skyhardsat

SKYOPEN

HARDWARE

Wafer(bcd)Pic16F876+Eeprom24LC64/65+8Led(4Red+4Green)

PREMESSE

Lo SKYHARDteam non si ritiene responsabile dell' uso di questo progetto nei paesi dove la legge lo vieta , ne di danni da esso provocati a cose o persone in quanto progetto puramente a scopi di studio!!
La SKYOPEN e' una card a scopo sperimentale e come cio' va considerata , quindi sono bene accetti consigli , commenti e disponobilita' a fare test , non saranno pero' accettate in alcun modo critiche riguardo eventuali malfunzionamenti , non obblighiamo nessuno ad usarla!!!!
ATTENZIONE visto le continue mutazioni della SKYOPEN (essendo nel pieno del suo sviluppo!) si raccomanda di utilizzare sempre per ogni versione il prorpio bin allegato!!
Inoltre dalla vers.1.6 non e' piu' possibile utilizzare bin gia'editati in precedenza!!!

Inizio documento

CARATTERISTICHE TECNICHE

La SKYOPEN emula la decodifica del sistema Mediaguard/Seca e' quindi totalmente autoaggiornante (con key valide naturalmente) , supporta la Superencryption con key secondarie distinte e supporta tutti i vari aggiornamenti di dati PBM , REGIONAL–CODE , PPUA , DATE , MK , PK .
La SKYOPEN e' in grado di selezionare il Provider in uso con 2 metodi : tramite il nano 24 xx xx (INS 40) seleziona il Provider xx xx , in mancanza del nano 24 seleziona il Provider tramite il valore di P1 , e' anche in grado di riconoscere INS dirette a Provider non supportati e rispondere di conseguenza .
Dalla vers. 1.8 sono implementati tutti i controlli su tutti i valori ricevuti di tutte le INS supportate (P1-P2-P3LEN con tutte le lunghezze supportate , anche la 00H) e sulle INS in coppia anche il controllo sull'INS precedentemente processata !!
Gestisce il Pin-code (parental) come una smart card originale per la sicurezza dei nostri bimbi ☺.

Gestisce come una smart card i record 8x-Cx-Ex-Ax-Bx (con il pregio che facendo un dump dei record restituisce le key gia' in chiaro senza fare alcuna estrazione!!) , per ora sono gestiti solo simbolicamente i record Dx .
Sono disponibili in totale 128 record,quantita' a disposizione verificabile tramite INS 1A o meglio ancora tramite il magnifico BTMosk2.0 , i record sono gestisti in maniera dinamica (senza limiti per ogni Provider) tutta via esiste un limite , non si possono creare piu' di 64 Record PPV !!!
Quindi nessun limite per tutti gli altri Record fino ad un max di 128 , ma non piu' di 64 Record PPV (e' logico che se creo 120 Record 8x-Cx poi avro' solamente disponibili 8 record per la PPV).
Dalla vers. 1.8 gestisce i record PPV (Ax-Bx) come una SmartCard originale : Record Ax>quando un canale PPV prevede la fase di Preview la SKYOPEN controlla che non esistano record Bx su quest' Event e crea un record Ax attivando la fase di Preview e decrementanto il contatore di visione ogni Nano 19 processato su quest'Event , quando il contatore e' a zero fine fase di Preview (no-vision) i record Ax vengono cancellati automaticamente ogni volta che si visiona un canale Preview con data superiore a quelli memorizzati (vedi Secafaq) possono in oltre essere cancellati tramite Nano 28 oppure 18 !!!
Record Bx>i record Bx si creano tramite Nano 32 , la SKYOPEN gestisce i loro valori in pieno come l' originale : il contatore di visioni diminuisce ogni volta che si riceve un nano 31 con N° di diffusione diverso e aggiorna la data dell'ultima visone quindi , quando il contatore di visioni e' a zero (Status 90 26) , i Record Bx si possono cancellare tramite Nano 40 !!!!
Il Nano 32 puo' essere bloccato tramite apposito flag Nano 26 (vedi Secafaq) .
La SKYOPEN di default con la PPV funziona come un originale (Normal) e' possibile pero' portarla in modalita' (PPV-Free) , cioe' compra tutto , in questa modalita' la SKYOPEN funziona come le versioni precedenti : aquistando tutto e potendo memorizzare i Fake-Event per riconoscerli.
Per portare la SKYOPEN in modalita' PPV-Free vi sono i soliti 2 metodi : tramite (bcd) sfilando la card portando il commutatore rotativo sul 5 facendo uno infila-sfila e riportando il comm. nello stato precedente (se normale 0 , se Invisible-mode 3) , ora la card aquista tutto , per tornare in modalita' Normal basta ripetere la stessa operazione.
Tramite Pin-code e' ancora piu' semplice , naturalmente prendere le dovute precauzioni per l'uso dei pin , basta inserire il pin 4455 spegni-accendi ed e' in PPV-Free stessa operazione per riportare in Normal , qua' non serve neppure riportare lo stato di Invisible-mode , se attivato rimarra' inalterato !!!
ATTENZIONE i Fake possono essere tranquillamente memorizzati anche in modalita' Normal , naturalmente non verranno usati finche' non si portera' la card in modalita' PPV-Free !!!
Gestisce come una smart card gli Index key INS 1A !!!!
La SKYOPEN gestisce le INS 3C/40 controllando , la signature , la validita' delle key usate , la validita' della data , la validita' del PBM , la presenza di nano errati (INS 40-3C) e l'avvenuto processo del nano D1(INS 3C)ecc.ecc.
Inizio documento

GESTIONE

La SKYOPEN e' editabile totalmente come una smart card , quindi con la maggior parte degli editor per MOSC , tuttavia si consiglia MKFind & BTMosc !!!!! (I piu' testati).
Si possono modificare-verificare-cancellare MK,PK,PPUA,PROVIDER NAME,REGIONAL CODE,ACTIVACTION DATE,SECA START-UP,PPV RECORD-SECA ecc. ecc.
Si possono aggiungere e cancellare Provider (adegua automaticamente la posizione dei Provider , la risposta all' INS 16 , cancella tutti i dati riguardanti il Provider eliminato) .

Tramite apposito editor (SKYOPENeditor) e' possibile modificare Unique Adress !!
ATTENZIONE non scrivere key FF FF FF FF FF FF FF FF questa vi verra' accettata ma non verra'piu' trovata dalla card .
Dall'uscita dei nuovi (eccezionali) MKFind 4.4 e BTMosk 2.0 non serve modificare la velocita' per nessuna operazione basta lasciare 9600 Baudrate!!
Una particolarita' sta' nella gestione della BACKDOOR , nella card sono gia impostate queste (Provider 00):
MK00 : 53 4B 59 48 41 52 44 2A
MK02 : 53 4B 59 4F 50 45 4E 2A
Basta impostarle nell' apposita sez.(setting) dell'editor .
E'comunque possibile modificarle tranquillamente con degli accorgimenti,
mi spiego : per modificare ad esempio la BACKDOOR 02 devo impostare la 00 nella sez. (setting) , poi passare al Provider 00 (SECA) nella sez.
(Key) e scrivere la nuova BACKDOOR nella sua posizione , scriverla (con INS 40 oppure tasto scrivi) tornare nella sez . (setting) scriverla nella casella BACKDOOR con il suo index (02) e verificarla , per modificare la 00 fare l'operazione opposta , per aggiungerne usare lo stesso metodo !!! (non scriverla col tasto "scrivi" della sez. "setting" perche' non porterebbe alcun risultato !!)
Naturalmente e' possibile bloccare l'aggiornamento PBM (tasto "blocca" MKFind) ricordatevi pero' di sbloccarlo quando dovrete modificarlo . Dalla vers.1.6a si blocca per ogni Provider singolarmente quindi si puo' bloccare per un Provider e per un altro no!!
Si puo' verificare lo stato del blocco da INS 1A(vedi Seca faq)!!
Si puo' azzerare anche il Pin-code con apposito tasto , e' consigliabile tuttavia non tenere il Pin-code a 00 00 in quanto vi puo' dare problemi nell'uso delle funzioni speciali .
ATTENZIONE dalla vers.1.7 non e' piu' possibile azzerare il Pin-code con lo SKYOPENeditor , perche' e ' stato posizionato nell'Eeprom int. , si consiglia di usare MKFind (tasto "azzera") o qualsiasi editor per Mosc che invii un INS 40 con il Nano 03.
La SKYOPEN gestisce anche l'uso dei nano 01-02 che abilitano l'utilizzo o no del nano 24 per ogni provider distintamente!!!
Il nano 01 puo' essere bloccato tramite nano 26 , verificabile anche questo da INS 1A (per queste operazioni si consiglia vivamente se non siete expert di far riferimento al Seca faq , in quanto compromettono il normale funzionamento della card se non usate con coscienza!!!)

Inizio documento

FUNZIONAMENTO DEI LED

L'impiego dei led e' molto semplice !
Red-led >>informazioni generiche
Green-led >> key in uso
ATTENZIONE e' ora possibile disattivare i led portando il (bcd) sul 4 e facendo sfila-infila riportare poi il comm. nella posizione precedente , per riattivarli ripetere la stessa operazione.
Oppure tramite Pin-Code inserendo il pin 4444 spegni-accendi , per riattivarli ripetere la stessa operazione.

SIGNIFICATO dei RED-LED

CLASSE ERRATA!!!

INS ERRATA!!!

INS 40 OK (processata)

INS 3C OK(processata)

LEN ERRATA!!!

SIGNIFICATO dei GREEN-LED

Chiave 0C

Chiave 0D

Chiave 0E

Inizio documento

FUNZIONI SPECIALI

FAKE-EVENT

La SKYOPEN e' in grado di memorizzare ben 16 fake-event e di testarli con gli eventi ricevuti riconoscendo i fake e rispondendo di conseguenza .
Ci sono 2 metodi diversi : tramite commutatore rotativo (bcd) , a fake beccato (schermo nero) sfilare la card , posizzionare il bcd a 1 (che normalmente deve essere a 0) reinfilare la card e il gioco e' fatto .
Quando la eeprom avra' memorizzato 16 fake al prossimo li azzerera' automaticamente , tuttavia possono essere azzerati in ogni momento posizzionando il bcd a 2 e facendo uno sfila-infila .
ATTENZIONE ogni reset fatto con bcd a 1 comporta la memorizzazione dell'ultimo evento ricevuto e di conseguenza per la card diventa fake-event
L'altro metodo comporta l'uso di un Pin-code speciale 4411 che va inserito nella funzione decoder "modifica pin" e non "parental control" , il pin che viene usato per attivare la modalita' e' : "ENTER CURRENT PIN" e non "ENTER NEW PIN" quindi inserite il pin tutte le volte necessarie fin che il decoder chiede il pin corrente .

La card non memorizzera' questo pin e rispondera' "pin errato" , tutto ok sfila-infila e il fake e' catturato (se avete problemi a inserire il pin con "schermo nero" passate direttamente su un canale free-to-air).
Per azzerare i fake tramite Pin-code usare lo stesso metodo inserendo il pin 4422 , ATTENZIONE quando nella card il pin e' 00 00 il decoder memorizza il primo pin inserito senza chiedere il pin vecchio , quindi se per primo inserite un pin speciale non sara' piu' possibile usare il "parental control" quindi e' sempre consigliabile averlo modificato in precedenza .

Inizio documento

INVISIBLE MODE

L'invisible mode serve per dare la possibilita' di vedere i Provider che controllano la quantita' sulla card senza doverla rieditare , difatti quando esso e' attivato la card rendera' visibile solo i primi Provider ,
da 2 a max 4 (quantita' settabile da SKYOPENeditor) mentre in modalita' normale saranno visibili tutti , come si attiva : tramite bcd , basta posizionare il bcd a 3 sfila-infila ed e' attivo , per ritornare in normal mode riportarlo a 0 sfila-infila.
Tramite Pin-code stesso metodo per la funzione fake-event inserendo pero' il pin 4433 sfila-infila ed e' attivo , Pin-code 4400 sfila-infila e si ritorna in normal mode!!!ATTENZIONE non e'possibile intrecciare i 2 metodi se si attiva col bcd non si puo' disattivare col pin e viceversa , in invisible mode i Provider non visibili non potranno essere utilizzati si dovra' tornare in normal mode per utilizzarli (in maniera completa aggiornamenti ecc.)!!!
Quando l'invisible mode e' attivato rimarranno accesi i primi 2 Red-led !

Inizio documento

SPEED

Versione per Decoder con velocita' di 12800 Baudrate es. SONY!!
Ogni versione della SKYOPEN dalla 1.6 conterra' anche l'.hex della SPEED (il bin naturalmente e'universale!!!)

Inizio documento

INS SUPPORTATE

02-04-0A-0E-12-16-1A-30-32-34-36-38-3A-3C-40-42-48-4A-4C-50-54-56-5A-5C-7C-8A

NANO SUPPORTATI

01-02-03-04-10-11-13-15-17-18-19-21-22-23-24-25-26-27-28-2C-31-32-40-41-71-80-82-90-91-B0-D0-D1-F0-F1

Inizio documento

VERSIONI

Release 0→0.9 >>versioni test
Release 1.0>>versione interna
Release 1.1>>versione interna
Release 1.1a>>versione interna
Release 1.2>>prima versione pubblica "Fake-event"
Release 1.3>>"Invisible mode ,Index key INS 1A"
Release 1.4>>"controllo validita' key per crypt-decrypt , controllo signature INS 3C , aggiunti diversi Status byte"
Release 1.5>>"controllo avvenuto processo nano D1/INS 3C , migliorata la gestione degli Index key per INS 1A"

Release 1.5a>>"piccole migliorie riguardanti le funzioni da Pin-code"
Release 1.6>>"Implementato l'interfacciamento con eeprom interna del Pic , implementata cancellazione Provider , implementato controllo errori su diversi nano , implementato controllo Date nano 27/INS 3C , implementato controllo PBM nano 13/INS 3C anti attakko , diverse migliorie"
Release SPEED>>Versione per decoder che funzionano a '12800'Baudrate (SONY)
Release 1.6a>>"Implementati nano 01-02 e modificato nano 26 (non piu'universale!) , modificata anche INS 1A rendendo visibili gli offset 0x19-0x1B del Provider indirizzato , migliorata INS 32/34 , INS 38 e Nano 13 , in fine perfezionata la versione SPEED eliminando quegli Status-byte sporchi che rispondeva!!"
Release 1.6b>>Risolto ultimo attacco INS 34/34 Record Ex 03 (release volante ☺)
Release 1.7>>"Implementata la gestione dei record totale per 8x-Cx-Ex parziale per gli altri!!Stabilizzata la velocita' del Pic,implementati diversi controlli su esistenza record , su valori ricevuti di P1-P2-LEN ecc.
Implementati Nano 11-22 e varie INS particolari ecc."
Release 1.7a>>"Sistemati i bug sulla scrittura record Ex e lettura PBM con len=0AH , perfezionati i controlli sui valori dell'INS 30 , migliorata risposta INS 4A (essendo un dump con lunghezze enormi oltre 59H puo' andare a leggere quella parte di eeprom che contiene l'ATR , e' normale !!!!) , risolto bug Nano 04 cartelli di attesa , risolto bug PBM canali F1 , stabilizzato l'Invisible-mode da telecomando (fateci sapere che adesso funge garantito!!). "
Release 1.7b>>"Risolto ultimo attacco nano 15 senza nano 2C"
Release 1.8>>"Implementata la gestione dei record Ax & Bx come SmartCard originale con gestione di tutti i Nano connessi : Nano 18-28-31-32-40 ecc. con possibilita' di portare la SKYOPEN in modalita'PPV-Free (compra tutto!) con pin 4455 oppure posizionando il (bcd) a 5 ogni volta che si verifica questo stato la SKYOPEN cambia modalita' (Normal-PPVFree).
Gestita' anche l'autorizzazione al Nano 32 , implementati tutti i controlli possibili sui valori di tutte
le INS (p1 , p2 , LEN con tutte le lunghezze possibili , anche la 00H!!).
Implementata gestione del Nano F1 come SmartCard e migliorati vari Nano con il controllo dell'INS per cui e' processato!!
Implementati vari controlli sulle INS 40-3C e Nano processati in esse con Status-byte adeguati in caso di errore!!
Aggiunte altre INS particolari:INS 7C , 48 ecc. , aggiunta disattivazione-attivazione LED tramite pin 4444 oppure (bcd) posizionandolo sul 4 !!"
Inizio documento

TANKS

Special tanks for Antotracer&VISIVA-GROUP e for PICC2RDteam per i loro asm pubblici che sono stati bibbia per noi e in particolare l'asm della SIMPLE-Card che e' stato base di studio per la progettazione della SKYOPEN !!!!
Un grazie anche all'amico Parsec che collabora molto attivamente nel Forum al nostro progetto !!
Inizio documento

DEDICHE

Dedichiamo e intitoliamo la SKYOPEN all'amico OPEN web-master di Opensat che ci ha ospitato e dato modo di conoscerci nella sua chat , nei primi tempi del suo sito "bei tempi quelli!!!"☺☺☺
Un saluto anche alla nostra Paoletta e Jeppy che ci tengono compagnia e ci sopportano ☺ nelle nostre lunghe chiaccherate notturne , un saluto anche agli amici del forum di AliceCooper !!

LINK

Aspettiamo suggerimenti e rispondiamo alle vostre curiosita' su tutti i nostri progetti sui forum "SKYHARDteam"&"SKY studio": http://www.la-splendente.com/forum/
Per il download dei progetti: http://members.xoom.virgilio.it/_XOOM/skyhardsat/index.htm

SKYHARDteam

Canzian_red >>very-expert SECA
Cavallopazzo>>SECA Tester
Chopperix >>Assembler-man & IRDETO expert
Maxx >>Vbasic expert-editor

E' nato anche un gruppo di studio sul nostro Forum con cui collaboriamo per la realizzazione di un Editor per la SKYOPEN e per MoscSeca "SKYHARDgroup" quindi grandi novita' anche in questo senso !!

SKYHARDgroup

Canzian_red >>very-expert SECA
Maxx >>Vbasic expert-editor
Chopperix >>Assembler-man & IRDETO expert
HTB
MaoTheBug
Ignazio
Ilsank

"Alla prossima!"SKYHARDteam.

Inizio documento