

ROCKEY2

Guida all'uso

V1.1 it

Annex A

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 ROCKEY2 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.
3. **Warranty** – Feitian warrants that the ROCKEY2 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.

5. **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.
6. **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.

Indice

Capitolo 1 Breve introduzione	4
Capitolo 2 ROCKEY2 Funzioni	2
Capitolo 3 ROCKEY2 API	3
Capitolo 4 Codici d'Errore	4
Capitolo 5 Protezione con Envelope.....	6

Capitolo1 Breve Introduzione

ROCKEY2 è una chiave di protezione di basso costo e estremamente semplice da utilizzare. ROCKEY2 peraltro non offre le molteplici funzioni di protezione disponibili con le ROCKEY4, ROCKEY4ND e ROCKEY6 Smart.

Queste le funzioni di ROCKEY2:

- ▶ ROCKEY2 ha 2560 byte di memoria riscrivibile, molto più di quanto generalmente offerto all'utente da altre chiavi di protezione.
- ▶ ROCKEY2 è un dispositivo conforme allo standard HID e quindi non necessita di installazione di alcun driver per Linux e Windows.
- ▶ Ogni ROCKEY2 ha un codice identificativo hardware unico.
- ▶ Più chiavi ROCKEY2 possono operare contemporaneamente nello stesso computer.
- ▶ ROCKEY2 è disponibile con connessione USB.
- ▶ ROCKEY2 fornisce la funzione Envelope (Ry2Env32.exe) per una rapida protezione e cifratura dei file eseguibili (.exe, .dll); fornisce anche una utilità di Envelope per file .NET e Flash (.swf): li trovate con una breve descrizione nella cartella Utilities
 - o Prima di utilizzare la Envelope dovreste personalizzare la chiave ROCKEY2 con il suo codice UID (vedi Capitolo 2).
 - o Per vostra comodità abbiamo realizzato una piccola utilità che vi permette di personalizzare la chiave: la trovate nella cartella ROCKEY2/Esempio

Capitolo 2 Funzioni di ROCKEY2

User ID (UID) e Hardware ID (HID)

Ogni chiave ROCKEY2 contiene un identificativo utente (User ID - UID) oltre all'identificativo Hardware ID (HID) che è unico e non ripetibile per ogni chiave. Sia UID che HID sono definite come 32-bit DWORD. UID e HID sono identificativi della chiave ROCKEY2.

Lo UID di default è "0". Con UID di default potete aprire e leggere/scrivere la memoria della chiave. Ma non potrete leggere lo HID. Lo HID è protetto in lettura quando lo UID è quello di default. Lo HID protetto ritorna il valore "0". Lo HID vero può essere letto solo dopo che sia stato inserito lo UID.

Quando si genera lo UID, viene richiesta una stringa di 64 byte come seed code. Lo UID si ottiene da questo seed code. La generazione dello UID è realizzata all'interno dello hardware della chiave. Il processo è assolutamente irreversibile, il che significa che solo l'utente che ha lanciato il seed code può conoscere lo UID generato. Anche se un hacker conosce lo UID e come generarlo, non conoscendo il seed code non può generare un'altra chiave con lo stesso UID.

Inoltre il programmatore può decidere dove scrivere dati nella memoria e, quando genera lo UID, se sia possibile scrivervi. Se la chiave è definita "non scrivibile" tutta la memoria è protetta dalla scrittura.

Per generare lo UID potrete usare le API (vedi cap. 3) oppure potete utilizzare l'utility ESEMPIO (nella cartella ROCKEY2/Esempio)

Driver di ROCKEY2

La chiave ROCKEY2 è un dispositivo USB che utilizza i driver nativi in Windows e Linux. Quando viene inserita per la prima volta la chiave nella porta USB, il sistema operativo vi avvisa che sta installando un nuovo dispositivo. Con Windows 98 potete aver bisogno di installare il driver Win98. Ma non c'è bisogno di alcuna installazione per Win Me/2000/XP/Vista – il driver viene installato automaticamente.

Il sistema operativo utilizza UID e HID per identificare la chiave e installare il driver. Alla prima connessione della chiave, si attiva il processo di installazione del driver. Quando reinsete la chiave, il computer verifica se una nuova chiave è stata connessa ed eventualmente installa il nuovo driver. Una volta assegnato lo UID, il computer registra l'accoppiata UID/HID e non procederà più alla installazione del driver per quella chiave. Ricordatevi che, dal momento che ogni ROCKEY2 ha un HID unico, ogni nuova chiave inserita richiede l'installazione di un suo nuovo driver. Tuttavia una volta installato un driver per una certa chiave, questa può essere rimossa e reinserita senza alcuna nuova installazione di driver.

ROCKEY2 è inizialmente formattato con UID=0 e HID nascosto HID=0. Il sistema operativo del computer vede questa chiave come unità "00". Voi dovete generare lo UID perché il sistema operativo veda una combinazione UID/HID specifica. Lo UID deve essere generato prima di inviare la chiave all'utente finale e la chiamata per la generazione dello UID **non** deve essere inserita nel pacchetto inviato al cliente finale.

Capitolo 3 API ROCKEY2

1. RY2_Find: Trova la chiave ROCKEY2 connessa al computer

EXTERN_C int WINAPI RY2_Find();

Valore di	<0	Codice Errore
Returno	=0	Chiave ROCKEY2 non connessa
	>0	Il numero di chiavi ROCKEY2 connesse

2. RY2_Open: Apri una specifica chiave ROCKEY2

EXTERN_C int WINAPI RY2_Open(int mode, DWORD uid, DWORD* hid);

Input	mode	Questo parametro indica come aprire una chiave mode = 0, apri la prima chiave ROCKEY2 trovata mode > 0, apri la chiave con quel UID. Il valore mode è il numero della chiave, per esempio: uid=12345678, mode=2, significa aprire la seconda chiave trovata con UID 12345678 mode = -1, apre la chiave con lo specifico HID, e *hid non può essere =0 Definiamo 2 MACRO: AUTO_MODE=0 e HID_MODE=-1
	uid(User ID)	Dovete specificare lo UID della chiave generato tramite RY2_GenUID
	hid(Hardware ID)	Apri la chiave con lo HID di *hid Lo HID della chiave viene risposto a *hid indipendentemente da come la chiave è stata aperta.
Return	>=0	Successo. Viene risposto lo handle della chiave aperta.
	< 0	Codice Errore. Vedere i codici errore al Capitolo 4

3. RY2_Close: Chiudi una specifica chiave ROCKEY2

EXTERN_C int WINAPI RY2_Close(int handle);

Input	ROCKEY2 handle. E' lo handle risposto da RY2_Open
Return	Codice Errore. Vedere i codici errore al Capitolo 4

4. RY2_GenUID: Genera lo User ID(UID)

EXTERN_C int WINAPI RY2_GenUID(int handle, DWORD* uid, char* seed, int isProtect)

Input	Handle	ROCKEY2 handle. E' lo handle risposto da RY2_Open
	Uid	Parametro Output. Lo UID da generare
	Seed	Seed per generare lo UID. E' una stringa di caratteri di massima lunghezza di 64 byte
	isProtect	Definisce la protezione in scrittura della memoria. 0=chiave non protetta in scrittura, 1=chiave protetta in scrittura. Definiamo 2 MACRO: #define ROCKEY2_DISABLE_WRITE_PROTECT 0 #define ROCKEY2_ENABLE_WRITE_PROTECT 1
Return	Codice Errore. Vedere i codici errore al Capitolo 4	

5. RY2_Read: Leggi il contenuto della chiave

EXTERN_C int WINAPI RY2_Read(int handle, int block_index, char* buffer512);

Input	handle	ROCKEY2 handle. E' lo handle risposto da RY2_Open
	block_index	Definisce il blocco. Specifica il blocco da leggere. Valore da 0 a 4
	buffer512	Buffer di lettura. Il buffer deve essere almeno di 512 byte per inserirvi il blocco di dimensione 512 byte.
Return	Codice Errore. Vedere i codici errore al Capitolo 4	

6. RY2_Write: Scrivi nella chiave ROCKEY2

EXTERN_C int WINAPI RY2_Write(int handle, int block_index, char* buffer512);

Input	handle	ROCKEY2 handle. E' lo handle risposto da RY2_Open
	block_index	Definisce il blocco. Specifica il blocco da scrivere. Valore da 0 a 4
	buffer512	Buffer di scrittura. Il buffer deve essere almeno di 512 byte per inserirvi il blocco di dimensione 512 byte.
Return	Codice Errore. Vedere i codici errore al Capitolo 4	

Capitolo 4 Codici Errore

MACRO	Value	Description
RY2ERR_SUCCESS	0	Successo
RY2ERR_NO_SUCH_DEVICE	0xA0100001	Chiave specificata no trovata (errore parametri)
RY2ERR_NOT_OPENED_DEVICE	0xA0100002	Eseguire la chiamata RY2_Open per aprire la chiave prima di lanciare questa chiamata (errore operazione)
RY2ERR_WRONG_UID	0xA0100003	UID errato (errore parametro)
RY2ERR_WRONG_INDEX	0xA0100004	Indicatore del blocco errato (errore parametro)
RY2ERR_TOO_LONG_SEED	0xA0100005	La stringa di caratteri Seed è più lunga di 64 byte quando lanci la GenUID(errore parametro)
RY2ERR_WRITE_PROTECT	0xA0100006	Tentativo di scrivere in una chiave protetta in scrittura (errore operazione)
RY2ERR_OPEN_DEVICE	0xA0100007	Errore aperture chiave (Errore Windows)
RY2ERR_READ_REPORT	0xA0100008	Errore lettura chiave (Errore Windows)
RY2ERR_WRITE_REPORT	0xA0100009	Errore scrittura chiave (Errore Windows)
RY2ERR_SETUP_DI_GET_DEVICE_INTERFACE_DETAIL	0xA010000A	Internal error (Windows error)
RY2ERR_GET_ATTRIBUTES	0xA010000B	Internal error (Windows error)
RY2ERR_GET_PREPARSED_DATA	0xA010000C	Internal error (Windows error)
RY2ERR_GETCAPS	0xA010000D	Internal error (Windows error)
RY2ERR_FREE_PREPARSED_DATA	0xA010000E	Internal error (Windows error)
RY2ERR_FLUSH_QUEUE	0xA010000F	Internal error (Windows error)
RY2ERR_SETUP_DI_CLASS_DEVS	0xA0100010	Internal error (Windows error)
RY2ERR_GET_SERIAL	0xA0100011	Internal error (Windows error)
RY2ERR_GET_PRODUCT_STRING	0xA0100012	Internal error (Windows error)
RY2ERR_TOO_LONG_DEVICE_DETAIL	0xA0100013	Internal error
RY2ERR_WRONG_REPORT_LENGTH	0xA0100020	Chiave sconosciuta (hardware error)
RY2ERR_VERIFY	0xA0100021	Errore verifica (hardware error)
RY2ERR_UNKNOWN_ERROR	0xA010FFFF	Errore sconosciuto(hardware error)

Capitolo 5 ROCKEY2 Envelope

Il programma Envelope di ROCKEY2 provvede a cifrare i file eseguibili (Win32 Portable Executable - PE) quali .exe, .dll. 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.

E' possibile anche proteggere file Flash (SWF) e .Net: trovate il tool e le descrizioni nelle cartelle Utilities/FlashEnv e Utilities/NetShell

Ry2Env32.exe nella directory "Utilities\ENVELOPer" lancia la ROCKEY2 Envelope. Vedete in Figura 5.1 la videata principale.

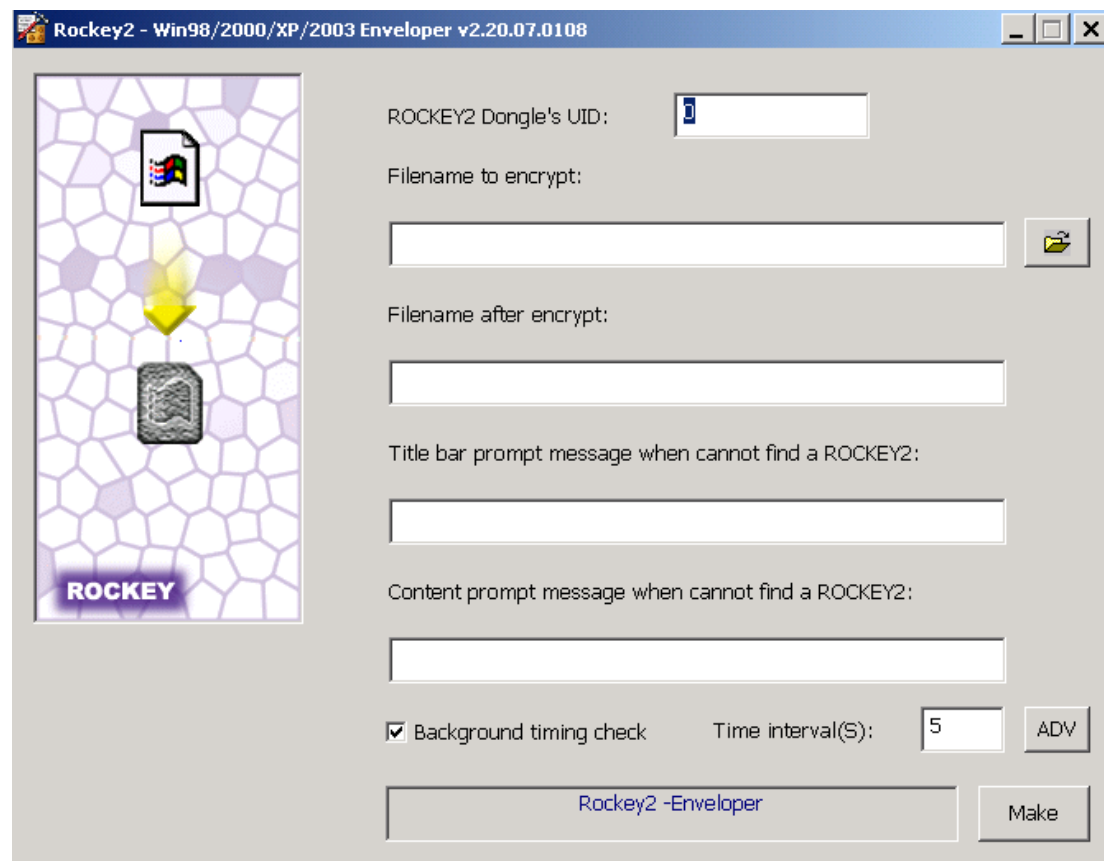


Figura 5.1

Nota: salvate i vostri file prima di cifrarli con la Envelope.

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.

5.1 Protezione con Envelope

Inserite una chiave ROCKEY2 di cui avrete precedentemente generato lo UID. Lanciate *Ry2Env32.exe* e per prima cosa inserite lo UID della chiave nel relativo campo. Selezionate il file da proteggere con il bottone "browse" o inserite il suo nome nel campo "File name to encrypt:". Poi inserite il nome del file protetto nel campo "File name after encrypt". Il programma propone di default il nuovo nome E24_vecchio-nome.

Nel campo "Titlebar prompt message when Rockey not found:" 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 "Content prompt message when Rockey not found:" inserite il messaggio che apparirà nel box di messaggio se all'avvio del programma la corretta chiave non è inserita.

Potete poi decidere ogni quanti secondi (Time Interval) la protezione automaticamente verifichi che la chiave non sia stata rimossa. Di default viene impostato 5 secondi. Vedere Figura 5.2.

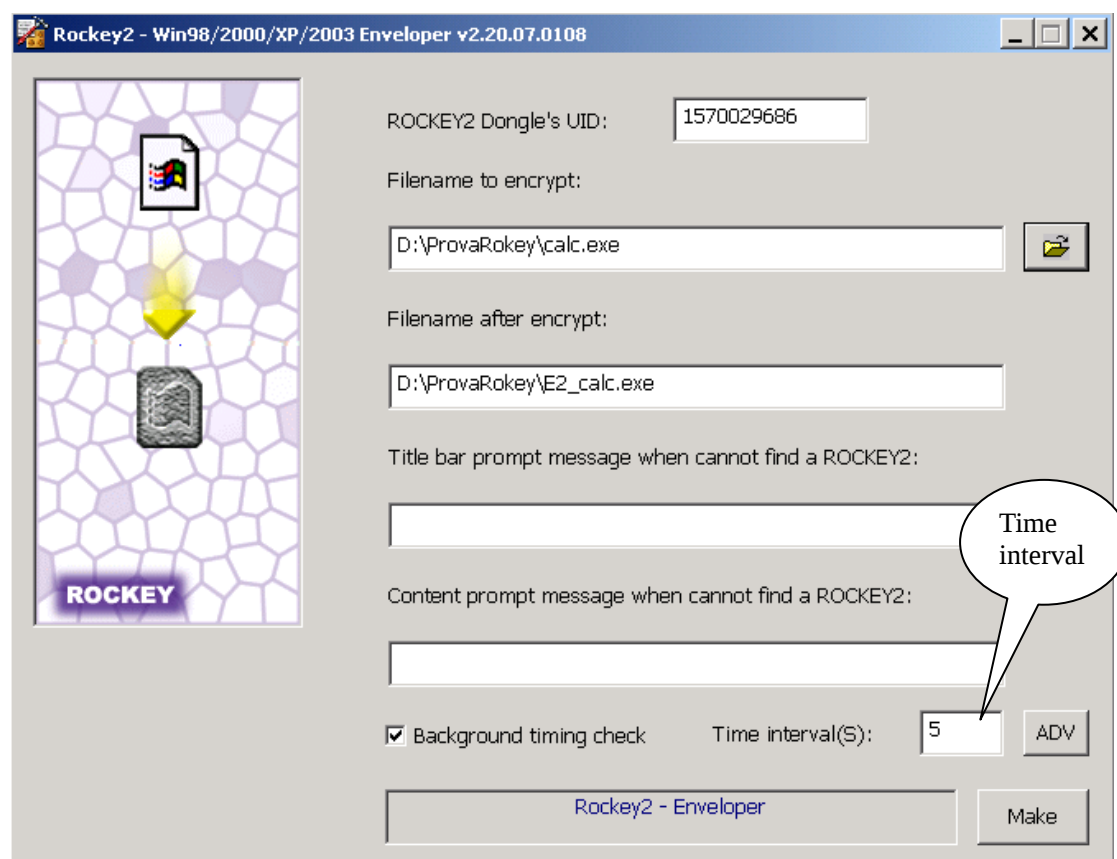


Figura 5.2

Ciccate Make per ottenere il file eseguibile protetto e cifrato.