DarkMosc MiniDoc

Questo piccolo manuale si prefigge lo scopo di aiutare coloro i quali, alle prime armi, si trovano in difficoltà nella creazione di un clone DarkMosc.

Pertanto questa guida è essenzialmente destinata ai principianti.
L'obbiettivo è quello di creare una DarkMosc il più possibile simile ad una carta originale; nell'esposizione ho quindi mantenuto un ordine nell'eseguire le varie operazioni in modo da ottenere una struttura dei record simile a quella presente nella mia carta originale.

Nella mia carta i record sono nel seguente ordine:
Provider00: Record 00 01= SECA Start-up Record
Provider00: Record 00 02= SECA PPV Record
Provider00: Record 00 03= Primary Key 00
Provider00: Record 00 04= Secondary Key 00
Provider00: Record 00 05= Activation Date
Provider01: Record 00 06= PPV Credit Record
Provider01: Record 00 07= Primary Key 00
Provider01: Record 00 08= Secondary Key 00
Provider01: Record 00 09= Package BitMap (PBM)
Provider01: Record 00 0A= Primary Key 01
Provider02: Record 00 0B= Primary Key 00
Provider02: Record 00 0C= Secondary Key 00
Ecc……

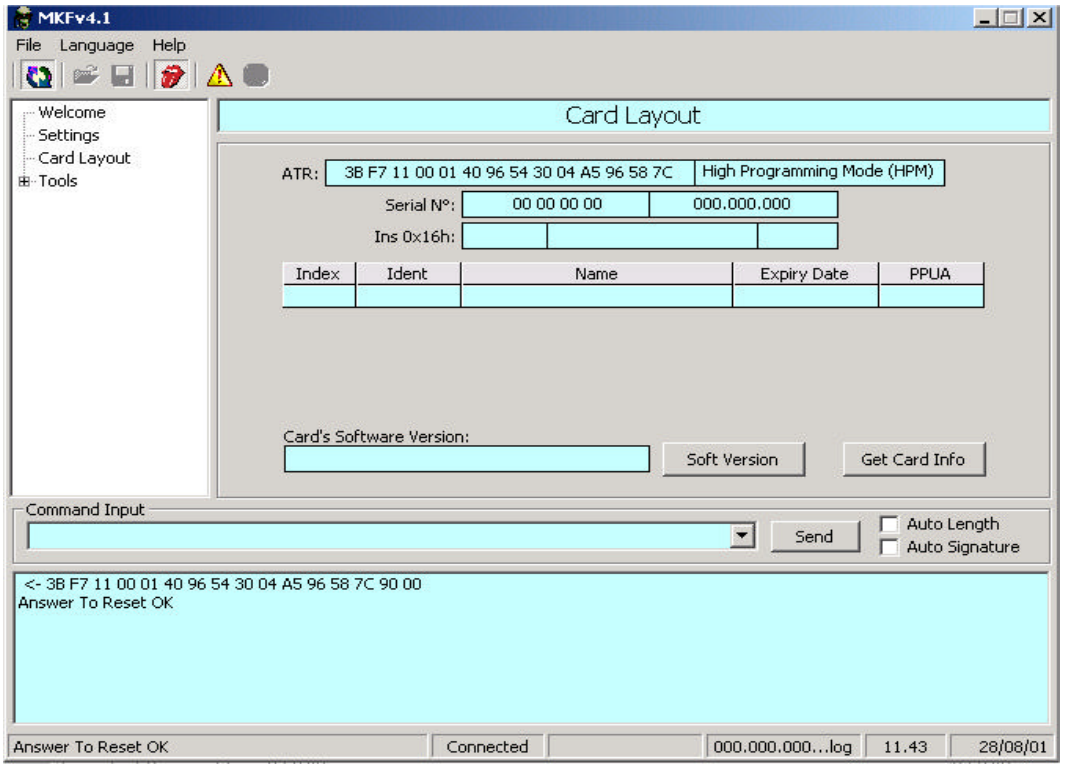
Se la Vostra scheda risultasse differente non resta che cambiare l'ordine nel quale verranno eseguite le varie operazioni

Hardware necessario:
Piccard2 o Evil o Silver
Ludipipo o simili con slot iso od adattatore per 16f876
Smartopo/Phoenix

Software necessario:
IC-Prog
MKFind 4.1 o superiori
(altri programmi possono essere usati in alternativa ad MKF, ma data la semplicità di utilizzo è da considerarsi particolarmente adatto anche ai principianti)

Per prima cosa è necessario programmare il 16f876 tramite ludipipo e IC-prog con il file HEX dei DarkMosc.
Non mi soffermerò sulla programmazione del 876 tramite IC-prog, ma do per scontato che tutti ne siano perfettamente all'altezza.
Non è necessario programmare la Eeprom in quanto sono implementate le routine di AutoDetect e di AutoFormat dell'eeprom esterna.

Una volta programmato il Pic inseriamo la carta nello smartopo ed eseguiamo MKF.
Clicchiamo su connect e ci troveremo nella situazione della figura sottostante:



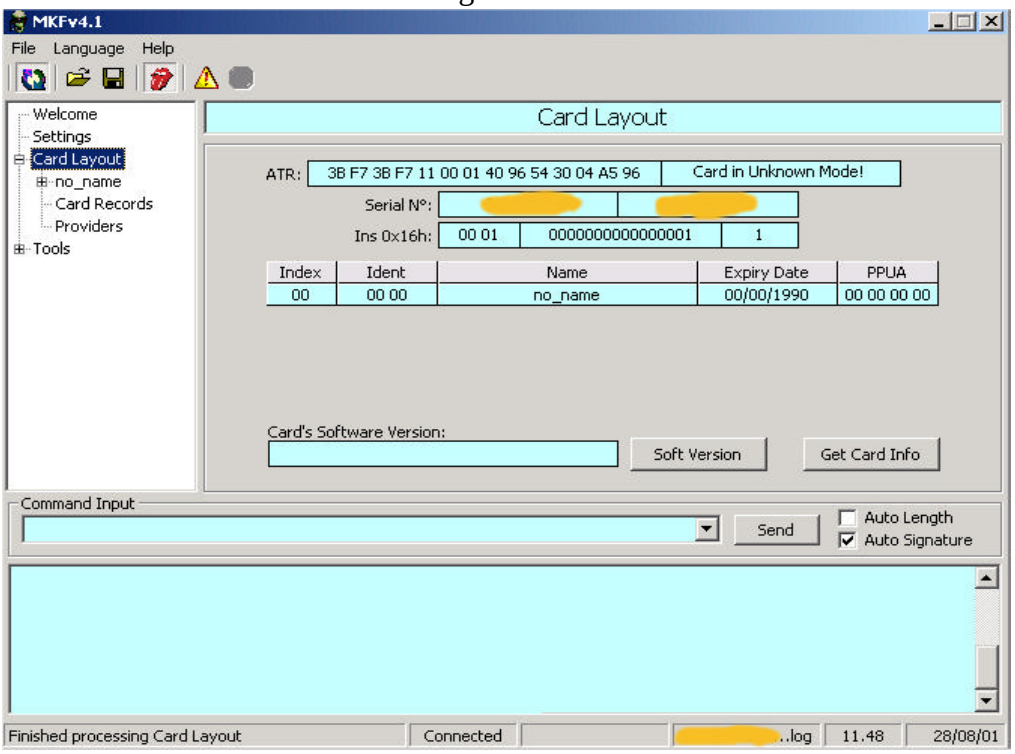
Se non dovesse comparire la modalità di programmazione avanzata, clicchiamo su reset e tutto dovrebbe funzionare.
Come si può notare la carta è sprovvista di UA e non è presente alcun provider (neppure il 00).
E' pertanto necessario inserirli (la carta risulta in questa modalità proprio per questa ragione).
Nella riga "Command Input" inseriamo pertanto:
`C1 0C 00 00 08 00 25 UA UA UA UA UA UA`
Dove UA…. è la nostra UA in formato HEX.
Clicchiamo quindi su send.
Ora inseriamo il provider 00 ed una backdoor.
Innanzitutto clicchiamo su Settings ed inseriamo la system key gentilmente fornitaci da Jack70:
`6A 61 63 6B 37 30 20 21`
Quindi all'interno della riga "Command Input" inseriamo il comando:
`C1 0C 00 01 16 23 ID ID 90 IK XX XX XX XX XX XX XX XX 82`
Dove ID ID è l'ident del provider (nel nostro caso 00 00), IK è l'indice della chiave (noi inseriremo 01) è XX…… è la nostra Backdoor (noi useremo 11 11 11 11 11 11 11 11 criptata con la chiave di sistema); dobbiamo poi abilitare la modalità "AutoSignature"; il nostro comando sarà pertanto:
`C1 0C 00 01 16 23 00 00 90 01 90 5F F7 B0 FC D0 2F 51 82`

N.B.: Come backdoor potete inserire anche qualunque altra cosa tanto, in questo caso MKF provvederà ad estrarla per voi e poi verrà cancellata in seguito.

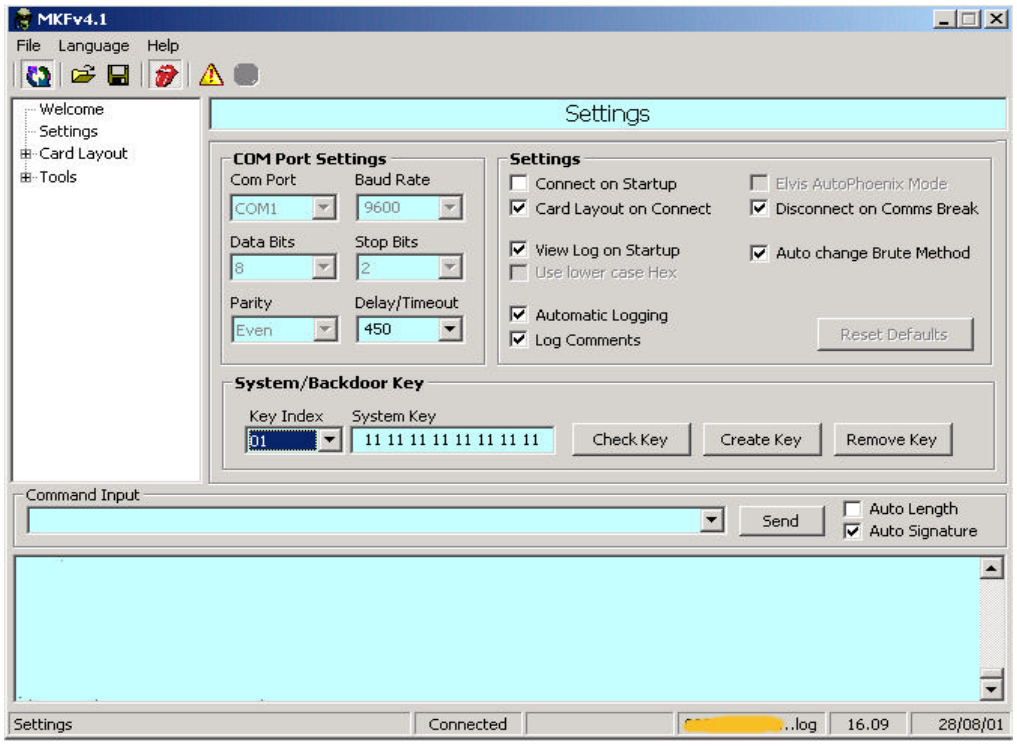
Ora clicchiamo su send.
Fatto questo possiamo riportare la carta in modalità utente; disabilitiamo la modalità "auto Signature" ed inseriamo il seguente comando nella riga "Command Input":

C1 0C 00 03 00
Clicchiamo su send.

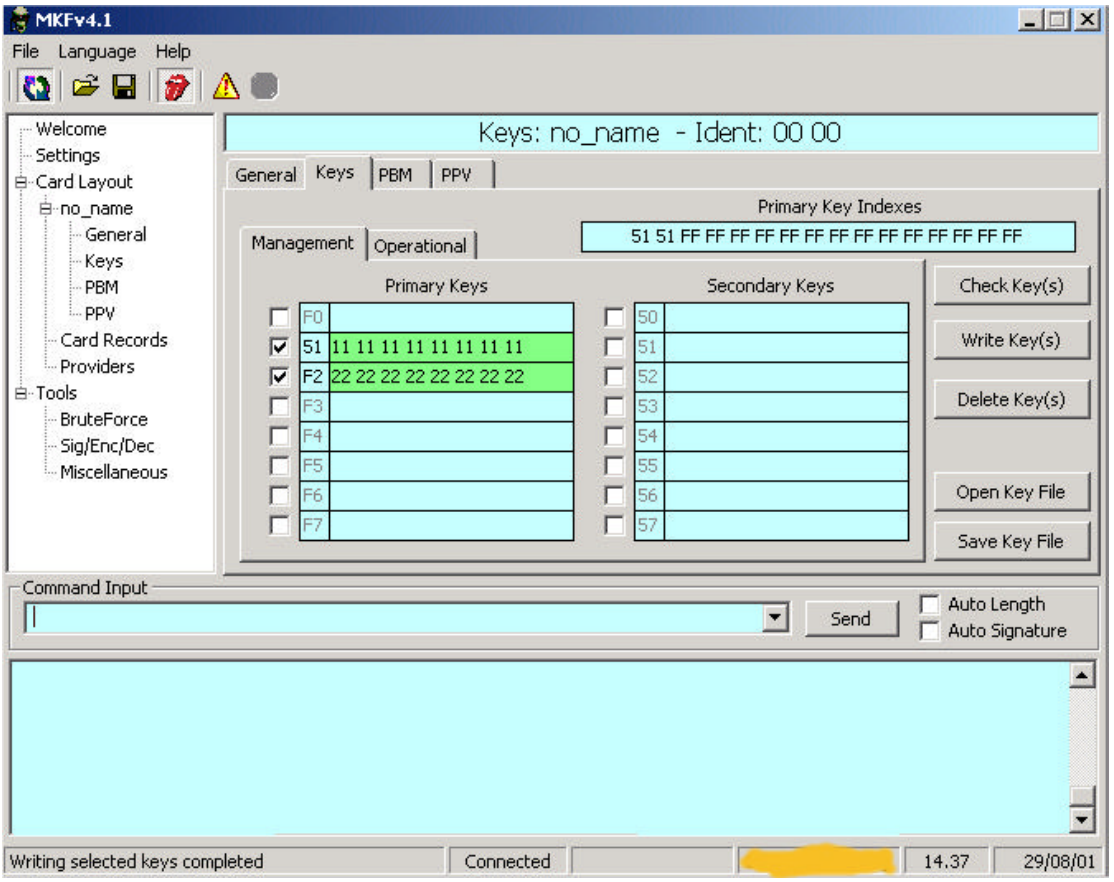
Disconnettiamoci e riconnettiamoci nuovamente per verificare che tutto abbia funzionato e ci ritroveremo nella seguente situazione:



Ora andiamo su settings e verifichiamo che la chiave 01 inserita funzioni correttamente; selezioniamo key index 01 ed inseriamo 11 11 11 11 11 11 11 11 come da figura e clicchiamo su chek key:



Una volta verificata la backdoor passiamo ad inserire un'altra chiave per il provider 00 (il motivo per cui dobbiamo creare un'altra backdoor è che abbiamo la necessita di scrivere nei primi due record della nostra DarkMosc il SUKA Start-up Record, il SUKA PPV Record, e quindi la Primary Key 00).
Il nostro scopo infatti è quello di creare una DarkMosc il più possibile simile ad una carta originale.
Selezioniamo il provider 00 andiamo nella sezione key ed inseriamo nel campo relativo alla chiave primaria 02 la chiave 22 22 22 22 22 22 22 22, quindi clicchiamo su write key.

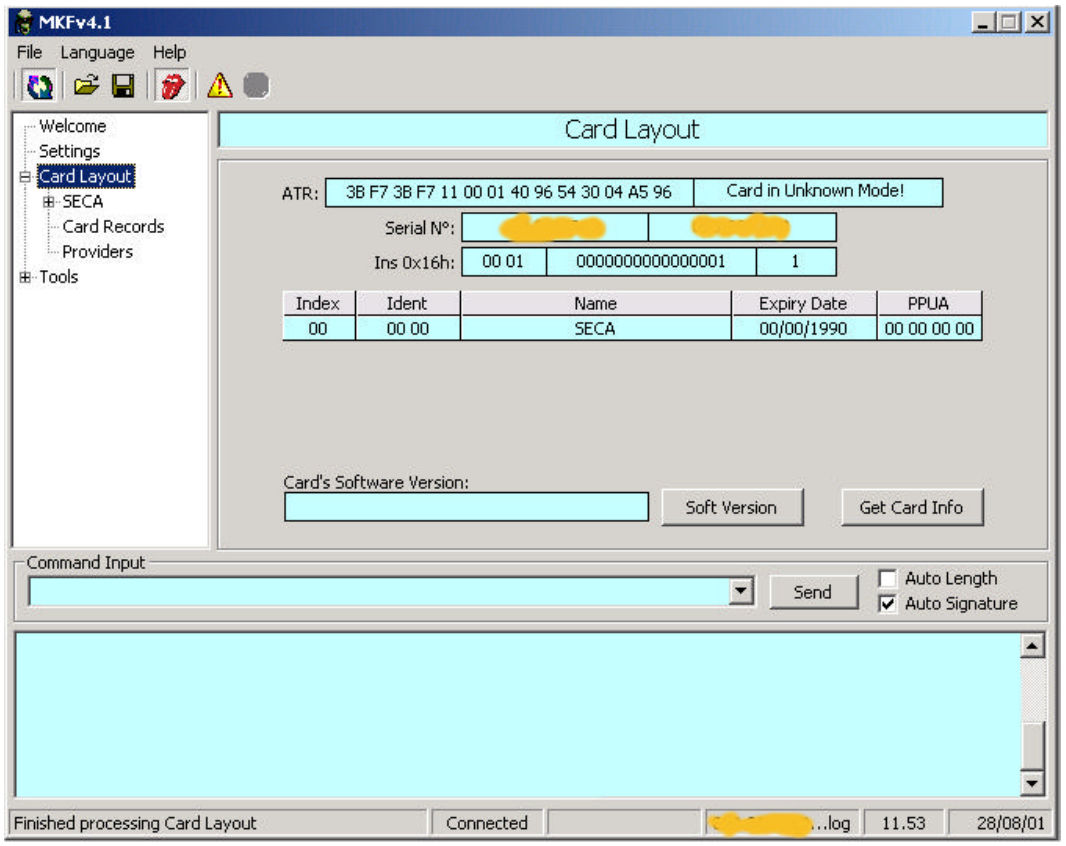


Una volta inserite le chiavi 01 e 02 possiamo inserire la chiave 00 che verrà quindi inserita nel record 03 della nostra DarkMosc come nella card originale.
Scriviamo nell'apposito campo della chiave 00 primaria la nostra chiave e clicchiamo su write key.

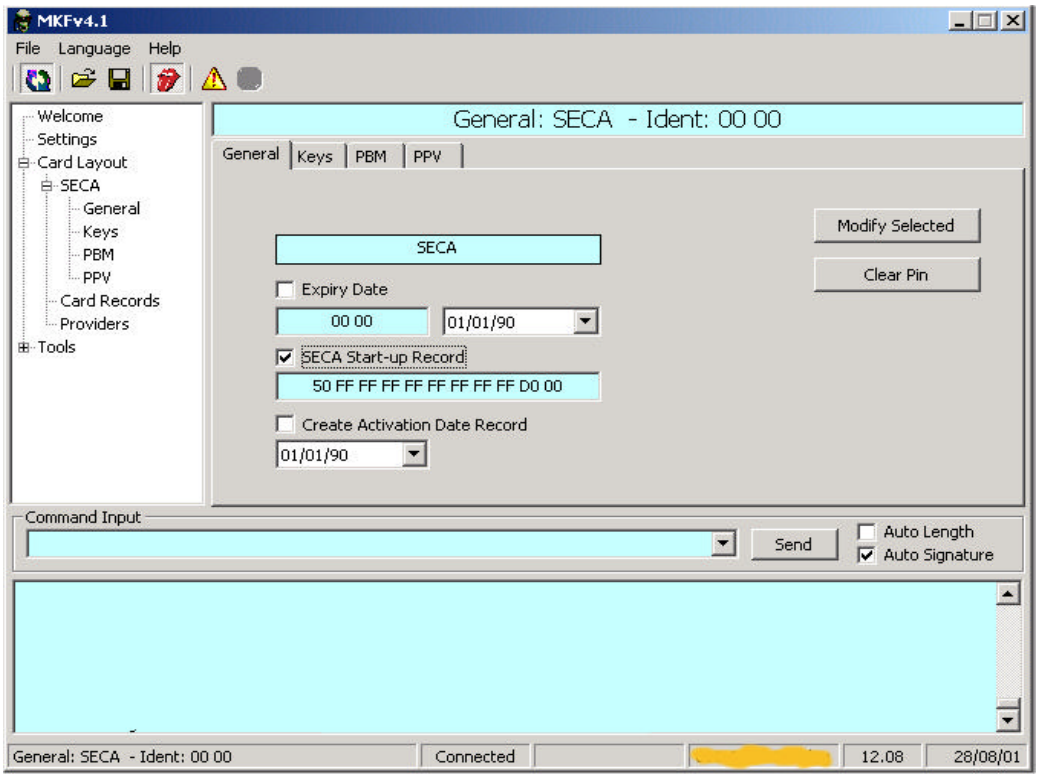
Dobbiamo ora eliminare le chiavi 01 e 02 per liberare i primi due record della DarkMosc.
Andiamo quindi di nuovo su settings selezioniamo key index 00 e ci comparirà la nostra chiave, clicchiamo su check key per verificarne la validità; una volta verificata disconnettiamoci e riconnettiamoci (è necessario la disconnessione e riconnessione delle carta altrimenti nelle prossime operazioni di eliminazione delle chiavi MKF sbaglierà a calcolare la signature).

Ritorniamo nella sezione key del privider 00 inseriamo le nostre key 01 e 02 e clicchiamo su delete key. Una volta eliminate ci troveremo con la nostra chiave 00 nel record 03 della DarkMosc e i primi due record liberi.
Ora possiamo quindi inserire il suka startup record.
Prima però possiamo cambiare il nome del provider 00 00 assegnandogli quello di default; come vedete infatti il provider 00 00 è inserito senza nome, pertanto dobbiamo assegnarlo; inseriamo nella solita riga “Command Input” il seguente comando:
C1 40 00 00 1D 24 00 00 D0 53 45 43 41 20 20 20 20 20 20 20 20 20 20 20 20 82

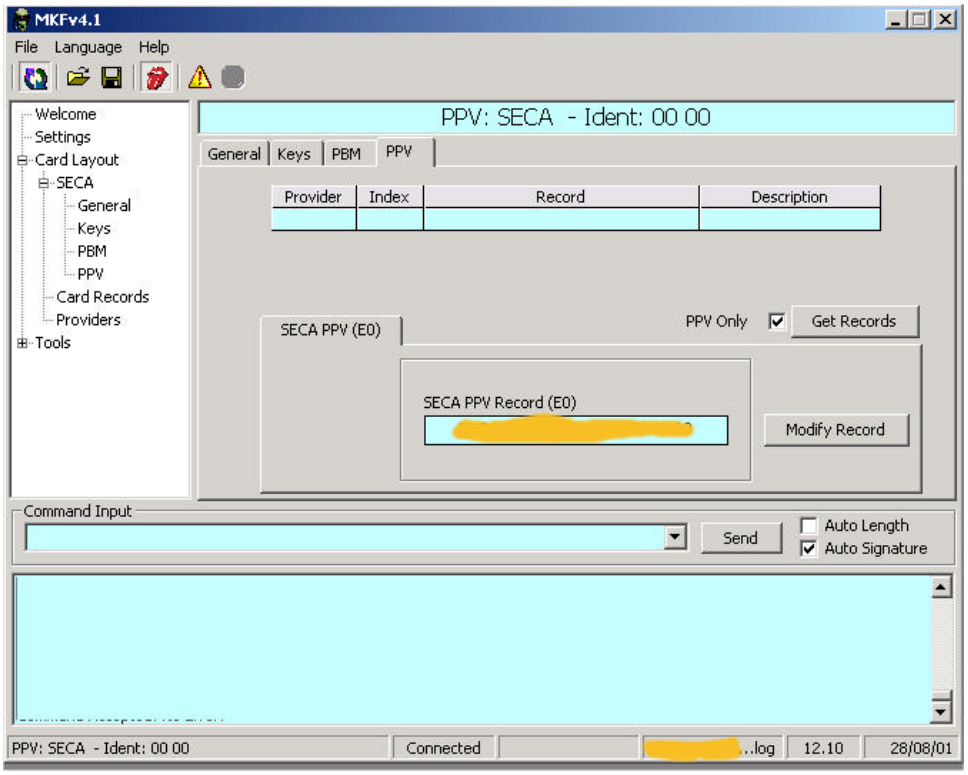
Sempre verificando che sia abilitata l’opzione “auto segnature” e clicchiamo su send.
Due click su connect/disconnect ed ecco la nuova situazione:



Inseriamo il suka startup record; clicchiamo su suka e su general:
nella riga startup record inseriamo il nostro record, spuntiamo la casella di modifica e clicchiamo su modify selected:

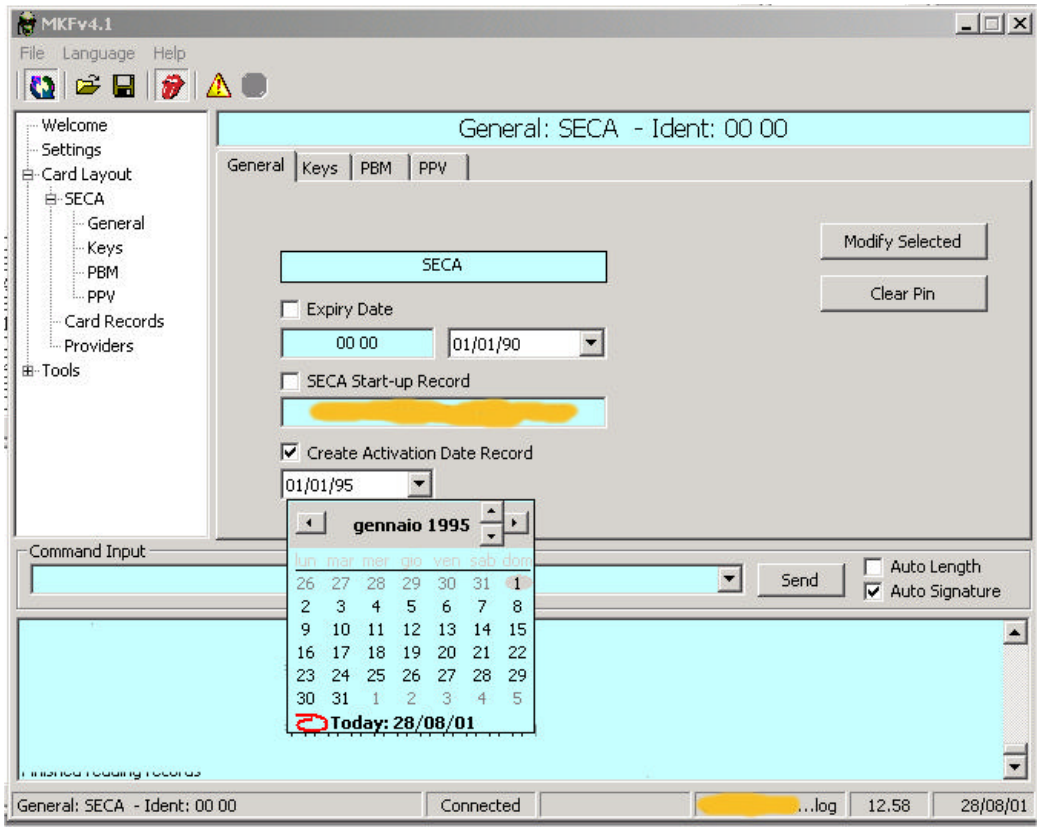


Inseriamo ora il suka PPV record; andiamo in PPV e nella riga PPV record 0E inseriamo il nostro record:

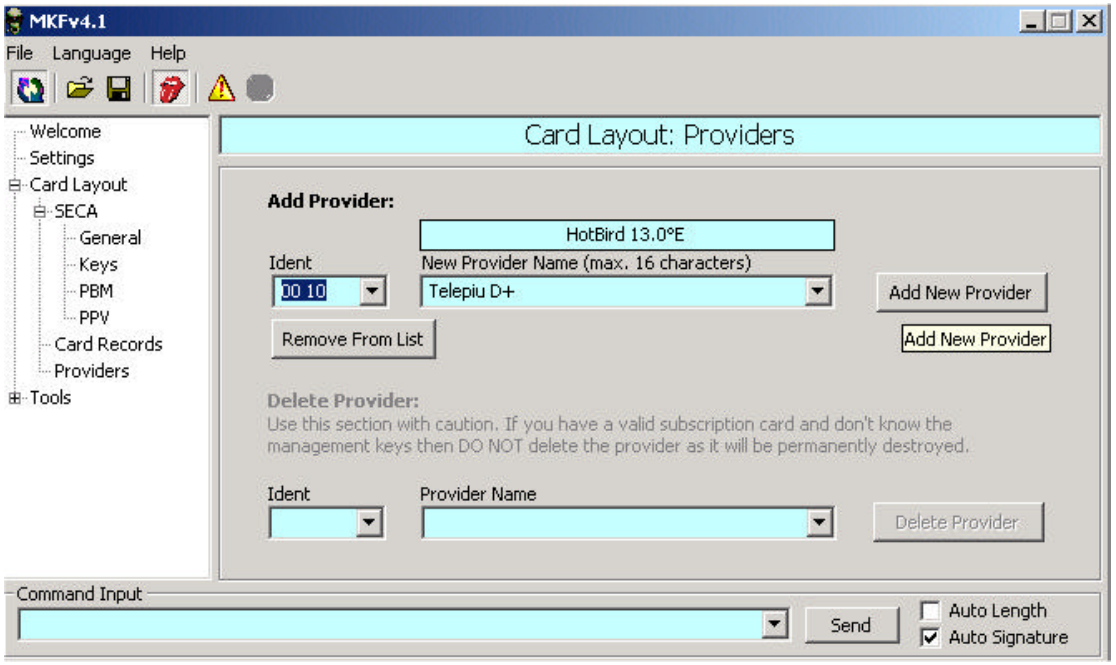


Clicchiamo su modify record.

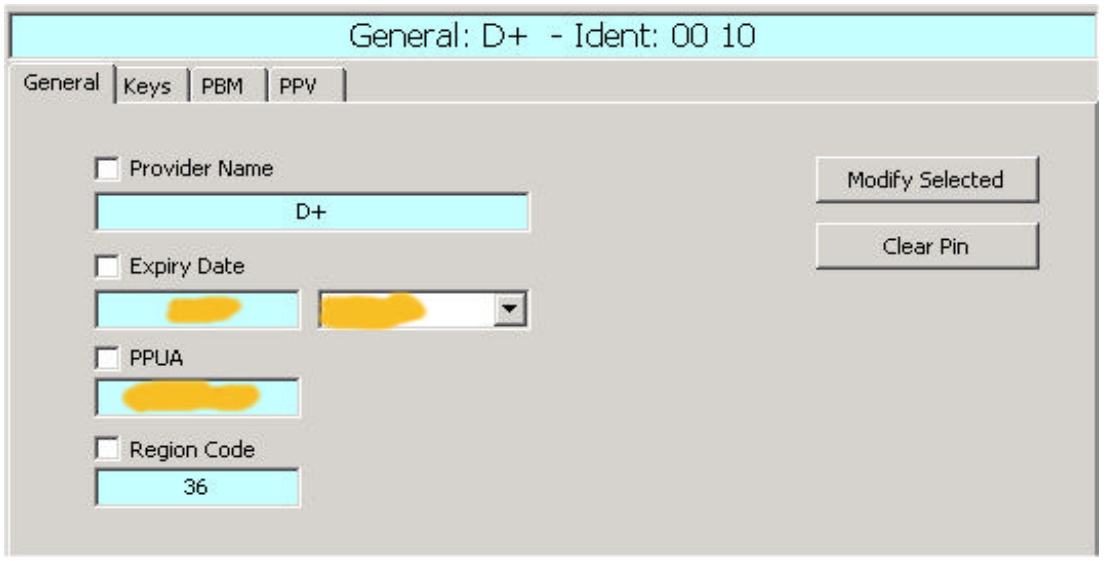
Bene ora ci troviamo con i primi tre record scritti delle nostra DarkMosc nel medesimo ordine della nostra scheda originale!!
Creiamo quindi la secondary key 00, nella sezione key del provider 00 inseriamo la key 00 secondaria e clicchiamo su write key.
Il quinto record è la data di attivazione, andiamo quindi nella sezione general del provider 00 ed inseriamola:



Bene bene il prov 00 è completato!!!
Possiamo passare ad inserire i prov che ci interessano!!
Cominciamo con D-
Andiamo in provider ed in add selezioniamo l'id di D- e clicchiamo su add new provider:



Andiamo quindi nella sezione general del nuovo prov creato e assegnamogli il nome.
Sulla mia scheda il primo record del prov01 è il ppv credit; inseriamolo;
nella solita “Command Input” digitiamo:
C1 40 00 00 11 24 00 10 43 dd dd 00 00 82
Dove:
dd dd è la data di acquisto dei gettoni in hex.
(Con questo comando acquistiamo 00 00 gettoni nelle data dd dd)
con la solita “auto segnature” abilitata, e clicchiamo su send.
Se sulla vostra scheda sono presenti dei gettoni acquistati modificate il comando di conseguenza.
Fatto questo inseriamo mk00 primaria e secondaria del prov D-, andando nella sezione key di tale prov, inserendo le key e ciccando su write key.
Inseriamo poi il PBM selezionando i byte a cui siamo interessati.
Fatto questo cambiamo il regional code (da 00 a 36) nelle sezione general del prov D- ed inseriamo la nostra PPUA, nonché la Expiry date:



Inseriamo poi la key primaria 01.
Inseriamo il prov +C***** e le sue chiavi nel modo analogo.
Completiamo con la key secondaria 01 di D- e le sue op key.

Bene abbiamo completato la nostra DarkMosc!!!!

Guybrush.

NDR.
Premetto che questo è solo uno dei metodi possibili per realizzare una DarkMosc, ma mi è sembrato abbastanza veloce semplici da realizzare per tutti; i ringraziamenti di rito vanno innanzitutto a Dark70 per lo splendido software che ha realizzato e poi a tutti quelli che hanno scovato i vari trucchi e soluzioni adottate in questo doc.
Io sono solo l'esecutore materiale di questo doc, ma non certo lo scopritore.