


Chiave 01


Chiave 05

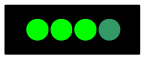

Chiave 09


Chiave 0D


Chiave 02


Chiave 06

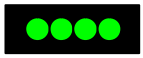

Chiave 0A


Chiave 0E


Chiave 03


Chiave 07


Chiave 0B


Chiave 0F

ERRORE


Errore generico


Data scadenza attraversata


Classe errata


Diritti non acquisiti


Istruzione non supportata


CWP non valido


Lunghezza errata

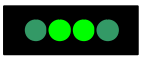

PIN errato

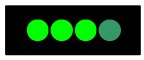

Errore signature

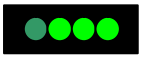

Fine della fase di preview

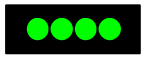

Provider non supportato


Regional Code non valido


Manca chiave primaria


Errore acquisto BX (01 o 02)


Manca chiave secondaria


Solo per provider 0

SIGNIFICATO LEDs DA 1 A 4

Ricezione e trasmissione

Errore nell'ultima istruzione ricevuta

Aggiornamento chiavi avvenuto

CWP trovato / Regional Code trovato

BUGs SIMULATI

1) Bugs INS 3C
2) Bug INS 32/34, l'estrazione delle chiavi può essere quindi fatta usando questo bug
3) Funny Bug

COMANDI SUPPORTATI

Questa versione supporta le seguenti istruzioni: 02, 04, 0E, 0A, 0C, 12, 16, 1A, 30, 32, 34, 36, 38, 3A, 3C, 40, 42, 48, 4A, 4C, 50, 54, 56, 5A, 5C, 7C, 8A.

I seguenti nanocomandi per l'INS 3C: 04, 12, 13, 15, 19, 27, 2C, 2D, 31, D1, 82, F1

I seguenti nanocomandi per l'INS 40: 01, 02, 03, 10, 11, 17, 18, 1D, 1E, 1F, 21, 22, 23, 24, 25, 26, 28, 30, 32, 33, 40, 41, 42, 43, 80, 90, 91, B0, D0, F0

DIFFERENZE TRA LA VERSIONE 1.0 E LA 1.1

BUGS CORRETTI

1. Risposta all'INS 1A corretta e migliorata
2. Corretta la lettura delle keys dopo un 901F
3. Corretta la gestione dei records Ax in multicard
4. Migliorata la visualizzazione della chiave sui leds da 5 a 8
5. Corretta e migliorata la gestione dei provider
6. Corretta e migliorata la simulazione del bug sulle INS 32/34
7. Correzioni varie

OTTIMIZZAZIONI

1. Velocizzate le routine di lettura e scrittura sull'eeprom esterna
2. Velocizzata la funzione di Encrypt

Ora la card risponde più velocemente (TimeOut consigliato: 150 ms)

NUOVE FUNZIONI

1. Gestione nano F1
2. Funzione di ricerca automatica del codice regionale

DIFFERENZE TRA LA VERSIONE 1.1 E LA 1.2

BUGS CORRETTI

1. Bug nano F0
2. Bug nano F1
3. Bug sul blocco del PBM
4. Bug nella cancellazione di una key duplicata
5. Correzioni varie

OTTIMIZZAZIONI

1. Migliorato l'AutoCWP
2. Migliorato l'AutoRegionalCode

DIFFERENZE TRA LA VERSIONE 1.2 E LA 1.3

1. Corretta la gestione delle INS non valide
2. Corretta la gestione del LEN a zero
3. Corretta la cancellazione dei record BX
4. Corretta l'estrazione delle keys
5. Migliorate le INS 04, 30, 7C
6. Migliorato il parsing dei nano nelle INS 3C e 40
7. Aggiunto nano 12
8. Aggiunto il nano 28
9. Aggiunto il nano 30
10. Migliorato il nano 19
11. Migliorato il nano 31

12. Aggiunti i nano 1D, 1E, 1F
13. Migliorati e ampliati i nano 42 e 43
14. Aggiunto il nano 2C (Records BX tipo 01)
15. Aggiunto il nano 15 (PPV a tempo e records BX tipo 02)
16. Aggiunto il nano 2D
17. Corretta e migliorata la gestione dei records E0

DIFFERENZE TRA LA VERSIONE 1.3 E LA 1.4

1. Corretta la cancellazione dei providers
2. Corretta la gestione dello status 9014
3. Corretta l'INS 02
4. Corretto il controllo su P1
5. Corrette le risposte in caso di LEN=00
6. Riscritta l'INS 32
7. Tolta la soprascrittura dei BX
8. Corretto il nano 28
9. Corretto l'inserimento dei BX da telecomando
10. Aggiunta la cancellazione degli AX durante la trasformazione in BX
11. Migliorata la gestione dei nano 19 e 31
12. Completata l'INS 38
13. Completata l'INS 36
14. Migliorata l'INS 0A
15. Migliorata l'INS 1A
16. Riscritte le routine di comunicazione. Aggiunto il supporto della ritrasmissione in caso di errore di parità e resa immune da disturbi la fase di ricezione.
17. Aggiunto il nano 18
18. Aggiunto il nano 33
19. Correzioni varie

DIFFERENZE TRA LA VERSIONE 1.4 E LA 1.5

1. Migliorato il nano 25
2. Migliorato il nano 26
3. Corretto il nano 2D
4. Corretto il calcolo degli indirizzi nell'INS 32
5. Corretta l'INS 3A
6. Corrette alcune risposte dell'INS 40
7. Corretti alcuni status dell'INS 3C
8. Corretti i nano 15 e 2C
9. Corrette le INS 04 e 7C
10. Corretta la gestione del PIN (ora sono gestiti tutti gli 8 bytes e non solo gli ultimi 2)
11. Correzioni e ottimizzazioni varie

JACK70

APPENDICE 1

Modifica UA:

```
C1 0C 00 00 08 00 XX UA UA UA UA UA UA
```

Inserimento provider e backdoor:

```
C1 0C 00 01 16 23 ID ID 90 KI XX XX XX XX XX XX XX XX 82+SIGNATURE
```

Chiave criptata e signature calcolata con la chiave `6A 61 63 6B 37 30 20 21`

Passaggio a livello 1:

```
C1 0C 00 03 00
```

Nome provider 0:

```
C1 40 00 0x 1A D0 NN NN NN NN NN NN NN NN NN NN NN NN NN NN NN NN
82+SIGNATURE
```

Creazione nuovo provider:

```
C1 40 00 0x 0C 23 ID ID 82+SIGNATURE
```

Start-Up record:

```
C1 40 00 0x 15 B0 01 xx xx xx xx xx xx xx xx xx xx xx 82+SIGNATURE
```

Lo start-up record è solitamente il primo record della card, conviene quindi creare inizialmente un MKx diversa dalla MK0 in modo da poterla poi cancellare per rendere così disponibile il record 1.

PPV record del provider 0:

```
C1 40 00 0x 15 B0 00 xx xx xx xx xx xx xx xx xx xx xx 82+SIGNATURE
```

E' solitamente il secondo record, conviene quindi inserirlo subito dopo essere passati a livello 1, quando cioè in memoria c'è solo la backdoor al primo record.

MK0 provider 0:

```
C1 40 00 0x 1D 90 F0 xx xx xx xx xx xx xx xx 91 50 xx xx xx xx xx
xx xx xx xx xx 82+SIGNATURE
```

Solitamente al 3° e 4° record.

Cancellazione backdoor:

```
C1 40 00 00 0B 10 KI 82+SIGNATURE(MK0)
```

Procedura consigliata:

Questo è solo un esempio, si può arrivare allo stesso risultato seguendo vie diverse.

1. Modifica UA
2. Inserimento provider 0 e backdoor MKx (x diverso da 0)
3. Passaggio a livello 1
4. Modifica del nome del provider 0
5. Creazione PPV record del provider 0
6. Creazione MK0 primaria e secondaria
7. Cancellazione backdoor
8. Creazione start-up record

Ora potete inserire ed editare nuovi provider utilizzando la MK0 del provider 0.

APPENDICE 2

OPZIONI SENZA TELECOMANDO E SELETTORE

Se il vostro decoder non supporta l'inserimento da telecomando potete comunque abilitare le opzioni previste inviando comandi manuali.

```
C1 3C 0p 0y 09 82+SIGNATURE

C1 30 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 XX XX
```

Dove XX rappresenta il codice in esadecimale e p l'indice del provider a cui è indirizzata l'opzione, il primo comando va inviato solo la prima volta dopo il reset della card e serve solo nel caso in cui si voglia utilizzare una funzione che fa riferimento ad un provider preciso.