

ROCKEY4ND

Guida all'uso



Versione 1.2-it
FEITIAN Technologies Co., Ltd.
Copyright © 1999-2005

Distributore per l'Italia:
Partner Data srl

Via Olivari, 9 – 20131 Milano
info@partnerdata.it

FEITIAN Technologies Co., Ltd.

Software Developer's Agreement

All Products of FEITIAN Technologies Co., Ltd. (FEITIAN) including, but not limited to, evaluation copies, diskettes, CD-ROMs, hardware and documentation, and all future orders, are subject to the terms of this Agreement. If you do not agree with the terms herein, please return the evaluation package to us, postage and insurance prepaid, within seven days of their receipt, and we will reimburse you the cost of the Product, less freight and reasonable handling charges.

1 **Allowable Use** – You may merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide. You may make archival copies of the Software.

2 **Prohibited Use** – The Software or hardware dongle or any other part of the Product may not be copied, reengineered, disassembled, decompiled, revised, enhanced or otherwise modified, except as specifically allowed in item 1. You may not reverse engineer the Software or any part of the product or attempt to discover the Software's source code. You may not use the magnetic or optical media included with the Product for the purposes of transferring or storing data that was not either an original part of the Product, or a FEITIAN provided enhancement or upgrade to the Product. You may not Transmit Any part of THE SOFTWARE in your public servers.

3 **Warranty** – FEITIAN warrants that the dongles and Software storage media are substantially free from significant defects of workmanship or materials for a time period of twelve (12) months from the date of delivery of the Product to you.

4 **Breach of Warranty** – In the event of breach of this warranty, FEITIAN's sole obligation is to replace or repair, at the discretion of FEITIAN, any Product free of charge. Any replaced Product becomes the property of FEITIAN.

Warranty claims must be made in writing to FEITIAN during the warranty period and within fourteen (14) days after the observation of the defect. All warranty claims must be accompanied by evidence of the defect that is deemed satisfactory by FEITIAN. Any Products that you return to FEITIAN, or a FEITIAN authorized distributor, must be sent with freight and insurance prepaid.

EXCEPT AS STATED ABOVE, THERE IS NO OTHER WARRANTY OR REPRESENTATION OF THE PRODUCT, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1 **Limitation of FEITIAN's Liability** – FEITIAN's entire liability to you or any other party for any cause whatsoever, whether in contract or in tort, including negligence, shall not exceed the price you paid for the unit of the Product that caused the damages or are the subject of, or indirectly related to the cause of action. In no event shall FEITIAN be liable for any damages caused by your failure to meet your obligations, nor for any loss of data, profit or savings, or any other consequential and incidental damages, even if FEITIAN has been advised of the possibility of damages, or for any claim by you based on any third-party claim.

2 **Termination** – This Agreement shall terminate if you fail to comply with the terms herein. Items 2, 3, 4 and 5 shall survive any termination of this Agreement.

Informazioni varie

World Wide Web:

www.rockey.it

www.FTsafes.com

FEITIAN Technologies Co., Ltd.

Tel: +86-10-62304466 Fax: +86-10-62304477 Email: world.sales@Ftsafe.com Add: Bldg 7A, 5th Floor, Xueyuan Road 40, Haidian District, Beijing 100083, P.R China

Partner Data srl

Tel: +39-02-26147380 Fax: +39-02-45477406 Email: info@partnerdata.it
Via P. Marocco, 11 – 20127 Milano - Italy

Inviare i vostri commenti, suggerimenti o domande relative a questo documento a info@partnerdata.it

Version	Date
1.1 it	2007.10

CE Attestation of Conformity



ROCKEY is in conformity with the protection requirements of CE Directives 89/336/EEC Amending Directive 92/31/EEC. ROCKEY satisfies the limits and verifying methods: EN55022/CISPR 22 Class B, EN55024: 1998.

FCC Standard



This device is in conformance with Part 15 of the FCC Rules and Regulation for Information Technology Equipment. Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



USB

This equipment is USB based.

Quick Start

- 1 Tutte le chiavi ROCKEY menzionate in questo documento sono chiavi ROCKEY4ND o NetROCKEY4ND (quando specificato). Quanto descritto per ROCKEY4ND vale anche per NetROCKEY4ND salvo diversamente specificato; tuttavia per NetROCKEY4ND rimandiamo alla specifica Guida Operativa
- 2 ROCKEY4ND è una chiave driverless, non richiede l'installazione di alcun driver per essere usata. Il sistema operativo ha i driver di ROCKEY4ND inseriti nel sistema. Forniamo tuttavia i driver per Windows 98, nella omonima directory, perché tale sistema operativo necessita di questi driver.
- 3 Viene fornito agli sviluppatori di software un Software Developer's Kit (SDK) per le loro valutazioni. Lo SDK contiene quanto serve per valutare il sistema di protezione del software: il CD-ROM con il sw, la documentazione operativa e una chiave demo ROCKEY4ND. La chiave demo ROCKEY4ND è esattamente la stessa della versione commerciale del prodotto, con tutte le stesse funzioni e con una unica diversità: le password cablate nella chiave dello SDK sono pubbliche (P1:C44C, P2:C8F8, P3:0799, P4:C43B). Se dopo la valutazione deciderete di utilizzare il prodotto, acquisterete chiavi con password uniche e segrete, cosicché altri non possano leggere e/o modificare il contenuto delle vostre chiavi. Non usate la chiave demo per proteggere il vostro software poiché tutti possono acquistare chiavi demo. Le chiavi demo servono solo per valutare il sistema ROCKEY4ND.
- 4 Per utilizzare la chiave ROCKEY4ND, non dovete installare alcun driver. Dovete solo copiare le librerie (Rockey4ND.dll e eventuali librerie specifica di linguaggi di programmazione) nella stessa directory della vostra applicazione.
 - ☐ Trovate i tool di ROCKEY4ND, quali il ROCKEY4ND Editor e il programma Envelope Encryption, nella directory ROCKEYND/Tools nel CD-ROM.
- 5 RyEnv32_ND.exe è il programma Envelope Encryption. Vi permette di proteggere una vostra applicazione senza scrivere alcuna istruzione: selezionate il vostro programma da proteggere Win32 (EXE/DLL/ARX) e quindi proteggerlo con la Envelope. (Vedere il Capitolo 6-- ROCKEY4ND: Protezione tramite Envelope)
- 6 Rocky4ND_Editor.exe vi permette di scrivere, modificare, provare, il contenuto della chiave.
- 7 Rocky4RU.exe è il programma per aggiornare in modalità remota la chiave ROCKEY4ND. Lo sviluppatore del sw può usare questo tool per far eseguire direttamente dall'utente un aggiornamento del contenuto della chiave.
- 8 DataRecorder.exe fornisce un sistema di gestione delle chiavi utilizzate. Grazie a DataRecorder.exe, il programmatore può registrare i dati della singola chiave, informazioni sullo hw, le password, e altre informazioni della singola unità. Il database che contiene tutte queste informazioni aiuta gli sviluppatori a controllare i vari rilasci e i relativi utenti.
- 9 Le librerie API di ROCKEY4ND sono il tool ideale per utilizzare a pieno le funzioni di sicurezza di ROCKEY4ND nelle vostre applicazioni. Potrete imparare rapidamente ad utilizzare le API grazie anche agli esempi forniti per i vari linguaggi.
 - ☐ Esempi per diversi linguaggi di programmazione si trovano nella directory Samples. La cartella Beginner in Samples fornisce un esempio completo, passo-passo, per ben capire le funzioni disponibili con ROCKEY4ND.
- 10 Visitate il sito <http://www.FTsafe.com> (inglese) o <http://www.rockey.it> (italiano). Sono spesso aggiornati per fornirvi utili informazioni e gli ultimi rilasci del software.

Indice

Capitolo 1 Concetti base.....	6
1.1 ROCKEY4ND	6
1.2 Il meccanismo di protezione di ROCKEY4ND	7
1.3 I vantaggi di ROCKEY4ND.....	7
1.4 Come scegliere la giusta soluzione per la protezione	8
Capitolo 2 Funzioni Hardware di ROCKEY4ND	9
2.1 Struttura Interna di ROCKEY4ND	9
2.2 Interfaccia HW di ROCKEY4ND	9
Capitolo 3 Installazione dello SDK ROCKEY4ND	10
3.1 Contenuto del CD-ROM	10
3.2 Installazione dello SDK	10
3.3 Disinstallazione dello SDK	13
Capitolo 4 Nozioni base per i progettisti.....	14
4.1 Password.....	14
4.2 Codice Cliente	14
4.3 Identificativo Hardware	14
4.4 User Data Zone.....	14
4.5 Module Zone.....	15
4.6 User Algorithm Zone	15
4.7 User ID	15
4.8 Numeri Random.....	15
4.9 Seed e Return Values	15
Capitolo 5 ROCKEY4ND Editor	16
5.1 Breve introduzione.....	16
5.2 Operazioni	19
5.3 Salvataggio della videata	25
5.4 Log File e File Setting	25
5.5 Versione dell'editor.....	26
Capitolo 6 ROCKEY4ND: Protezione Tramite Envelope.....	27
6.1 Protezione di applicazioni PE (.exe/.dll).....	28
6.2 Protezione di applicazioni .NET più file	30
6.2 Protezione di file dati.....	31
Capitolo 7 ROCKEY4ND API.....	32
7.1 Esempi di utilizzo di API	33
7.2 Consigli per la massimizzare la sicurezza	33
Capitolo 8 ROCKEY4ND Algoritmi Hardware.....	34
ROCKEY4ND Specifiche tecniche.....	35

Capitolo 1 - Concetti Base

1.1 ROCKEY4ND

ROCKEY4ND è un avanzato sistema di protezione del software: una piccola chiave che va inserita in una porta USB del computer. La vostra applicazione potrà essere duplicata, ma funzionerà solo se la opportuna chiave ROCKEY4ND è collegata al computer. Può anche solo limitare l'uso del vostro programma ad un certo numero di esecuzioni e di alcuni moduli. La vostra applicazione interagirà con ROCKEY4ND all'avvio e durante il suo utilizzo. Se la chiave viene rimossa o se un modulo del programma è stato utilizzato per un numero di volte oltre il previsto, verrà evidenziato un messaggio di errore e l'applicazione si chiuderà o eseguirà altre operazioni (attivare una modalità demo o limitare certe funzioni.) in conformità al contratto di licenza d'uso che avrete previsto.

ROCKEY4ND è molto versatile e può essere applicato a diversi scenari contrattuali. Per esempio:

- **Prova e poi acquista:** potete limitare l'uso di un programma ad un certo numero di esecuzioni, superato il quale il programma (o alcune funzioni) non si attiverà più. Se poi il cliente vorrà acquistare la licenza d'uso, basterà aggiornare remotamente il contenuto della chiave, tramite l'invio di un piccolo eseguibile, per riattivarne l'uso.
- **Paga quanto consumi:** potete consegnare il programma con un limitato numero di esecuzioni prepagate; quando saranno state consumate, il cliente ne acquisterà altre e con il programma di aggiornamento remoto gliele riattiverete.
- **Paga per quello che ti serve:** potete offrire un costo differenziato della licenza d'uso a seconda delle funzioni selezionate dal cliente; sempre tramite l'aggiornamento remoto potrete poi attivare altre funzioni che il cliente richieda nel prosieguo dell'utilizzo.
- **Paga per quanti utenti utilizzano il programma:** grazie alla chiave di rete NetROCKEY4ND potete inserire nelle sue memorie il numero massimo di utenti contemporanei che possono utilizzare quel programma; il cliente pertanto può acquistare la licenza limitatamente ai suoi utenti; e potrete sempre ampliare tale numero inviando l'aggiornamento alla chiave tramite il programma di remote update.
- **Paga per quanto tempo vuoi usare il programma:** conteggiando il tempo d'uso e via via addizionandolo nelle memorie della chiave, potrete concedere licenze dei programmi limitate nel tempo d'utilizzo (ad esempio 50 ore). Quando il tempo d'uso previsto sarà scaduto, potrete riattivare per un altro periodo l'uso dell'applicazione semplicemente aggiornando i dati contenuti nella chiave tramite il programma di remote update..

A differenza di altri prodotti concorrenti, ROCKEY4ND è un potente computer in miniatura, con una sua CPU, memoria e firmware specialistico per permettere una sicura interazione con la vostra applicazione. Potete scrivere complessi algoritmi che verranno registrati in modalità sicura nella chiave, e poi far richiamare tali algoritmi in vari momenti dall'applicazione. Questa metodologia di protezione è fortemente raccomandata perché è molto difficile superarla. ROCKEY4ND è progettato per realizzare altissimi livelli di sicurezza ed è abbastanza facile raggiungere questi livelli di protezione. Le librerie API di ROCKEY4ND sono state semplificate ed ottimizzate sulla base dell'esperienza maturate con le altre versioni di chiavi Rockey. Tuttavia un notevole livello di protezione si raggiunge in pochi attimi e con estrema facilità con il programma Envelope, senza scrivere alcuna istruzione.

Envelope cifra i file eseguibili di Windows (quali .dll, .exe e .arx) ed è così semplice da essere usato in pochi secondi. La ROCKEY4ND Envelope è la soluzione ideale se non possedete il codice sorgente dell'applicazione da proteggere o

se non volete mettervi a scrivere delle istruzioni. Una protezione che combini API e Envelope offre il più elevato livello di protezione raggiungibile..

Il sistema di protezione ROCKEY4ND fornisce vari componenti che vengono presentati in questo documento. Di seguito una lista di questi componenti, con breve descrizione e riferimenti a capitoli che li trattano estesamente.

Il programma ROCKEY4ND Envelope (*RyEnv32_ND.exe*) permette di cifrare file.exe, .dll, .arx e altri file Portable Executable (PE) a 32 bit. Soluzione ideale se non possedete il codice sorgente dell'applicazione da proteggere o se non avete esperienza di programmazione con API. (Vedere Capitolo 6: ROCKEY4ND Protezione Tramite Envelope)

ROCKEY4ND ha una serie di librerie API che possono essere usate per creare un flessibile e potente sistema di protezione. Questo documento fornisce esempi VC ++ ed esempi di altri linguaggi sono contenuti nel CD-ROM. (Capitolo 7: ROCKEY4ND API)

1.2 Il meccanismo di protezione del software di ROCKEY4ND: il sw protetto invia chiamate alla chiave durante l'esecuzione; l'esecuzione dell'applicazione dipende dalla presenza della chiave stessa. E' impossibile duplicare il chipset dello hardware ROCKEY4ND, di conseguenza è impossibile duplicare dispositivi che permettano l'esecuzione dell'applicazione, garantendovi così la protezione dell'applicazione da ogni duplicazione pirata.

1.3 Vantaggi di ROCKEY4ND

Massima flessibilità e sicurezza per il produttore del software

1 **Ampia gamma di soluzioni e funzioni** – la gamma di prodotti Rockey offre soluzioni driverless (ROCKEY4ND / NetROCKEY4ND / ROCKEY2/ ROCKEY6), con driver (ROCKEY4 / NetROCKEY4), per rete (NetROCKEY4ND / NetROCKEY4 / NetROCKEY6), con funzioni di smartcard (ROCKEY6 Smart). Potrete anche proteggere file Flash (SWF) (ROCKEY4ND / ROCKEY2)

2 **Alto Livelli di Sicurezza**– Rispetto ad altre soluzioni, ROCKEY4ND offre un livello di sicurezza notevolmente più alto. ROCKEY4ND realizza un sistema a due livelli di sicurezza distinguendo tra utenti che necessitano un accesso in sola lettura alla chiave da quelli che richiedono privilegi di amministratore. ROCKEY4ND è realizzato per impedire la tracciatura del sw ed è così potente da poter eseguire algoritmi sviluppati dal cliente che possono portare la protezione del sw ad un livello di sicurezza mai raggiunto.

3 **Facilità d'Uso** – il set di API di ROCKY4ND rende semplice lo sforzo di programmazione per implementare le chiamate nell'ambito del linguaggio di programmazione prescelto e l'Envelope è stato ulteriormente ottimizzato per ancora aumentarne la sicurezza. Il tempo necessario al programmatore per applicare la protezione offerta da ROCKEY4ND è stato notevolmente ridotto, con conseguente risparmio di costi e tempi nel rendere sicuro il vostro sw contro l'azione dei pirati informatici.

4 **Alta Affidabilità**– FEITIAN, certificata UNI 9001, utilizza un avanzato sistema di gestione dei clienti per la produzione di ROCKEY4ND. Sia le password dei clienti che anche i codici hw di ogni chiave sono garantiti unici. Password e codice hardware sono cablati nella cpu ed è assolutamente impossibile cambiarli, anche per il produttore della chiave.

5 **Ampio Supporto di Sistemi Operativi** – Le applicazioni protette con ROCKEY4ND possono essere eseguite in: Windows 98SE/ME/2000 /XP/2003/Vista; LINUX; MAC.

6 **Soluzione Multiplatforma** – la stessa chiave ROCKEY4ND può essere utilizzata con diversi sistemi operativi, Windows, LINUX, MAC

7 **API per Numerosi Linguaggi di Programmazione** -- ROCKEY4ND fornisce le librerie API per: PB, DELPHI, VFP, VB, VC, C++ BUILDER ecc..

Massima trasparenza e facilità d'uso per l'utente finale

- 8 **Nessun driver da installare** - ROCKEY4ND non richiede l'installazione di alcun driver: basta inserirlo in una porta USB e lanciare l'applicazione protetta
- 9 **Alta Velocità** -- ROCKEY4ND è stato progettato per eseguire anche algoritmi molto complessi con ritardi inavvertibili nell'esecuzione dell'applicazione. L'utente non si accorge di alcuna degradazione nell'esecuzione di una applicazione protetta con ROCKY4ND.
- 10 **Design compatto**—Le chiavi USB prodotte da FEITIAN sono tra le più piccolo nel mercato: misurano infatti 50mm x 17mm x 7mm.
- 11 **Il cliente può fare copie di sicurezza dell'applicazione** - Il vostro cliente può fare copie di sicurezza dell'applicazione che all'occorrenza possono essere eseguite liberamente su ogni computer purché sia connessa la chiave corretta.

1.4 Come Scegliere La Giusta Soluzione Per La Protezione

Il livello di protezione raggiunto dal vostro programma non dipende solo dalla chiave ma anche da come l'applicazione usa la chiave. Anche con la miglior chiave del mondo una realizzazione rudimentale può rendere debole il livello di sicurezza globale. ROCKEY4ND offre due metodologie di protezione, non alternative: Envelope e API.

Potete utilizzare il programma Envelope *RyEnv32_ND* per realizzare la protezione e cifratura dell'applicativo. Come indica lo stesso nome, la protezione tramite envelope cifra l'eseguibile e lo racchiude in un involucro per ulteriormente proteggerlo. L'involucro stesso lancerà le chiamate alla chiave. Quando l'utente esegue un programma protetto con Envelope, l'applicazione chiamerà automaticamente la chiave ROCKEY4ND e deciderà se continuare l'esecuzione del programma in funzione ai risultati della chiamata. Il programma Envelope inoltre cripta i file eseguibili che diventano così illeggibili. Il vantaggio della protezione tramite il programma Envelope è che è estremamente facile e veloce da farsi e il codice sorgente non va modificato. La metodologia envelope è la scelta ideale se non si ha tempo per imparare l'uso delle API o se il sorgente non è disponibile. Peraltro Envelope non supporta linguaggi non compilabili, come ad esempio VBA.

Per la cifratura tramite API, il progettista deve scegliere la corretta libreria API, in funzione del suo linguaggio di programmazione, per lanciare le chiamate alla chiave. La protezione tramite API è molto flessibile, onde permettere un uso completo delle funzioni di protezione di ROCKEY4ND. E' il progettista che decide dove e come proteggere il suo sw. La protezione con le API è più sicura di quella fatta con Envelope specie se si utilizzano le funzioni algoritmiche interne in ROCKEY4ND. Ma la protezione tramite API deve essere inserita nel programma originale e ciò può richiedere un tempo più lungo.

Per il massimo della protezione usate sia l'Envelope che l'API: Incorporate le API nel sorgente dell'applicazione, compilate i file o le DLL all'applicazione, quindi usate la protezione Envelope sull'eseguibile.

Capitolo 2 - Funzioni Hardware di ROCKEY4ND

2.1 Struttura Interna di ROCKEY4ND

Nel cuore di ROCKEY4ND c'è una CPU specializzata con interfaccia USB. Supporta lo standard USB 1.0 ed è compatibile con lo standard USB 2.0. Oltre alla CPU c'è un chip con memoria non volatile dove i vostri dati si mantengono anche in caso di mancanza di alimentazione elettrica. Le memorie di ROCKEY4ND sono divise in tre zone: User, Module e Algorithm. Si può scrivere nelle memorie della chiave ROCKEY4ND almeno 100,000 volte e non ci sono limiti al numero di letture.

Il chip di ROCKEY4ND supporta funzioni quali la generazione di numeri casuali, la generazione dei seed code, e l'esecuzione di algoritmi scritti dall'utente

2.2 Interfaccia Hardware di ROCKEY4ND

ROCKEY4ND supporta lo standard USB 1.0. Con un hub USB si possono collegare fino a 16 chiavi allo stesso computer. Il LED di ROCKEY4ND indica lo stato della chiave: in situazione normale, dopo la connessione al PC, il LED resta sempre acceso. Se il LED lampeggia questo significa che il driver non è installato (per Win98). Altri comportamenti del LED indicano un guasto hw.

Nota: ROCKEY4ND è un dispositivo USB plug and play. Rimuovere una chiave ROCKEY4ND mentre è in lettura o scrittura, può causare un blocco del sistema operativo.

Capitolo 3 - Installazione dello SDK ROCKEY4ND

Lanciate *Setup.exe* dalla directory ROCKEY4ND del CD-ROM che trovate nel Software Developer's Kit (SDK). Il contenuto del CD-ROM non è zippato. Volendo, basta semplicemente ricopiare tutto il contenuto o quanto serve nel computer.

3.1 Contenuto del CD-ROM

Il contenuto del CD-ROM è diviso in due parti: □

- Tool nella directory Tools. Alcuni documenti sull'uso di questi tool sono contenuti nelle rispettive cartelle.
- Librerie API per i vari linguaggi di programmazione

3.2 Installazione dello SDK

Step 1.

Chiudete altre applicazioni aperte nel PC.

Step 2.

Viene fornito nel CD-ROM il programma *Setup.exe* che vi guiderà nell'installazione. Potrete selezionare i soli componenti che vi servono. Lanciate *setup.exe* dal CD. Appare la prima immagine (Figura 3.1). Selezionare la lingua.



Figura 3.1

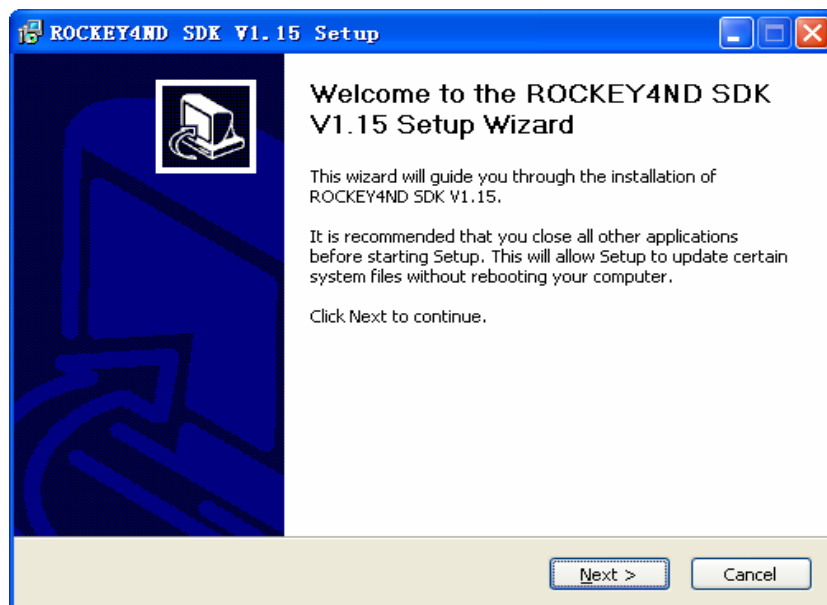


Figura 3.2

Step 3.

Leggete il software release agreement.



Figura 3.3

Step 4.

La figura 3.4 mostra l'elenco delle funzioni installabili. Selezionate quelle che volete installare.

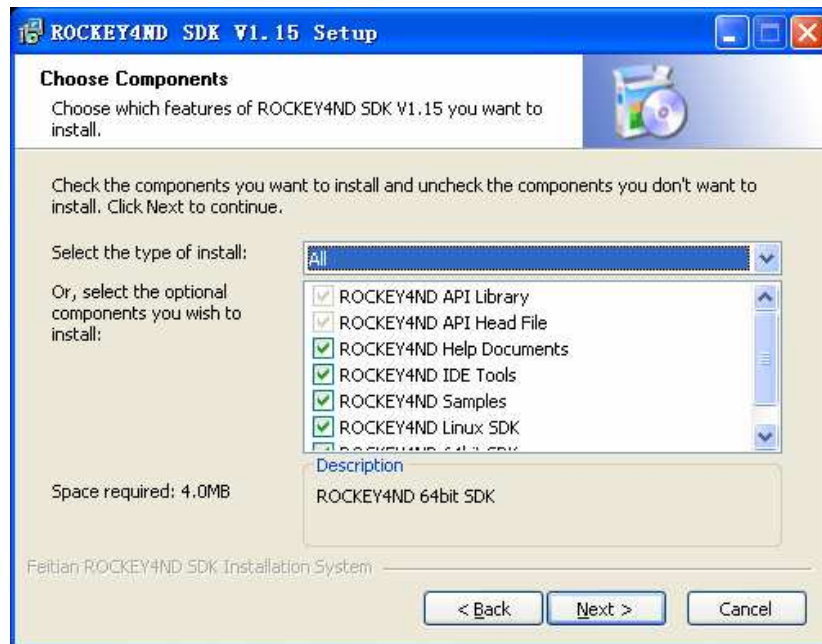


Figura 3.4

Step 5.

Selezionate dove volete installare lo SDK.

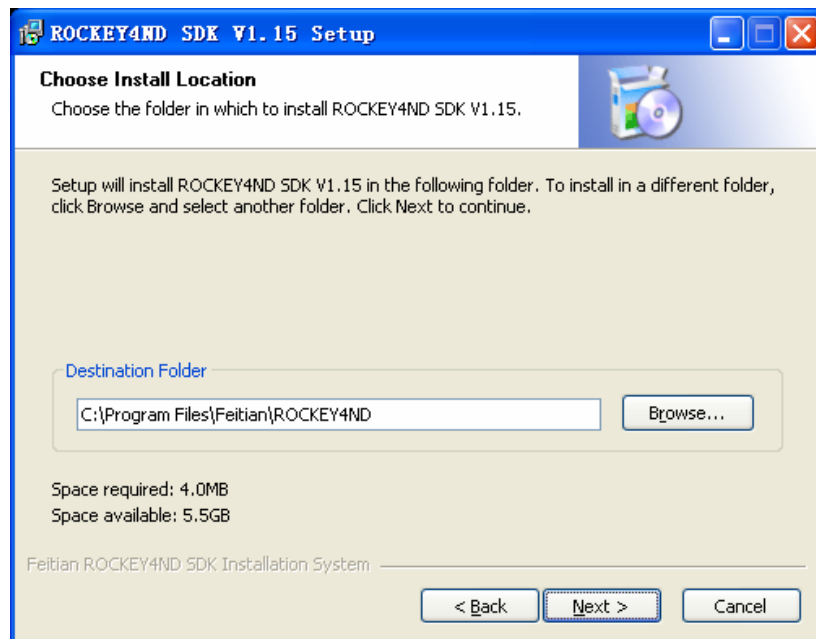


Figura 3.5

Step 6.

Cliccare Finish per completare l'installazione.

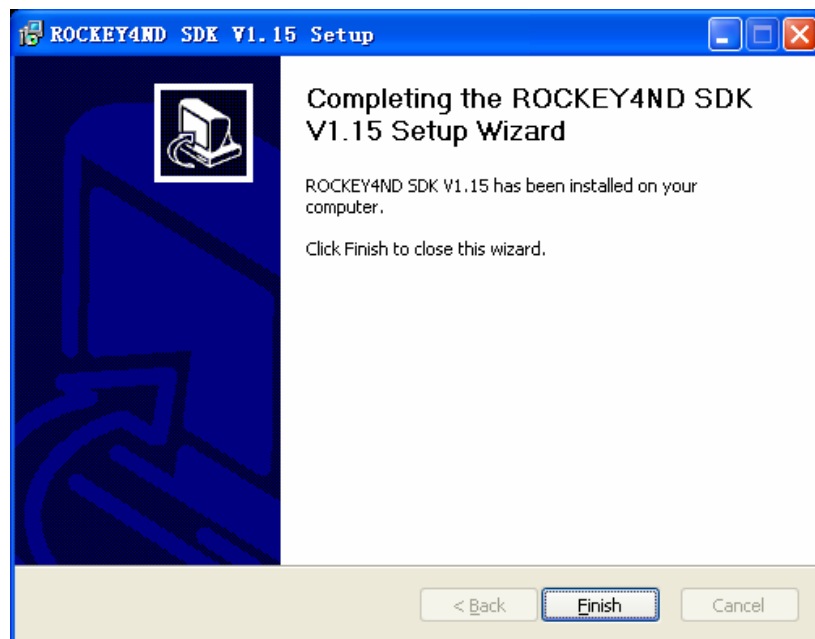


Figura 3.6

3.3 Disinstallazione dello SDK

Potete usare la funzione *Rimuovi da Pannello di Controllo/Installazione applicazioni* oppure selezionate “FEITIAN” dal comando Start/Programmi e quindi Uninstall.

Capitolo 4 - Nozioni Base per i Progettisti

Questo capitolo descrive le nozioni base e le principali funzioni del sistema di protezione ROCKEY4ND. I programmatori che utilizzeranno ROCKEY4ND per proteggere le proprie applicazioni devono leggere attentamente questo capitolo per prendere confidenza con ROCKEY4ND.

4.1 Password

Quando l'azienda sviluppatrice di software acquista un set di chiavi ROCKEY4ND ottiene un Codice Cliente e 4 password da 16-bit. Potrà sempre riordinare le proprie chiavi indicando il codice cliente, a cui sono indelebilmente associate le stesse password. Le prime due password sono definite password Basic (password di primo livello); le ultime due sono password Advanced (password di secondo livello).

Le 4 password per la chiave demo nello SDK sono: P1: C44C, P2: C8F8, P3: 0799, P4: C43B.

Le password sono cablate nello hardware e ne l'utente e neppure il produttore possono cambiarle. Il programmatore deve inserire correttamente le 4 password per avere l'accesso completo alla chiave con il programma di Editing. Il programmatore non dovrebbe mai inserire le password Advanced nel programma che viene rilasciato ai clienti finali – le password Advanced non devono essere rivelate all'utente finale in nessun modo. Descriveremo l'uso delle 4 password nel prossimo capitolo.

4.2 Codice Cliente (Customer Code)

Il Codice Cliente è lungo da 5 a 7 caratteri e corrisponde ad un set di password univoco. Utilizzerete questo codice per riordinare altre chiavi ROCKEY4ND ed essere così sicuri che tutte le vostre chiavi abbiano le stesse password.

4.3 Identificativo Hardware (HW ID)

Nella chiave è inserito un codice identificativo (Hardware Identification - HID). Lo HID è sempre diverso, unico per ogni chiave e non può essere cambiato. Il codice HID può utilmente essere usato per identificare una singola chiave ROCKEY4ND.

HID è leggibile con le password Basic. HID non è modificabile anche conoscendo la password advanced.

4.4 User Data Zone

La User Data Zone (UDZ) è uno spazio di memoria che il programmatore può usare per registrarvi dati richiamabili dalla procedura di protezione. I dati sono sempre modificabili. La UDZ è composta da 1000 bytes.

La UDZ è divisa in 2 parti.

- Area bassa (0-499 byte): è leggibile e scrivibile accedendo anche con le sole password Basic.
- Area alta (500-999 byte): utenti con le password basic possono solo leggere quest'area. Utenti con la advanced password leggono e scrivono quest'area.

La UDZ viene modificata con l'Editor o con le API ed utilizzata dalle API

4.5 Module Zone

La Module Zone comprende 64 contatori. Ad ogni contatore può essere abbinata una o più applicazioni e moduli di applicazione. Se il contatore è attivato, ogni esecuzione dell'applicazione abbinata ne decrementa il valore di una unità; fino a 64 diverse applicazioni o moduli di una applicazione possono riferirsi a questi contatori in una singola chiave. La singola applicazione, abbinata ad uno dei 64 contatori, smetterà di funzionare quando il valore del contatore sarà azzerato. Si possono quindi ad esempio distribuire CD con molti programmi in demo, ognuno dei quali avrà un suo limite d'uso. Quando poi il cliente, provati i programmi, vorrà acquistarne qualcuno, il produttore potrà inviare al cliente un eseguibile prodotto con il programma di Remote Update, per attivare l'uso dei programmi/moduli acquistati.

Inoltre utilizzando questi contatori potete proteggere con la stessa chiavi fino a 64 diversi programmi, autorizzando però il funzionamento solo ai programmi licenziati; vedere in proposito al Capitolo Envelope, punto 6.1.2

I contatori di ROCKEY4ND non possono essere letti ma solo impostati con le password Advanced.

4.6 User Algorithm Zone (UAZ)

La User Algorithm Zone (UAZ) è un'area per la registrazione delle istruzioni definite dall'utente. ROCKEY4ND supporta un massimo di 128 istruzioni. (Vedere il Capitolo 8 ROCKEY4ND Algoritmi Hardware.)

La UAZ viene editata con l'Editor o con le API ed utilizzata dalle API

La UAZ non può essere letta ma solo scritta con le password Advanced.

4.7 User ID

Lo User ID è una memoria di 32 bit che può essere usata per inserire un codice relativo all'applicazione o all'utente o ad altri riferimenti. La protezione può essere vincolata alla singola UID cosicché solo chiavi con quella UID, tra le chiavi con la stessa password, permettono il funzionamento di quella applicazione

Lo UID può essere impostato con l'Editor o con le API e può essere utilizzato da Envelope e da API.

Può essere letto con le password Basic e scritto con le Advanced.

4.8 Numeri Random

ROCKEY4ND può generare dei numeri casuali. Questi numeri possono essere usati negli algoritmi o per prevenire il tracciamento. Sono gestiti tramite API

4.9 Seed e Return Value

ROCKEY4ND contiene un algoritmo proprietario che genera quattro codici di ritorno (Return value) a seguito dell'invio di un codice (seed code) di 32 bit e relative password (Basic). Ogni chiave con le stesse password risponde con gli stessi valori per lo stesso seed code. Ovviamente i seed code sono diversi per chiavi con diverse password. Sono gestite tramite API ma l'editor permette di testarle ed individuarle con password Basic

Capitolo 5 - ROCKEY4ND Editor

5.1 Breve Introduzione

Potete usare l'Editor di ROCKEY4ND per scrivere/aggiornare dati nella chiave, per testare il suo funzionamento e per scrivervi dati in batch. L'Editor è utile per capire il funzionamento di ROCKEY4ND. La videata dell'Editor di ROCKEY4ND è suddivisa in 5 parti: Tool Bar & Pull down Menu, Status Bar, Device Selector, Operation Status Log e Operation Main Window. Vedere la Figura 5.1.

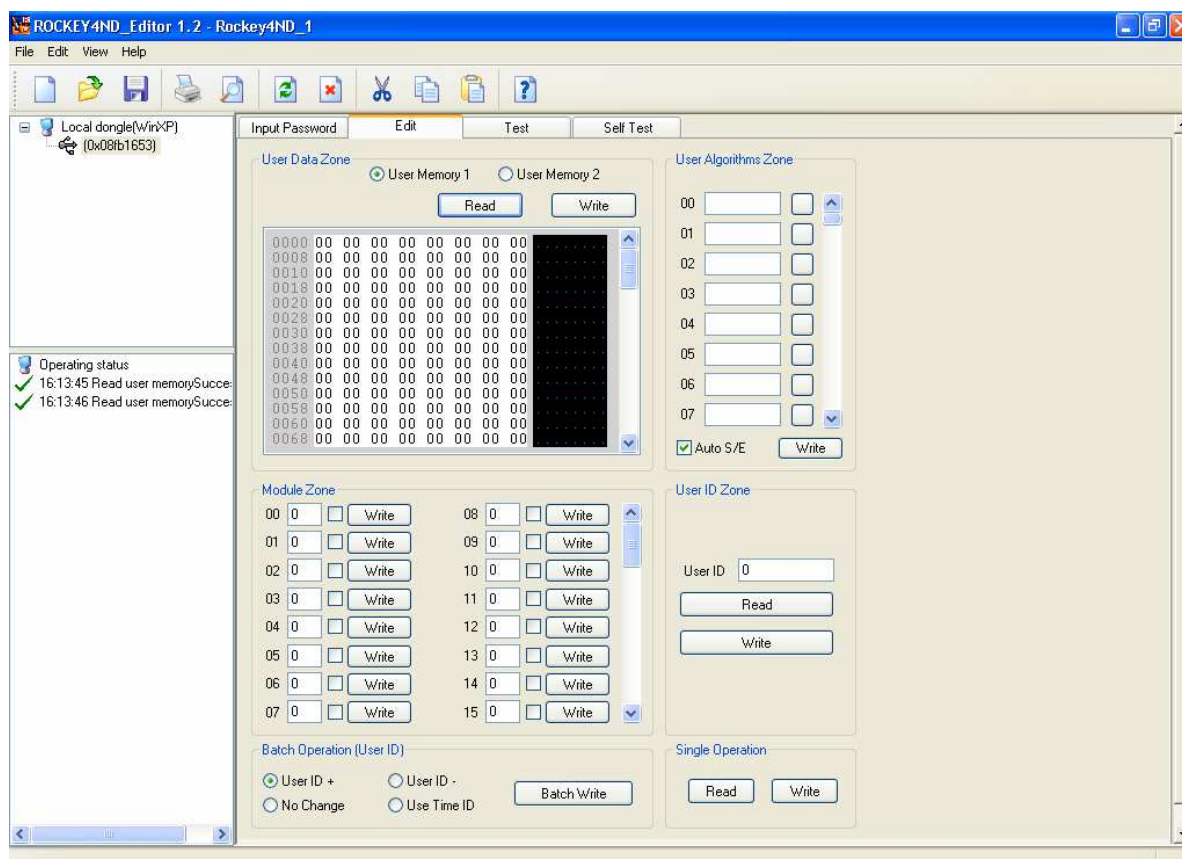


Figura 5.1

1. **Tool Bar & Pull down Menu** – E' la sezione in alto della videata. Vi sono inserite le tipiche funzioni di Windows. Vedere le figure 5.2 e 5.3.

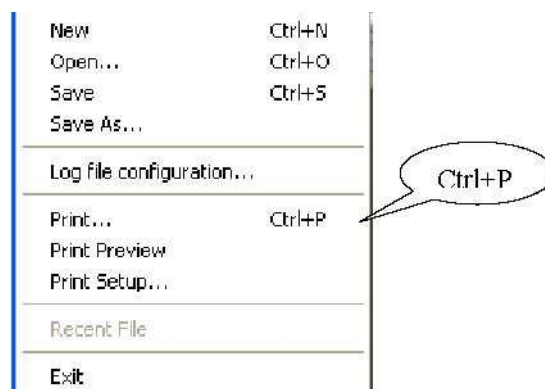


Figura 5.2



Figure 5.3

2. **Status Bar** -Lo Status Bar è al fondo della videata. Indica lo stato di avanzamento delle operazioni lanciate. Vedere Figura 5.4.

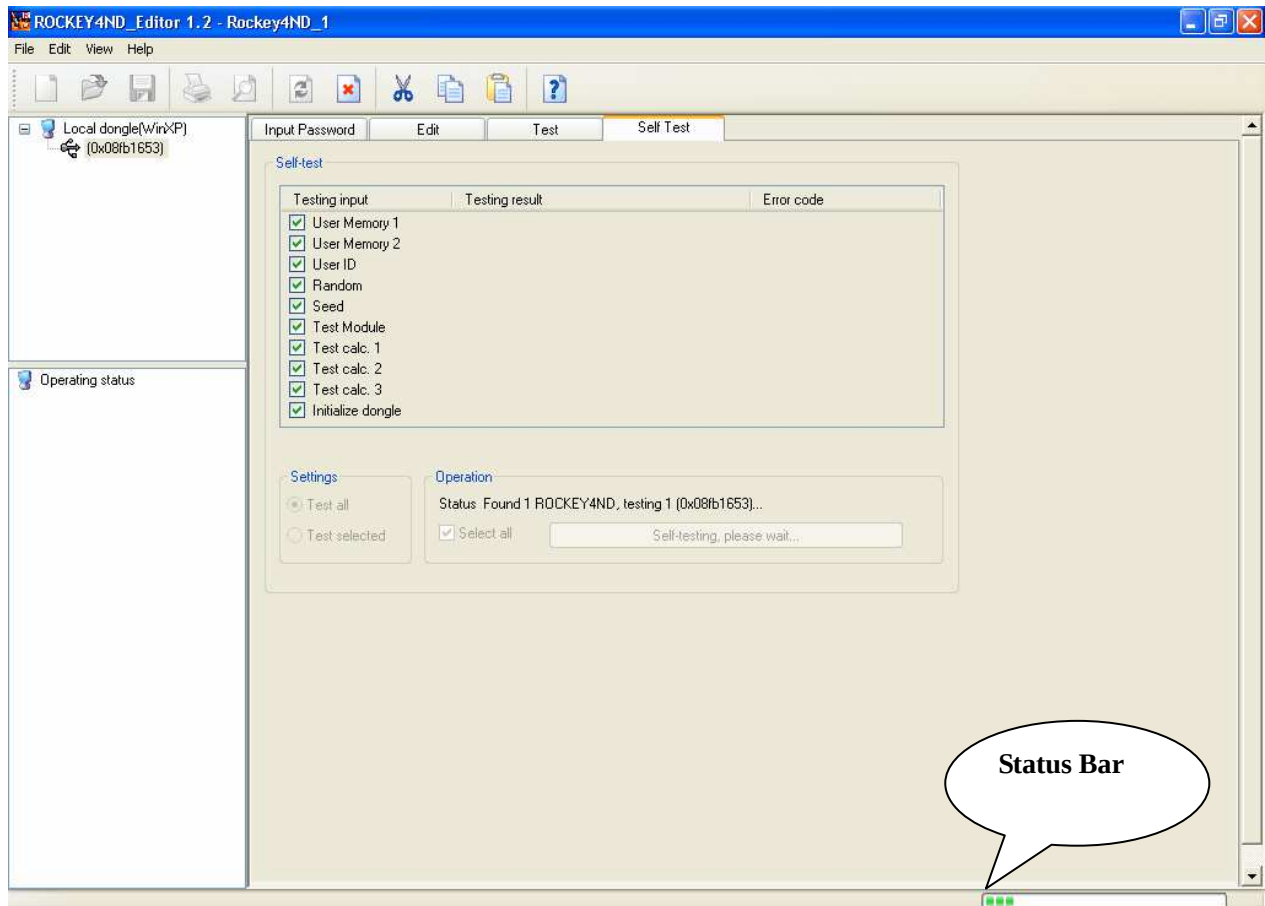


Figura 5.4

3. **Device Selector** – Quest’area è nella parte alta a sinistra della videata e mostra il codice Identificativo Hardware (HW ID) delle chiavi collegate al computer. Vedere Figura 5.5.

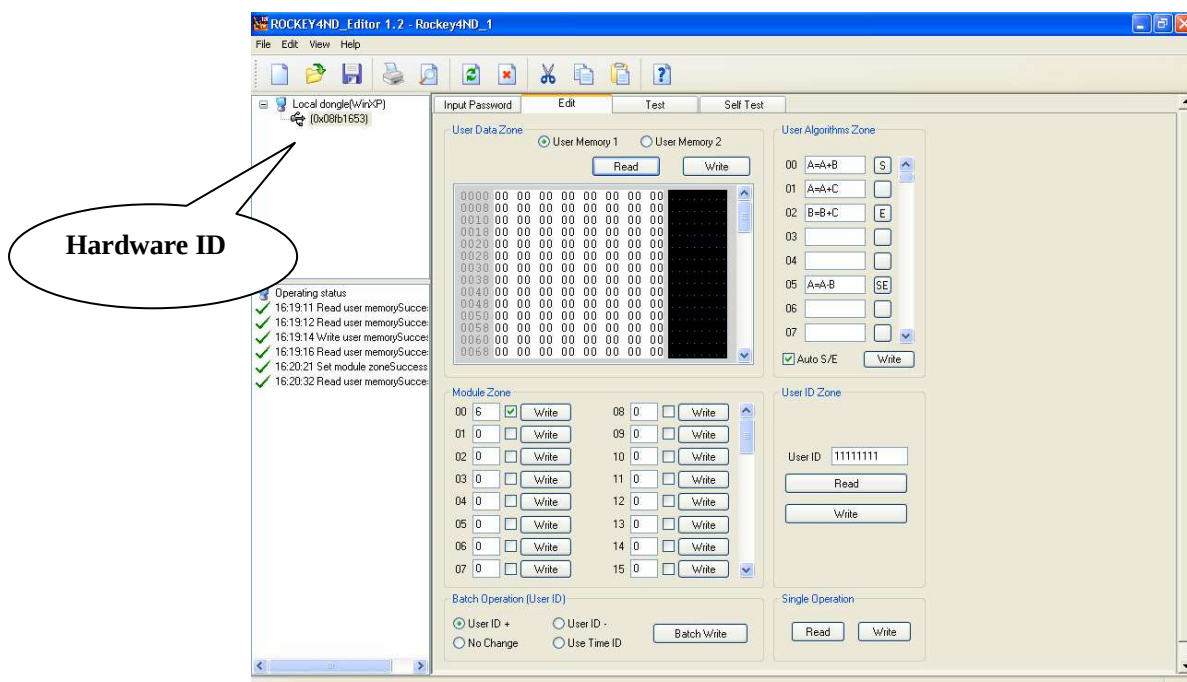


Figura 5.5

4. **Operation Status** – Data, ora e risultato delle operazioni effettuate vengono listati in quest’area, nella parte sinistra in basso della videata. Vedere Figura 5.6.

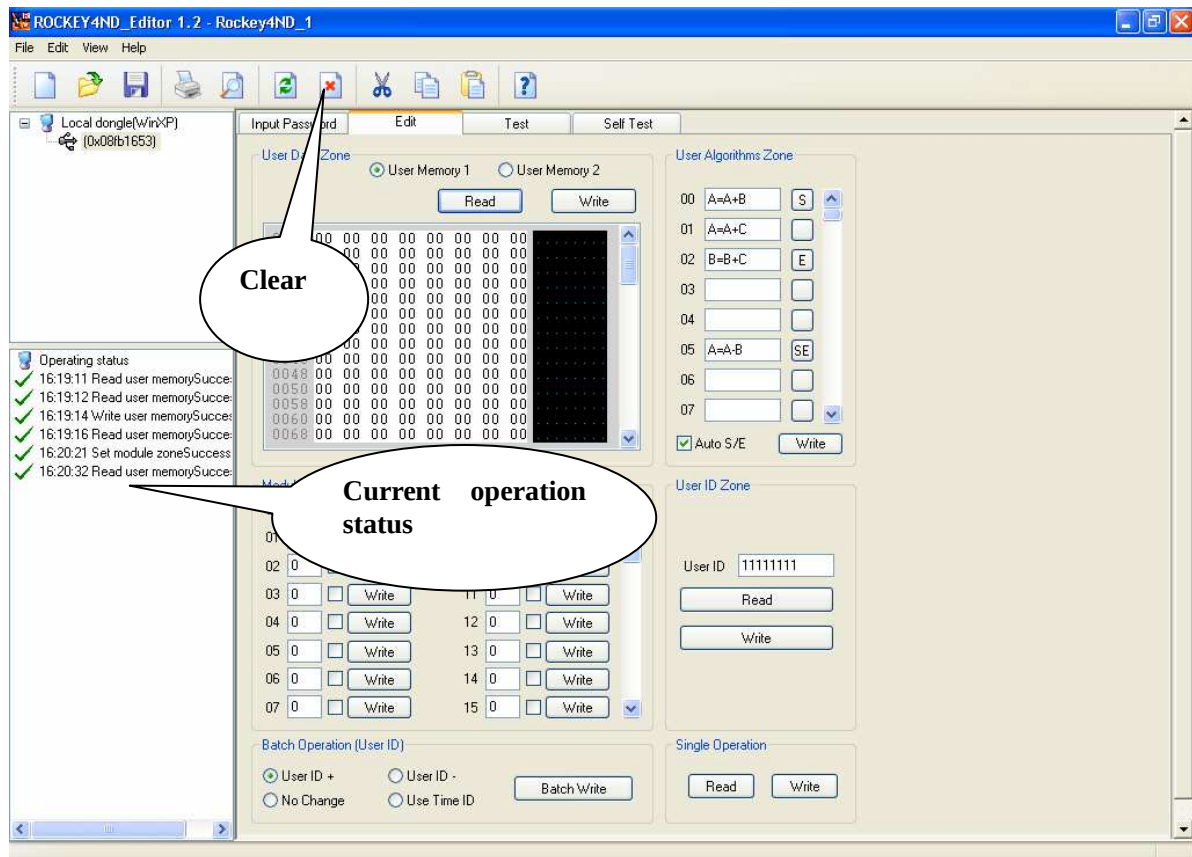


Figura 5.6

5. **Operation Main Window** – La Operation Main Window ha 4 sezioni: Password, Edit, Test, Self Test

I dati di quest’area possono essere stampati, salvati e poi richiamati (file .rki). Potete usare l’Editor anche senza inserire una chiave, salvarne il contenuto e poi richiamarlo per aggiornare una chiave.

Nota: tutti I numeri sono inseriti e evidenziati in esadecimale ad eccezione del numero di seed code generati in batch nella finestra test.

5.2 Operazioni

1. Input Password

Inserite le password Basic e/o Advanced come mostrato in figura 5.7.

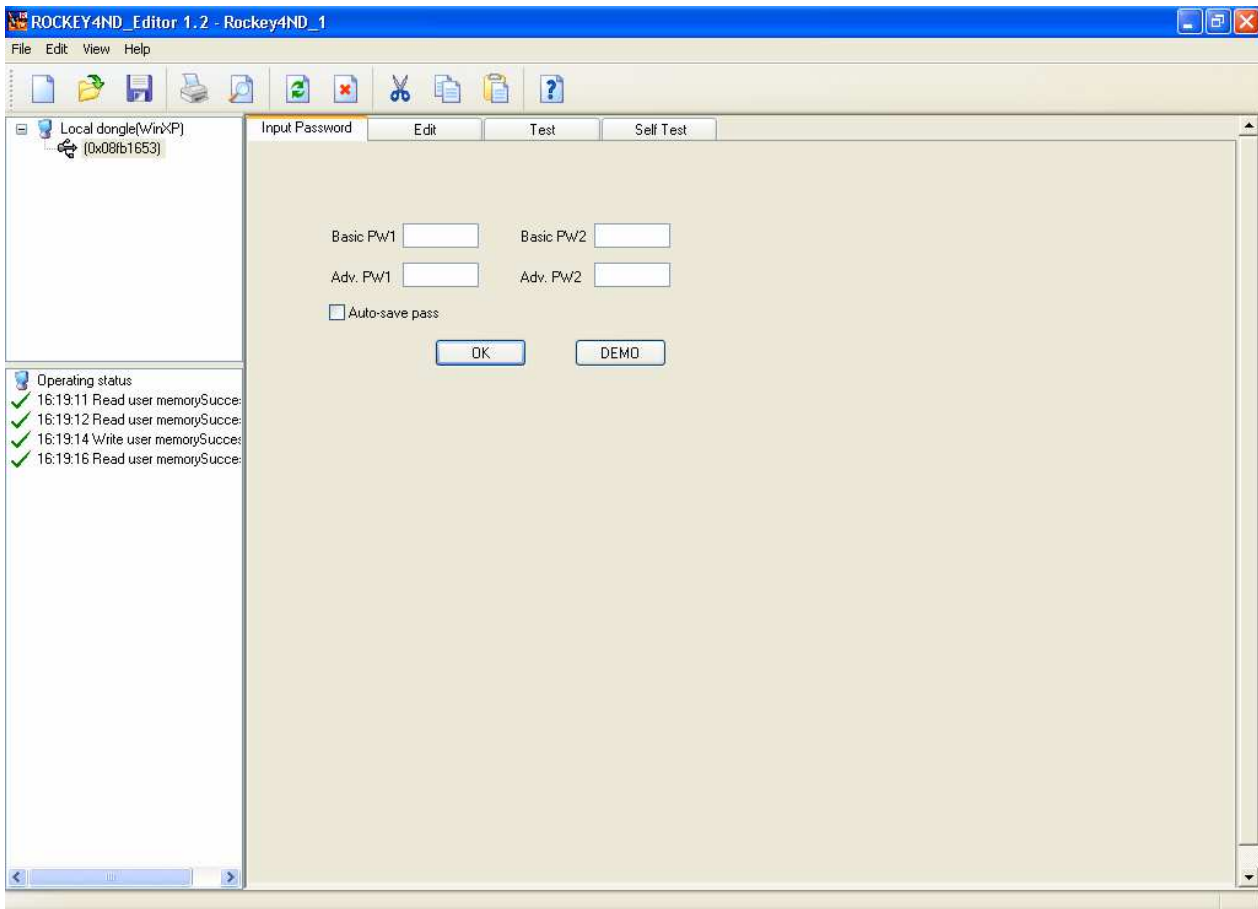


Figure 5.7

Assicuratevi di inserire le password corrette. Se le Basic non sono giuste, l' Editor non può trovare la chiave. Se le Basic sono giuste ma non le Advanced, l'Editor trova la chiave e permette solo le funzioni Basic.

Se premete il bottone "DEMO", potrete eseguire ogni operazione con la chiave demo. Le 4 password DEMO sono: P1: C44C, P2: C8F8, P3: 0799, P4: C43B.

2. Edit ROCKEY

La Hardware ID (HID) delle chiavi è evidenziato per tutte le chiavi trovate. Lo HID è unico e non può essere modificato. Vedi Figura 5.8:

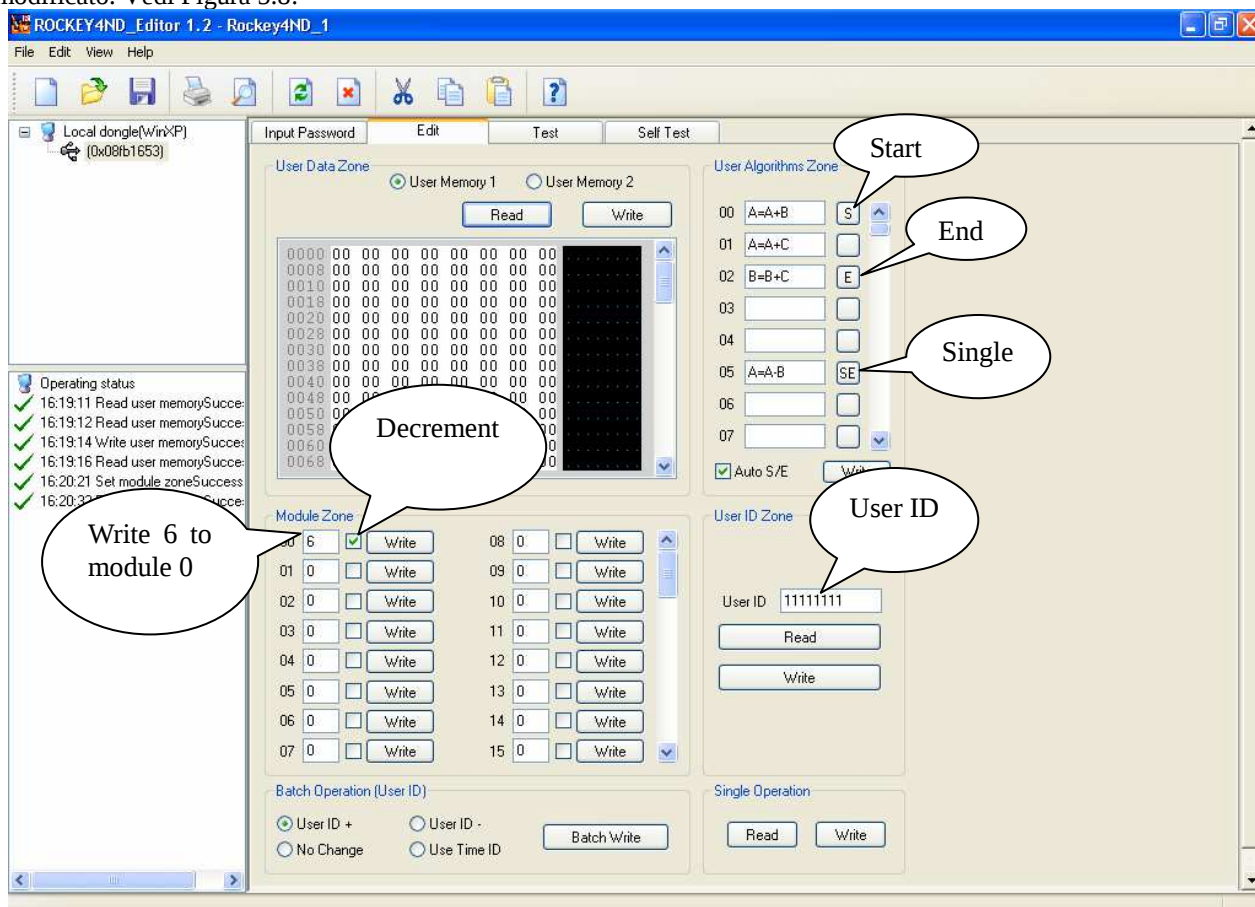


Figura 5.8

User Data Zone (UDZ) – La User Data Zone (UDZ) è uno spazio di memoria che il programmatore può usare per registrarvi dati utilizzabili dalla procedura di protezione. I dati sono sempre modificabili. La UDZ è composta da 1000 byte.

La UDZ è divisa in 2 parti.

- Area bassa (0-499 bytes): è leggibile e scrivibile accedendo anche con le sole password Basic.
- Area alta (500-999 bytes): utenti con le password basic possono solo leggere quest'area. Utenti con la advanced password leggono e scrivono quest'area.

I dati possono essere inseriti in esadecimale o in testo ASCII. Vedere Figura 5.9.

Module Zone – Qui potete inserire il numero di volte che un'applicazione/modulo può essere eseguita. Inserite il numero massimo e cliccate "Write" per registrarlo nella chiave. Anche il box deve essere attivato perché la funzione di decremento sia attivata (tutti i 64 moduli di ROCKEY4ND sono qui elencati, numerati da 0 a 63). Inoltre utilizzando i moduli potete proteggere con la stessa chiavi fino a 64 diversi programmi, autorizzando però il funzionamento solo ai programmi licenziati; vedere in proposito al Capitolo Envelope, punto 6.1.2

User Algorithm Zone (UAZ) – Qui potete impostare vostri algoritmi. L'algoritmo è formato da operatori e operandi, quali $A=A+B$ (Vedere il capitolo 8 ROCKEY4ND Algoritmi Hardware). Il bottoncino alla destra di ogni istruzione

definisce l'attributo Start/End. Un algoritmo inizia con una istruzione marcata "S" e finisce con una marcata "E". Se l'algoritmo ha una sola istruzione, sarà marcata "SE". Il valore nullo vale per ogni istruzione non iniziale o finale. La opzione "Auto S/E" assegna automaticamente gli attributi. Cliccare "Write" per registrare le istruzioni nella chiave. Vedere Figura 5.9.

User ID Zone (UIZ) – Lo User ID viene letto o scritto nella UIZ della chiave ROCKEY4ND in esadecimale. Vedere Figura 5.9.

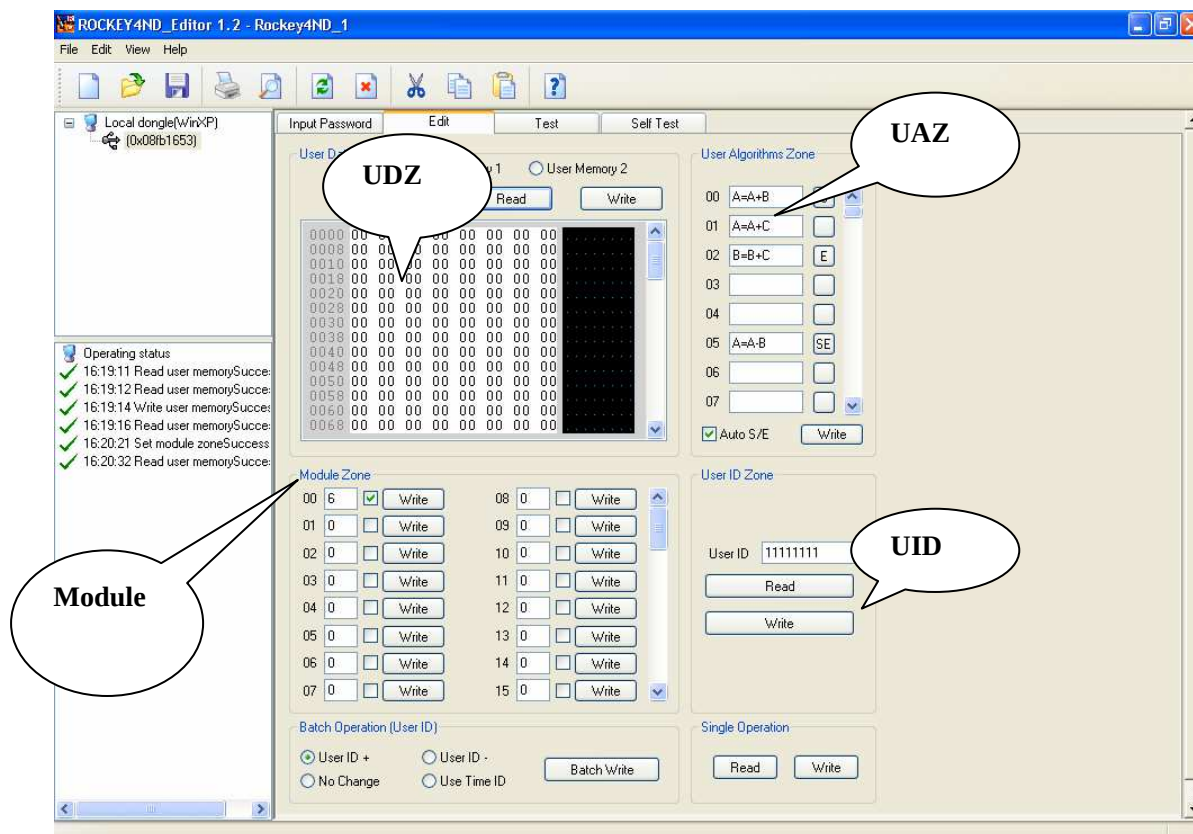


Figura 5.9

3. Batch Operation

Vedere Figura 5.9a

Batch Write: registra il contenuto della videata in tutte le chiavi collegate. Lo User ID viene registrato secondo le seguenti modalità:

- **User ID +:** se è selezionato questo campo, nella prima chiave collegata viene registrato il valore UID presente nel relativo campo. In ogni altra chiave collegata verrà registrato un valore UID aumentato di 1. Per esempio, se nel campo User ID è scritto "123", nella prima chiave sarà registrato "123" e "124" / "125"....nelle altre chiavi.
- **User ID -:** Come sopra ma qui i valori UID vengono decrementati di 1, anziché incrementati.
- **Use Time ID:** se è selezionato questo campo, lo UID sarà preso dall'orologio del computer.
- **No Change:** se è selezionato questo campo, le UID registrate nelle chiavi saranno tutte eguali al valore scritto nel campo UID.

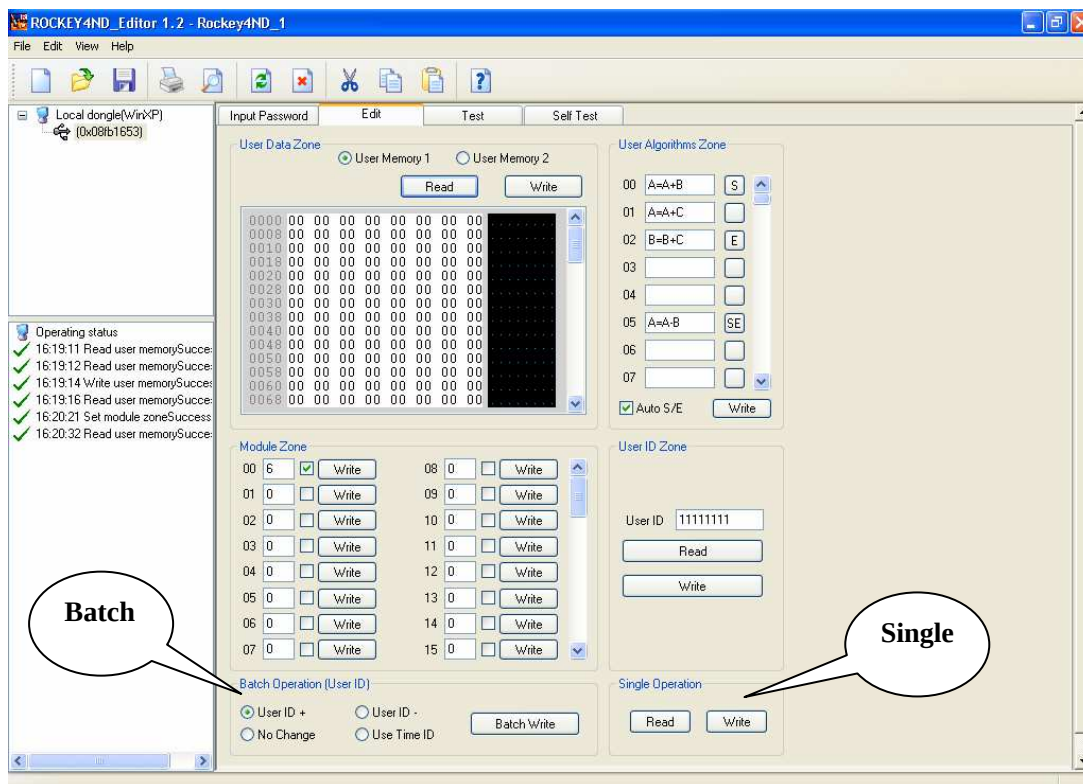


Figura 5.9a

3. Test ROCKEY Ci sono 5 zone di Test: User Data Zone (UDZ), Calculation Zone, User ID Zone (UIZ), Module Attribute Zone e Seed Calculation Zone. Vedere Figura 5.10.

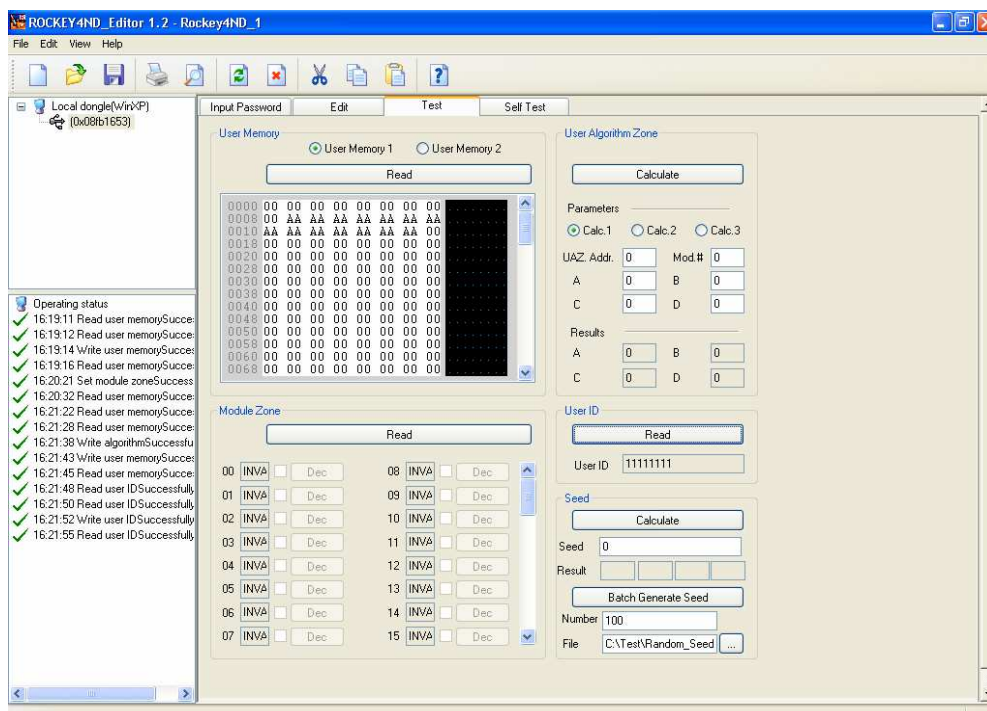


Figura 5.10

User Data Zone –Cliccare il bottone “Read” per leggere i dati esadecimali o in testo ASCII.

User Algorithm Zone – Prima di usare questa zona dovrete aver imparato le funzioni di calcolo. Per prima cosa selezionate il calcolo che volete verificare (Per Calc1 e Calc3 appare un box “Module”. Per Calc2 appare un box “Seed Code”). Quindi inserite l’indirizzo dell’istruzione iniziale (“S” o “SE”) dell’algoritmo registrato precedentemente nella UAZ. Inserite poi i valori esadecimali che volete assegnare ai parametri A, B, C e D. Inserite anche il numero del modulo o il seed code e cliccate “Calcolate”. Il risultato dell’operazione appare nelle caselle dei parametri nella sezione “Results”.

User ID Zone (UIZ) – Cliccare il bottone “Read” per leggere lo ID registrato. UIZ è di 32 bit.

Module Attribute Zone (MAZ) – Qui leggete lo stato dei contatori della MAZ. Cliccate “Read” per attivare questa zona. “VALID” significa che il contatore è stato impostato a valore diverso da zero; il box attivato significa che il modulo è attivo. “INVALID” sta per contatore=0. Se il bottone “Dec” è grigio (non attivo) il modulo non può essere decrementato. Diversamente, cliccando “Dec” decrementate di 1 il valore del contatore.

Seed Zone – Ci sono 2 piccole sezioni nella Seed Zone. La sezione superiore evidenzia i 4 codici di ritorno per ogni seed code inserito (fino a 8 caratteri esadecimali). Digitate nel campo “Number” un numero decimale e un tal numero di seed code casuali e relativi codici di ritorno verranno calcolati e registrati nel file di testo indicato nel campo “file”. Vedere Figura 5.11.

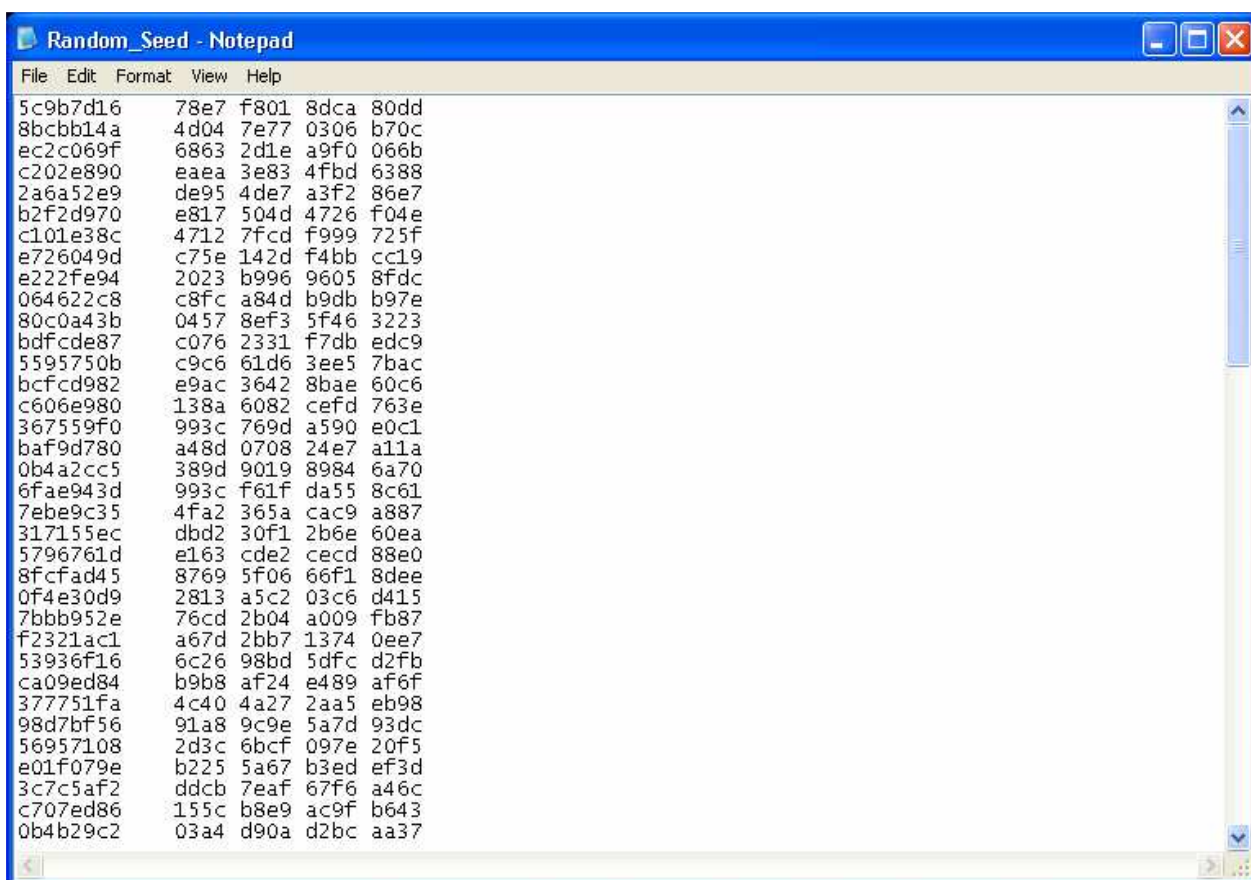


Figura 5.11

4. Self Test

ATTENZIONE !!!

Questo test è simile ad un comando di riformattazione: cancella ogni dato o parametro registrato nelle chiavi.

Esegue automaticamente il test di tutte le operazioni selezionate per tutte le chiavi connesse o selezionate. Vedere Figura 5.12.

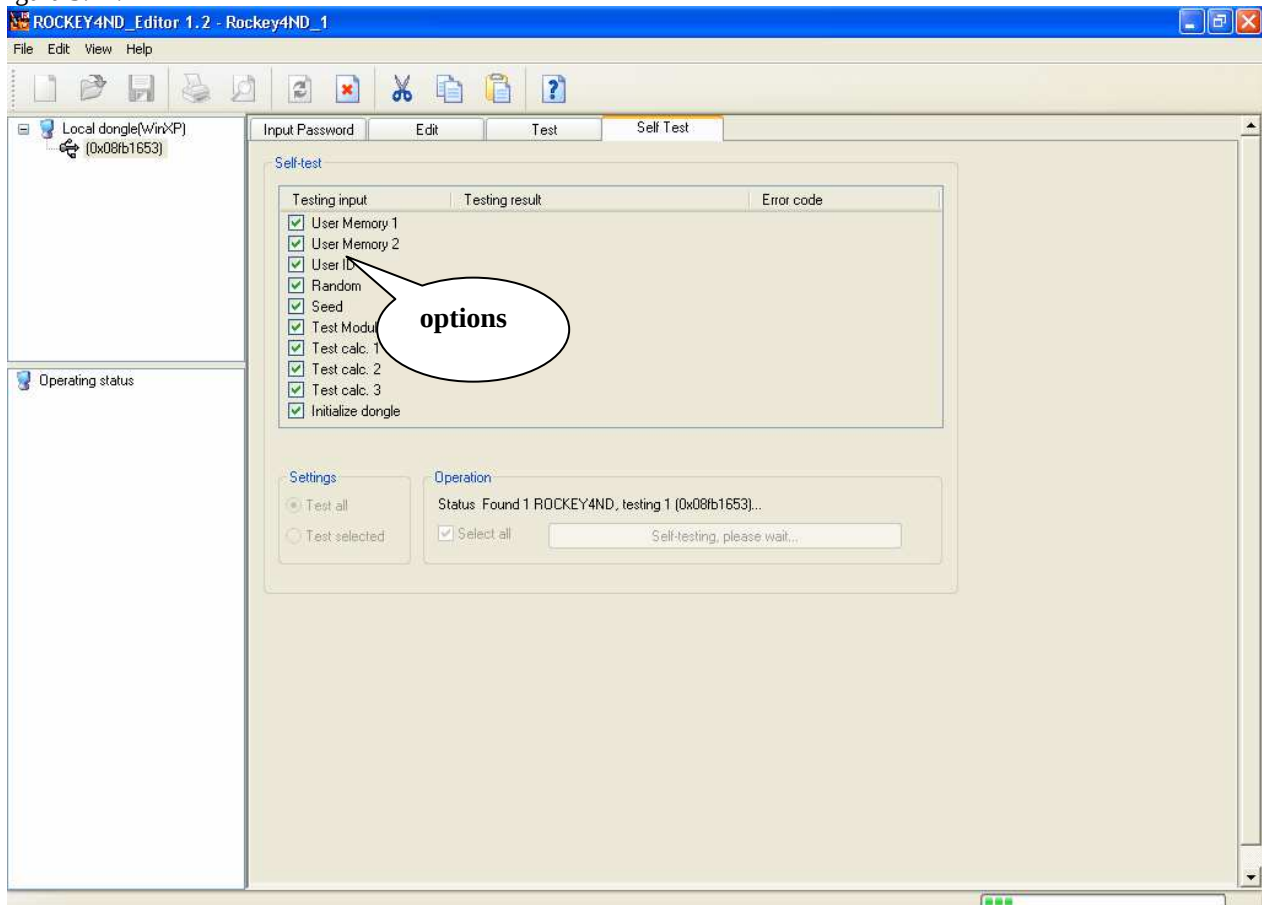


Figura 5.12

Il Self Test registra ora/data e Hardware ID (HID) in un file "log.txt". (Vedere "File/Log File Configuration", punto 5.4).

5.3 Salvataggio della videata

Potete salvare lo schema ed i dati nel disco e richiamarlo quando serve. Vedi Figura 5.14.

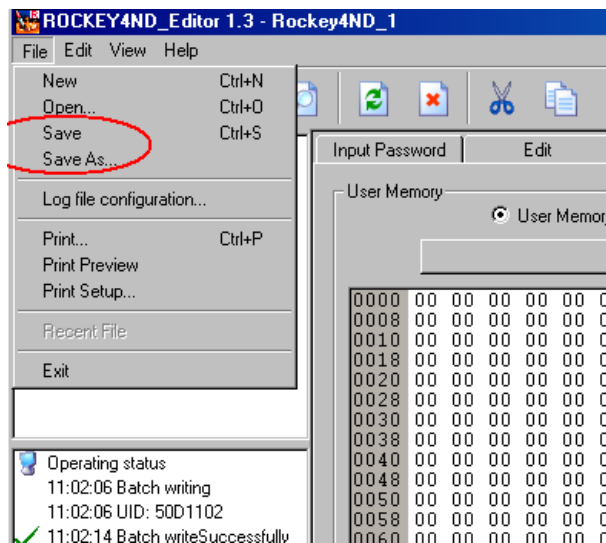


Figura 5.14

5.4 Log File e File Setting

La HID della chiave, lo User ID registrato dal Self Test e dal Batch Write possono essere registrate in un file di log. La funzione è attivata di default. Potete disabilitare questa funzione nella videata “Log file configuration” che trovate sotto il comando File (Figura 5.14). Vedere anche Figura 5.15 and 5.16.

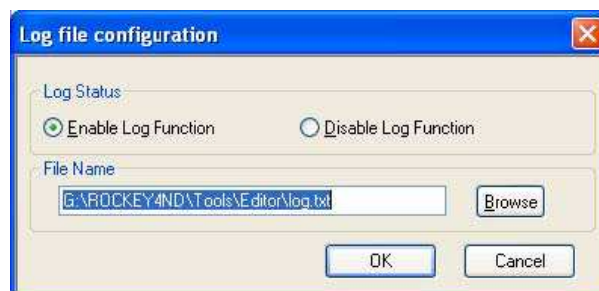


Figura 5.15

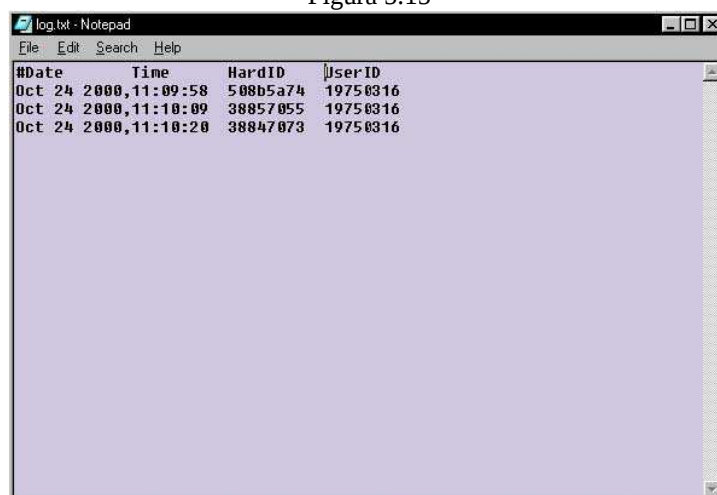


Figura 5.16

5.5 Versione dell'Editor

Cliccare il bottone “Help” per leggere la versione dell’editor. Vedere Figura 5.17.



Figura 5.17

Nota: se le funzioni di Editor non rispondono a tutte le vostre esigenze o vorreste ampliare qualcuna delle funzioni presenti, contattateci: ne terremo conto per le prossime versioni.

Capitolo 6 ROCKEY4ND Envelope

Il programma Envelope di ROCKEY4ND provvede a cifrare i file eseguibili (Win32/64 Portable Executable - PE) quali .exe, .dll o .arx, file .NET e file dati. La protezione tramite Envelope è un'ottima soluzione se non avete a disposizione il codice sorgente o non volete metterci mano o semplicemente non avete tempo per imparare l'uso delle API. Envelope funziona con applicazioni a 32 bit. Per raggiungere il massimo della protezione, vi consigliamo di usare sia la Envelope che le API.

L'Envelope può anche essere utilizzata tramite command line: a richiesta possiamo fornirvi un programma in C che genera la linea di comando

E' possibile anche proteggere file Flash (SWF): contattateci in proposito.

Lanciare Envelope.exe nella directory "WINDOWS/UTILITIES/ENVELOPE" lancia la ROCKEY4ND Envelope.

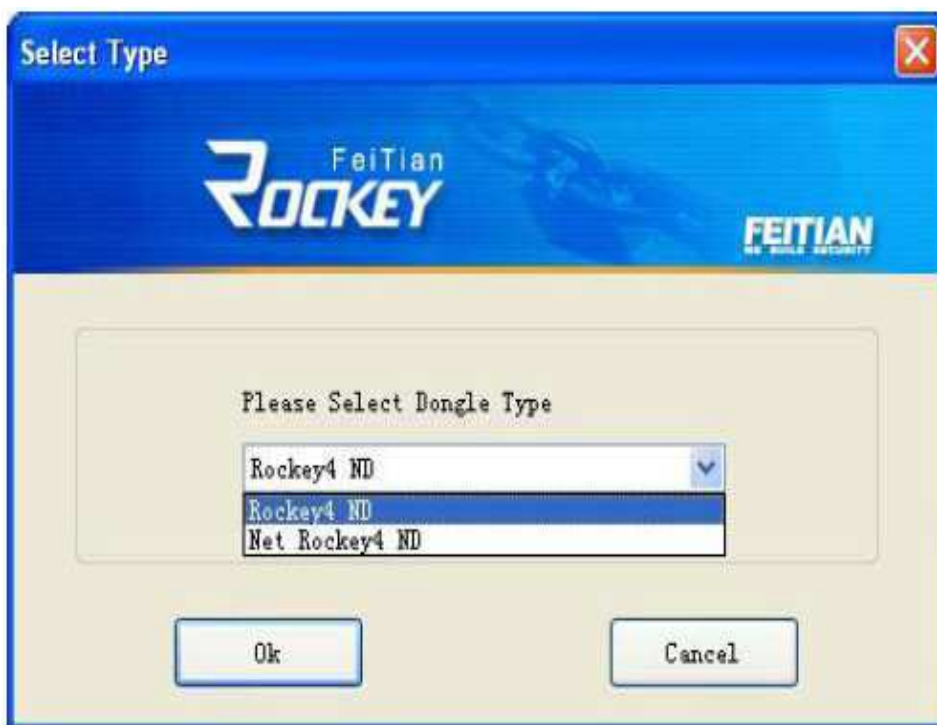


Figura 6.1

Selezionate la chiave da utilizzare (R4ND o NetR4ND).

Nota: salvate i vostri file prima di cifrarli con la Envelope. Con Envelope potete cifrare i file eseguibili più volte e in diversi modi. Se cifrate i file con i settaggi di default, l'applicazione protetta con una chiave ROCKEY4ND funzionerà con ogni altra chiave ROCKEY4ND con le stesse password. Se progettate di proteggere la vostra applicazione sia con Envelope che con API, prima inserite le chiamate API nel programma e poi procedete con la Envelope.

6.1 Protezione di Applicazione PE32/64

6.1.1 Protezione con il Settaggio di Default (fig. 6,2)

1. inserire le prime 2 password della chiave
2. cliccare il bottone 2 e
3. selezionare Program
4. inserire il file da proteggere; per il nome del file protetto di default viene proposto enc_nome-file.exe
5. selezionare il file da proteggere, quindi cliccare il bottone 5 per proteggerlo
6. se l'operazione va a buon fine avrete il messaggio **Result: success** nel campo 6

Nel campo 7 inserite il titolo che vorrete dare al box di messaggio che apparirà se all'avvio del programma la corretta chiave non è inserita.

Nel campo 8 inserite il messaggio che apparirà nel box di messaggio se all'avvio del programma la corretta chiave non è inserita.

Se volete che l'applicazione, una volta partita, controlli che la chiave non sia stata rimossa inserite **Yes** nel campo 9 e digitate ogni quanti secondi la protezione automaticamente verifica la presenza della chiave. Di default viene impostato 120 secondi.

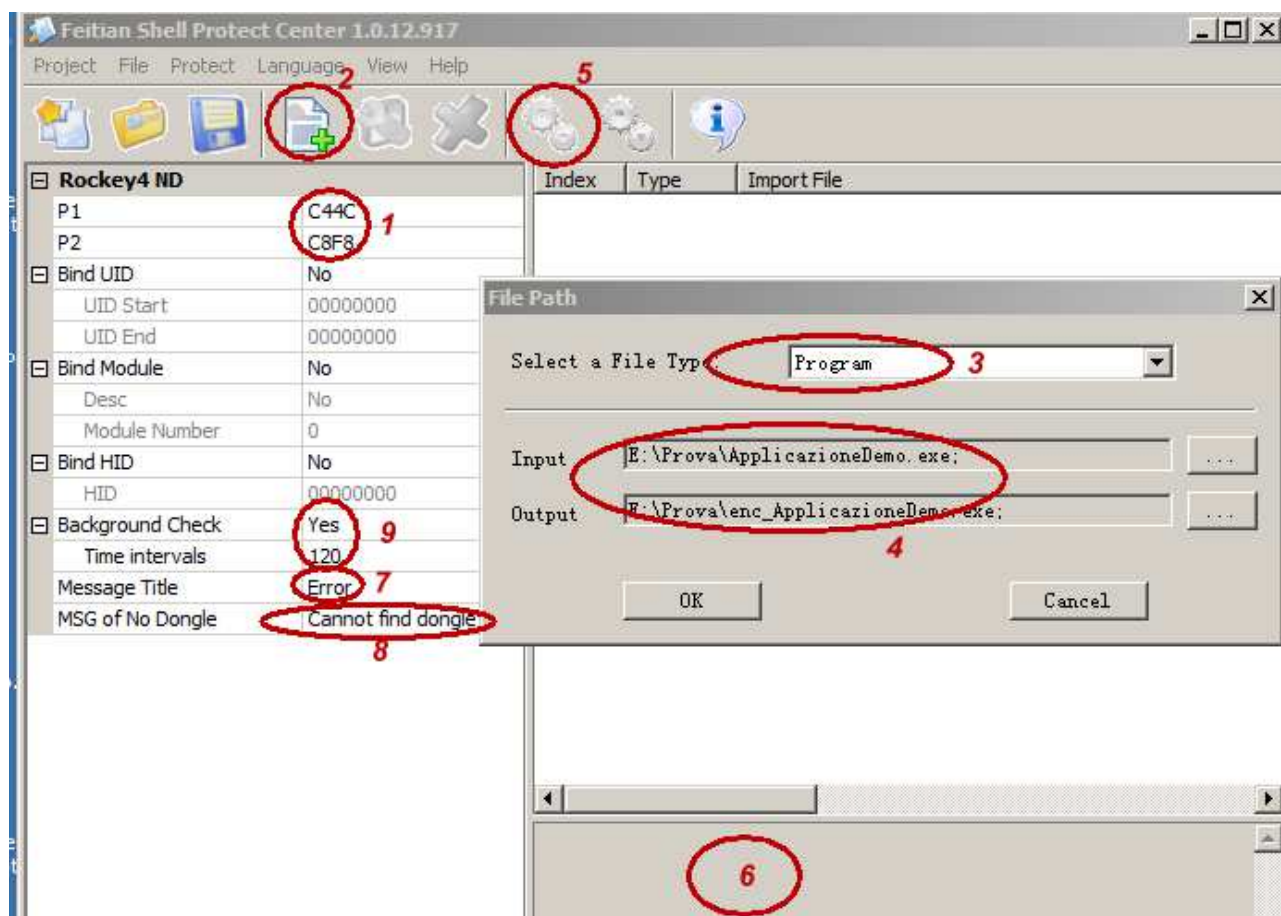


Figura 6.2

6.1.2 Protezione con i Contatori (fig 6,3)

Se selezionate “Bind module = YES”, il sistema non solo verificherà la presenza della corretta chiave, ma anche verifica che il contatore riportato nel campo “Module Number.” sia attivato. Per poter utilizzare il contatore dovete inserire un valore diverso da zero nel corrispondente modulo con il programma Editor. Inoltre va attivata la casella DEC se il contatore va decrementato.

Usate i Moduli anche proteggere con la stessa chiave fino a 64 diverse applicazioni, creando una relazione diretta tra la singola applicazione e il modulo. Ad esempio usate il modulo “0” per proteggere l’applicazione “A” e il modulo “1” per proteggere l’applicazione “B”; con l’Editor avrete inserito un valore diverso da 0 nei moduli 0 e 1 (se volete attivare la chiave per ambedue le applicazioni, oppure solo in uno dei due moduli); eseguite l’Envelope per il programma “A” attivando il campo “Use Module”, utilizzate 0 come numero di modulo e non attiverete il campo DEC. Analogamente operate per l’applicazione “B”, ovviamente utilizzando 1 come numero di modulo.

Otterreste lo stesso risultato ordinando gruppi di chiavi con diversi Codici Cliente/Password, specifici per ogni applicazione. Ma diventerà più difficoltosa la gestione delle chiavi a magazzino.

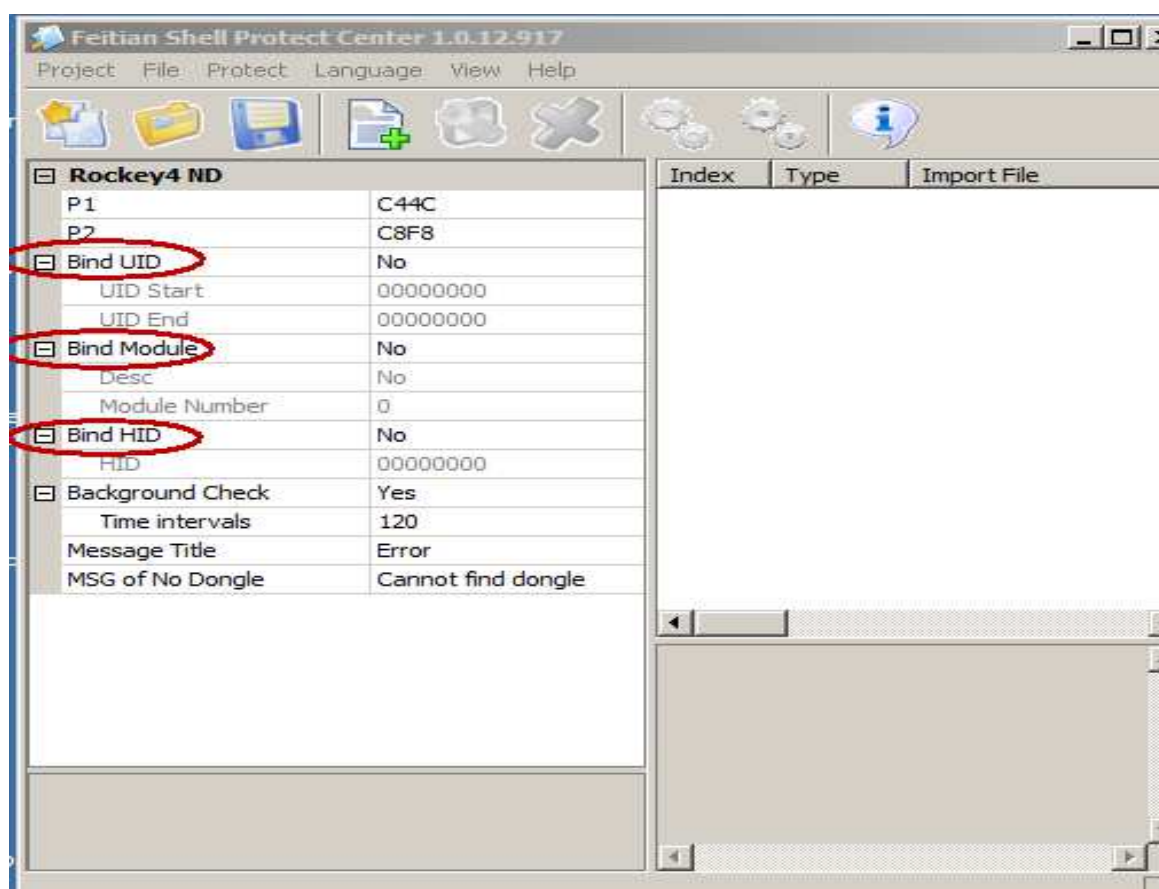


Figura 6.3

6.1.3 Protezione con HID (fig. 6.3)

Se selezionate “Bind HID = YES” la protezione avverrà tenendo conto della HID di quella singola chiave di cui avrete inserito il codice (che potete leggere con il tool Editor) e quindi il programma protetto funzionerà solo con questa chiave e non con altre con le stesse password.

6.1.4 Protezione con UID (fig. 6.3)

Se attivate questa casella, l’applicazione protetta funzionerà solo con quelle chiavi che, oltre alle corrette password, hanno l’UID, precedentemente inserito nella chiave con l’Editor, compreso tra UID Start e UID End.

6.2 Protezione di Applicazione .Net

Cliccando il tasto **Method List** potrete selezionare i moduli da cifrare (fig. 6,4)

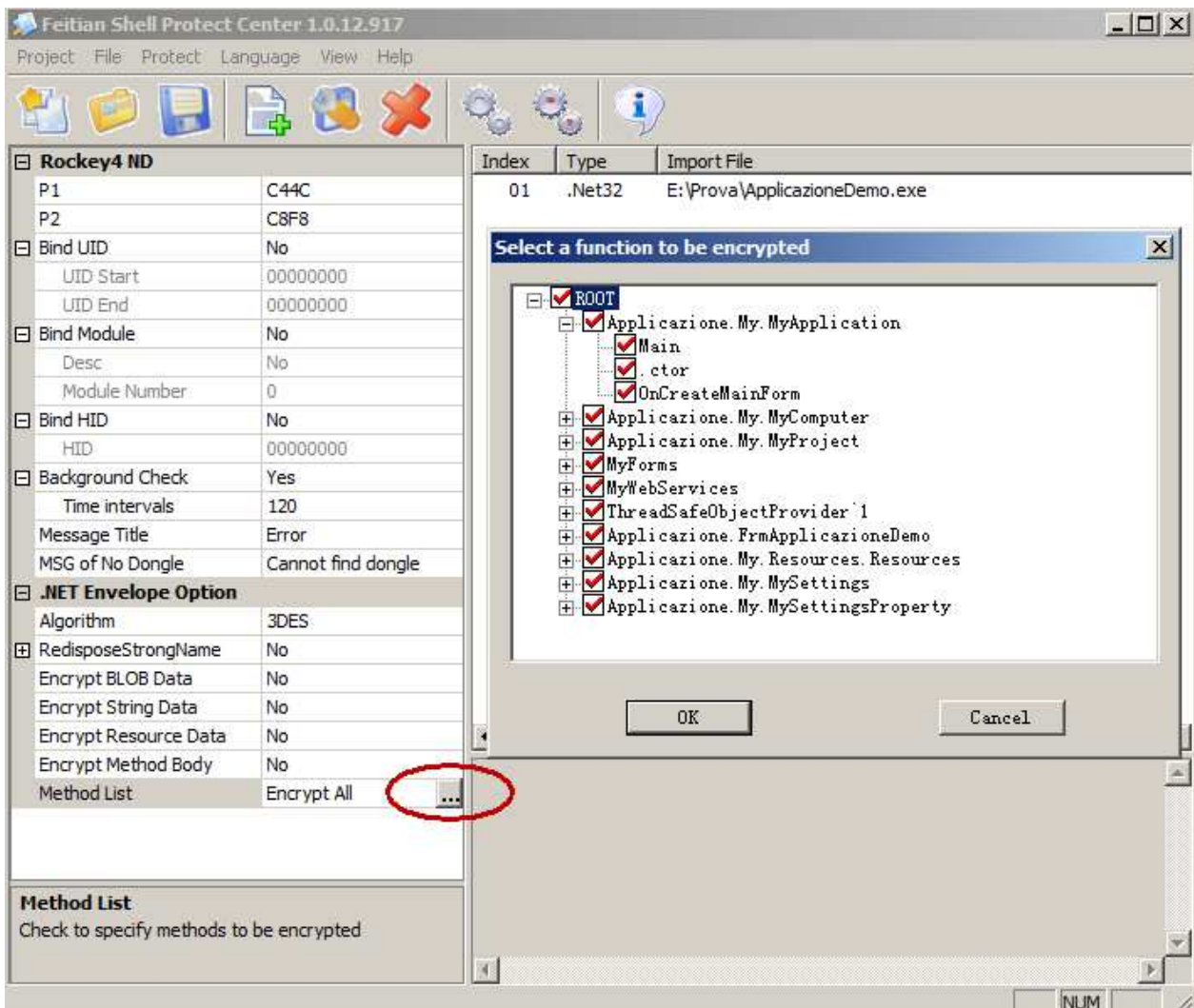


Figura 6.4

6.3 Protezione di file dati

Caricherete sia il file dati (si attiverà la **Data Protection Option**) che il file .exe, cioè l'applicazione che dovrà leggere e quindi decifrare questo o altri analoghi file dati (fig. 6,5).

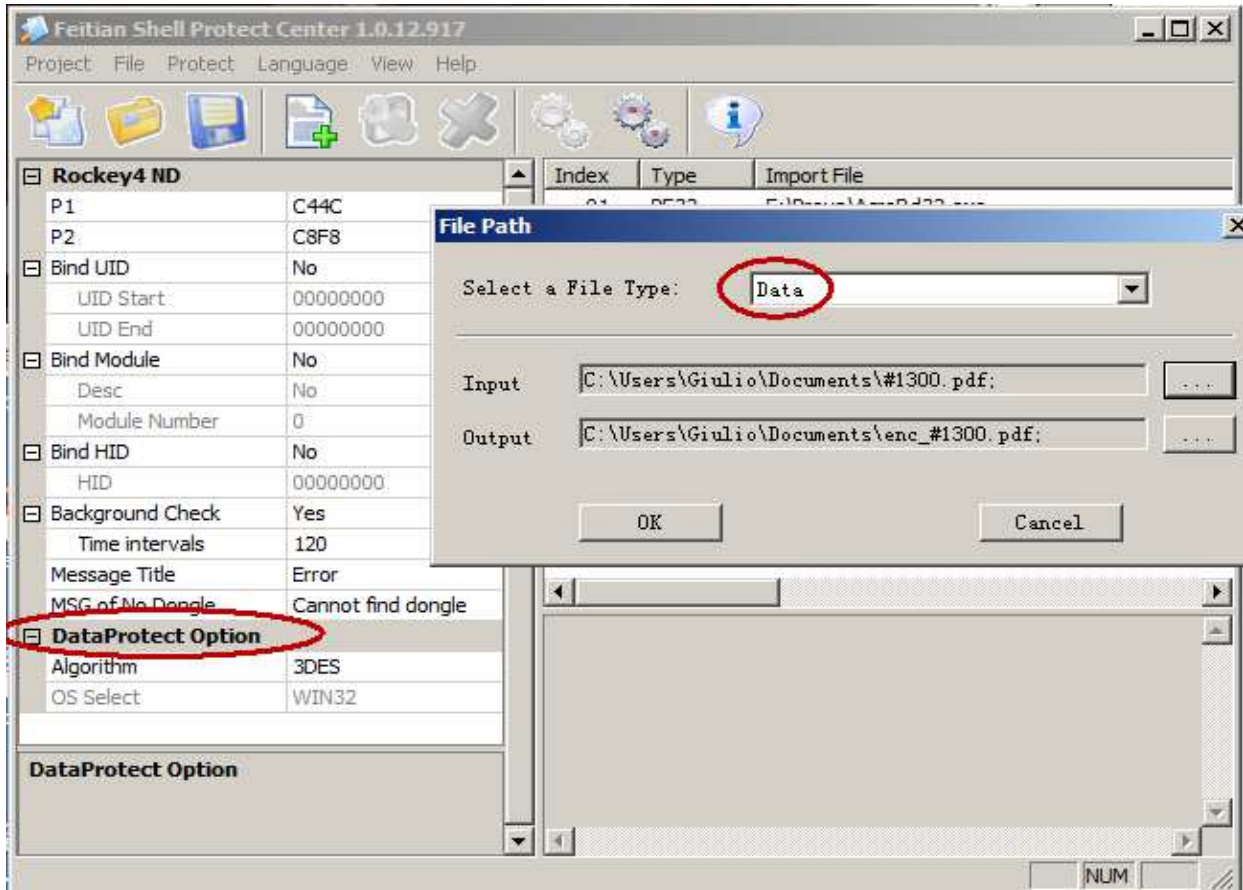


Figura 6.5

Capitolo 7 - ROCKEY4ND API

La ROCKEY4ND Application Programming Interface (API) è il mezzo più flessibile e potente per proteggere la vostra applicazione. Il livello di sicurezza che raggiungerete dipende da come utilizzerete l'API.

Grazie all'API l'applicazione protetta potrà lanciare chiamate alla chiave per verificare la sua presenza, leggere campi e parametri e comportarsi di conseguenza.

Potete utilizzare l'Editor per definire parametri e scrivere dati e algoritmi nella chiave. Tutte queste operazioni possono essere fatte anche con l'API; alcune operazioni però richiedono l'inserimento delle password Advanced e questo non è consigliabile per mantenere alto il livello di sicurezza.

E' inoltre consigliato cifrare l'eseguibile protetto con l'API con l'Envelope per massimizzare la sicurezza.

Queste le istruzioni disponibili.

RY_FIND	1	// Find ROCKEY4ND
RY_FIND_NEXT	2	// Find next ROCKEY4ND
RY_OPEN	3	// Open ROCKEY4ND
RY_CLOSE	4	// Close ROCKEY4ND
RY_READ	5	// Read ROCKEY4ND
RY_WRITE	6	// Write ROCKEY4ND
RY_RANDOM	7	// Generate Random Number
RY_SEED	8	// Generate Seed Code
RY_WRITE_USERID	9	// Write User ID
RY_READ_USERID	10	// Read User ID
RY_SET_MOUDLE	11	// Set Module
RY_CHECK_MOUDLE	12	// Check Module
RY_WRITE_ARITHMETIC	13	// Write Arithmetic
RY_CALCULATE1	14	// Calculate 1
RY_CALCULATE2	15	// Calculate 2
RY_CALCULATE3	16	// Calculate 3
RY_DECREASE	17	// Decrease Module Unit

Nella Developer's Guide (versione inglese) nel capitolo 7 trovate la descrizione dei vari servizi e come utilizzarli.

7.1 Esempi di Utilizzo di API

Nella Developer's Guide (versione inglese) nel capitolo 7.4/ 7.5 trovate descritta una serie di esempi semplici ed avanzati d'uso di tutti i servizi. Questi esempi sono intenzionalmente semplificati per facilmente illustrare i vari strumenti di sicurezza utilizzabili. Gli esempi sono quindi solo per scopo dimostrativo. Non si intende illustrare come utilizzare al meglio il sistema di protezione ROCKEY4ND – ciò dipende dalle caratteristiche del programmatore, dell'applicazione e dagli obiettivi della licenza d'uso.

Gli esempi descritti sono scritti in VC 6.0. I programmatori che utilizzano altri linguaggi sono invitati a leggere questi esempi che non richiedono una particolare conoscenza del linguaggio C. E' importante capire i concetti illustrati negli esempi.

Esempi in moltissimi altri linguaggi sono elencati ne CD nella directory *Samples* mentre in *Samples\Beginner* trovate tutti i programmi descritti in 7.4.

7.2 Consigli per massimizzare la sicurezza

- 1 **Fate chiamate alla chiave in modalità casuale** – Inserite nella vostra applicazione dei metodi casuali di chiamata alla chiave in modo da rendere difficile che altri possano capire la strutturazione delle chiamate e quindi imitare/riprodurre il funzionamento della protezione.
- 2 **Usate informazioni dinamiche per i seed code** – L'uso di informazioni dinamiche nei seed code, come ad esempio la data letta dal sistema, aumentano il livello di sicurezza in quanto variano i codici di ritorno.
- 3 **Non ripetete spesso le stesse metodologie di protezione nell'applicazione** – Se usate molte volte la stessa metodologia di protezione nell'applicazione, sarà più facile per un hacker trovare le regole di protezione usate. Metodi di protezione complessi ed attuati con diversi calcoli e parametri sono più difficilmente individuabili.
- 4 **Cifrate le stringhe di caratteri e dati**– Nello "Step 18" degli esempi è descritto come cifrare dati utilizzando informazioni ottenute dalla chiave (return code). Cifrare dati in questo modo è una metodologia molto sicura in quanto un errore nella corretta decifratura del dato potrà causare il blocco dell'applicazione o altre azioni in funzione di quanto previsto dalla licenza d'uso.
5. **Usate sia API che Envelope.** – Il più alto livello di protezione sarà raggiunto utilizzando prima una metodologia complessa e dinamica di chiamate API, e quindi cifrando l'eseguibile con l'Envelope.

Capitolo 8 ROCKEY4ND - Algoritmi Hardware

I progettisti possono definire algoritmi proprietari e registrarli non nel programma ma nella memoria della chiave ROCKEY4ND. La chiave calcolerà i risultati e li manderà all'applicazione che li utilizzerà. Dal momento che la Algorithm Zone (UAZ) di ROCKEY4ND non è leggibile, neppure dal produttore delle chiavi, questo tipo di protezione è estremamente potente.

I programmatori possono registrare nella chiave i loro algoritmi con l'Editor o con il comando `RY_WRITE_ARITHMETIC`

Nella Developer's Guide (versione inglese) nel capitolo 8 trovate la descrizione di come scrivere il vostro algoritmo ed alcuni esempi di algoritmi.

ROCKEY4ND - Specifiche Tecniche

	
Dimensioni	51 x 16 x 7 mm
Colore	Blu, Verde, Grigio, Marrone
Memoria	1k
Min. Operating Voltage	5V
Current Consumption (active/idle)	<= 50 mA
Max cicli di scrittura	>100,000
Connessione	USB Type A
Temperatura Operativa	0-70°C
Data Retention	10 Anni
Algoritmi registrabili	128 algoritmi definiti dall'utente
Hardware ID	Unico in tutto il mondo
Driver	No Driver
Aggiornamento Remoto	Eseguito in modalità altamente sicura,
Production Tool	Batch Production Tool
Module Management	Multiple-Module and Management Schemes
Operating Systems	Windows 98SE/ME/2000/XP/ Server 2003, Linux, Mac OS
Enveloper	Sì
Invisible Module Zone	64 moduli per gestire 64 contatori e/o 64 diverse applicazioni con la stessa chiave
Random Generator	Hardware Random Generator
API Fornite	VB, VC, Delphi, FoxPro, Java, PB, VS.Net...