

FEITIAN



Rockey4ND Product Introduction

V1.1

Feitian Technologies Co., Ltd.

Website: www.FTSafe.com

Revision History:

Date	Revision	Description

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 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 hardware 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.

Contents

Rockey4ND	1
Product Introduction	1
Chapter 1. Introduction	1
1.1 About ROCKEY4ND	1
1.2 Software Protection Mechanism of ROCKEY4ND.....	1
1.3 Hardware Configuration	2
1.4 ROCKEY4ND Benefits.....	2
1.5 How to Choose a Right Software Protection Solution.....	2
Chapter 2. ROCKEY4ND Hardware Features	4
2.1 ROCKEY4ND Internal Structure	4
2.2 ROCKEY4ND Hardware Interface.....	4
Chapter 3. Basic Concepts.....	5
3.1 Passwords.....	5
3.2 Order Code	5
3.3 Hardware ID	5
4.4 User Data Zone.....	5
3.5 Module Zone	5
3.6 User Algorithm Zone	6
3.7 User ID.....	6
3.8 Random Number	6
3.9 Seed and Return Values.....	6
Chapter 4. FAQs	7
4.1 Typical Solutions to Some Problems	7
4.2 FAQs	7

Chapter 1. Introduction

1.1 About ROCKEY4ND

ROCKEY4ND is an advanced software protection system that attaches to the USB port of a computer. Your software may be duplicated, but it will only run when your ROCKEY4ND “dongle” is attached to the computer. It can also limit the use of your software. Your application will interact with ROCKEY4ND at start-up and during runtime. If the dongle has been removed, or if an application module has been accessed a preset number of times, it can issue an error message and terminate, or take other alternative actions to ensure compliance with your licensing agreement. ROCKEY4ND is versatile and can be applied to other scenarios as required.

Unlike some competing products, ROCKEY4ND is a powerful miniature computer, with a CPU, memory and specialized firmware built-in that allows for a robust interaction with your application. You may write complex algorithms that are securely stored in the dongle, and then call those algorithms from time-to-time in your application. This method for software protection is strongly recommended and is very difficult to crack, and although ROCKEY4ND was designed to implement extremely high levels of security - it is also relatively easy to implement. The ROCKEY4ND API set has been simplified and improved based on experience gained from earlier versions.

The ROCKEY4ND product also includes an Envelope encryption tool - Envelope.exe for encrypting Windows Portable Executable files (such as .dll, .exe and .arx), .Net file, and data files. It is very easy to use. Only a few seconds will be taken to encrypt a file. The ROCKEY4ND Envelope tool is an ideal solution if you do not possess the source code for your application, or are unfamiliar with implementing an API. A security system that combines both the API set and the Envelope program will offer the greatest level of protection.

There are several components to the ROCKEY4ND software security solution and each of them will be discussed in this document. The following is an overview of the ROCKEY4ND components, along with a reference to where they will be discussed in this document:

- The ROCKEY4ND Envelope program (Envelope.exe) is a fast and convenient means of encrypting .exe, .dll, .arx and other Portable Executable (PE) files. This solution is ideal if you do not have access to source code or you are not familiar with the ROCKEY4ND API set. (See Chapter 6: ROCKEY4ND Envelope Encryption)
- The ROCKEY4ND Editor (Rockey4ND_Editor.exe) is a graphical tool for performing operations on the dongle. The Editor may be used to read data from and write data to the dongle, perform arithmetic operations in the dongle or test the dongle for malfunctions. (See Chapter 5: ROCKEY4ND Editor)
- ROCKEY4ND has an API set that you may use to create flexible and powerful software protection systems. This document provides VC ++ examples and other examples are provided on the CD-ROM under Samples directory. (See Chapter 7: ROCKEY4ND APIs)

1.2 Software Protection Mechanism of ROCKEY4ND

The protected software application must call the ROCKEY4ND dongle during run time, since the application is

dependant on the hardware. It is impossible to duplicate the chipset of the ROCKEY4ND hardware, and so too it is impossible to duplicate your software, ensuring your software is protected from piracy.

1.3 Hardware Configuration

User memory is divided into 2 parts. The size of each is 500 bytes. The length of the algorithm area is 128 units. The number of the modules is 64.

1.4 ROCKEY4ND Benefits

1. **Compact Design** – The dongle is compact and portable.
2. **High Speed** -- ROCKEY4ND was designed to process even very complex algorithms with minimal delay for your application. Users will typically notice no degradation in application performance as a result of ROCKY4ND being implemented.
3. **Ease of Use** – ROCKY4ND's reduced API set simplifies the programming effort in implementing API calls within your code, and the Envelope program has also been improved for increased security with the release of ROCKEY4ND. Developers lead time in implementing ROCKEY4ND is vastly reduced, saving both time and costs in deploying security into your software.
4. **High Security Levels** – Redesigned ROCKEY4ND offers a much higher level of security over previous version. ROCKEY4ND implements a two level security system to segregate users who require read only access from those who require administrative privileges. ROCKEY4ND has a built in time gate to prevent software tracking and is powerful enough to support developer defined algorithms that brings software protection to a new level of security.
5. **High Reliability** – FEITIAN employs an advanced customers managing system for ROCKEY4ND. We guarantee that the password of every customer is unique and that the hardware ID of every dongle is also unique. The password and hardware ID are burnt into the CPU, it is absolutely impossible to change, even for us—the manufacturer.
6. **Broad Support for Operating Systems** -- ROCKEY4ND protected applications may run on: Windows 98 SE/ME/2000 /XP/2003; Linux; MAC.
7. **Abundant Programming Language Interfaces** -- ROCKEY4ND provides interfaces for these common development tools: PB, DELPHI, VFP, VB, VC, C++ BUILDER and etc.

1.5 How to Choose a Right Software Protection Solution

The protection level applied to software not only depends on the dongle, but also on how the developer uses the dongle. Even if the dongle is the best in the world, a rudimentary implementation of security with your dongle can render the total security solution weak. ROCKEY4ND dongles offer two protection methods: envelope encryption and API encryption.

You may invoke the program Envelope.exe under Envelope directory of the SDK to perform the envelope encryption function. As the name indicates, envelope encryption adds an envelope to the user's designated files to protect them. The envelope will call the dongle. When users execute the program protected by the envelope, the protected program will automatically call the ROCKEY4ND and decide whether to allow the program to continue according to the results of the call. The envelope program directly encrypts the compiled files. The

advantage of envelope encryption is that it is very easy and quick to implement and the source code does not need to be modified. The envelope method is the ideal choice if there is no time for learning the API method or if the source code is lost or unavailable. The disadvantage is that an envelope program uses a rule based encryption method, and rule based encryption methods are not as strong as methods that use an encryption key. Also, envelope encryption cannot support script languages that cannot be compiled, such as VBA.

For API encryption, developers need to choose the appropriate language interface according to their programming language to access the dongle. API encryption was designed to be flexible; so you can make full use of the encryption functions of ROCKEY4ND. Developers can decide where and how to encrypt their software. API encryption is more secure than envelope encryption and especially so when the internal algorithm function of ROCKEY4ND is utilized. But API encryption must work with the original program and it can take the developer more time to become familiar with the API.

Chapter 2. ROCKEY4ND Hardware Features

2.1 ROCKEY4ND Internal Structure

At the core of ROCKEY4ND is a specialized CPU with a USB interface. It supports the USB 1.0 standard and is compatible with USB 2.0 standard. In addition to the CPU is a non-volatile memory chip that can save your data in the event of a power loss. The ROCKEY4ND functions are divided into User, Module and Algorithm zones. The developer may store important information (such as an application serial number) inside the dongle. You can write to the ROCKEY4ND dongle as many as 100,000 times – there is no appreciable limit on the numbers of reads. The ROCKEY4ND chip supports special functions for random number generation, seed code generation and user defined algorithm interpretation.

2.2 ROCKEY4ND Hardware Interface

ROCKEY4ND USB supports USB Standard 1.1. At the most 16 USB dongles can attach to a computer with a USB extension HUB. The LED of ROCKEY4ND USB indicates the status of the dongle. (In a normal state after the dongle is attached to the computer the LED will be on all the time. If the LED blinks it indicates that the driver is not installed. Other LED responses indicate hardware failure.)

Note: ROCKEY4ND is a plug and play USB device. To unplug a ROCKEY4ND while writing/reading, the dongle may cause crashes to the operating system in some instances.

Chapter 3. Basic Concepts

This chapter covers the basic concepts and functions of the ROCKEY4ND software protection system. All ROCKEY users should read this chapter carefully to familiarize themselves with ROCKEY.

3.1 Passwords

When developers purchase ROCKEY they will get 4 16-bit passwords. The first two are Basic passwords (first grade passwords); the last two are Advanced passwords (second grade passwords). The 4 passwords for the demo dongles in the SDK are: P1: C44C, P2: C8F8, P3: 0799, P4: C43B. The passwords are “burned” into the hardware so that neither the user nor the manufacturer may change them. The developers must input the 4 passwords correctly to have full access to the dongles. The developer should set any reference to the Advanced password set to zero in the application program that is delivered to the end user – you should never reveal the Advanced passwords to the end user in any form. The Basic passwords allow the end users to access all necessary ROCKEY functions. We will discuss when one should input the Basic passwords, and when both Basic and Advanced passwords are required in the chapters that follow.

3.2 Order Code

The Order Code is five to seven characters in length and corresponds to a unique customer password set. You may use the Order Code for reordering ROCKEY4ND to be sure that all of the units in your inventory are consistent.

3.3 Hardware ID

FEITIAN will burn a globally unique Hardware Identification (HID) number into each ROCKEY4ND dongle. The HID cannot be changed. You may use the HID to positively identify an individual ROCKEY4ND. The HID is readable with the Basic passwords. It is impossible to write HID even if you have the advanced passwords.

4.4 User Data Zone

The User Data Zone (UDZ) is a memory space that the developer can use to store data needed by the software protection system. Users can read from and write to this space at any time. The total UDZ is 1000 bytes. The UDZ is divided into 2 parts.

The low part (0-499 bytes): Users with any level of passwords have full permission (read/write). **The high part (500-999 bytes):** Users with basic passwords (password 1 and password 2) can only read the UDZ. Users with advanced passwords (password 3 and password 4) have full permission (read/write).

3.5 Module Zone

The Module Zone was designed for multi-module encryption. It may be used to store module specific data for

Envelope encryption and/or API calls.

A ROCKEY4ND module is a 16-bit protected memory space. There are 64 “modules” in each ROCKEY4ND dongle, so as many as 64 application modules may be protected with a single ROCKEY4ND dongle. The developer may write data into the ROCKEY4ND modules and then use that data, along with ROCKEY4ND functions, to create powerful and flexible software protection systems. If the content of the module is not “0” you can use the module; if it is “0” you cannot use the module. You may determine if a module is useable by analyzing the attributes of the module. The exact content can only be determined algorithmically.

ROCKEY4ND modules cannot be read and it can only be written with Advanced passwords.

The “Decrement” attribute can be read with the Basic passwords and can be written with the Advanced passwords.

3.6 User Algorithm Zone

The User Algorithm Zone (UAZ) is a user-defined area for instruction storage. The number of instructions that may be stored in the UAZ varies according to the ROCKEY4ND model. ROCKEY4ND supports a maximum of 128 instructions. (Please refer to Chapter 8 ROCKEY4ND Hardware Algorithms.)

The User Algorithm Zone (UAZ) cannot be read and may only be written with Advanced passwords.

3.7 User ID

The User ID is a 32-bit memory allocation that may be used to store an application serial number or other identification information.

It may be read with the Basic passwords and written with the Advanced passwords.

3.8 Random Number

ROCKEY4ND can generate a true random number from its hardware. The random number can be used to prevent tracing or used in hardware algorithms.

3.9 Seed and Return Values

ROCKEY4ND contains a proprietary algorithm that will generate four 16-bit return values from input of a 32-bit seed code and the Basic/Advanced passwords. ROCKEY dongles with the same passwords should return the same values if the seed codes are the same. The return values will be different for ROCKEY dongles with different Basic/Advanced passwords.

Chapter 4. FAQs

Some frequently asked questions about ROCKEY4ND are listed in this chapter. You may find the solution to your problems with the use of the ROCKEY4ND dongle hereinafter.

4.1 Typical Solutions to Some Problems

- Test the dongle using Rocky4ND_editor under *Editor* directory.
- Replace the current version of the driver with the newest version, which can be downloaded from Feitian website. The website will be updated between whiles.
- Check if the problem persists after using another computer with your device.
- Check if your computer has been attacked by a virus or the like, which may block the program you are using.

4.2 FAQs

4.2.1 What is an evaluation kit?

The evaluation kit is designed for developers to evaluate the dongle product. It usually includes a package, documentation, a CD-ROM, and a dongle. The dongle is the same as the formal dongle, except that the access password for it is public. If customers want to purchase the product after evaluation, a dongle with a unique password will be provided for security consideration.

4.2.2 What is the order number?

The order number is a reference number for management purpose in fact. It does not associate with the passwords of the dongle directly.

4.2.3 Is it possible that others can buy a dongle as same as mine?

That is impossible. The passwords of the dongle of each customer are different. We keep the record of each customer. We can sign a security agreement with you if necessary. We will deliver the dongle to you as required.

4.2.4 Are the passwords of ROCKEY4ND dongle secure enough?

Yes, they are very secure. They include 4 passwords divided into 2 levels. Each is 16 bits in length. The 1st level includes 2 basic passwords for basic operations on the dongle. The 2nd-level passwords are dedicated advanced passwords provided to developers for controlling writing to the dongle and defining encryption algorithms. These

2 passwords must not appear in the software delivered to end users. If the advanced passwords are entered in error and the special memory has been written 4 times, the dongle will be locked for 2 seconds. No operations can be performed during the 2 seconds. This measure prevents attempts of the passwords by attackers.

4.2.5 What are same-numbered dongles?

The dongles have the same order number. In other words, they share the same passwords. Each copy of the software is delivered with a dongle to end users. Since all the delivered dongles have the same number, developers do not need to re-compile each copy of the software.

4.2.6 What can I do if I forget the passwords of the dongle?

Use another dongle. Or, you must prove that you ordered that dongle before. For details, consult our post-sales.

4.2.7 Is it true that a data sharer can be used to share a dongle?

The data sharer can be prevented if you do as follows: generate a random number at the beginning of the program and store it at a fixed address in the memory of the dongle; and verify if the data at that address is equal to the random number at runtime of the program. If the program is also running on another computer, which works with the dongle, a different random number must have been written to that address.

4.2.8 Will it slow down the running of software to write a complex algorithm to the ROCKY4ND dongle?

No. The difference between the time consumed by the simplest algorithm and the time consumed by the most complex algorithm is merely several tens of milliseconds. If the complex algorithm is not invoked frequently, you cannot perceive the slowness.

4.2.9 What is the problem if my USB dongle is recognized as Unknown Device?

This problem occurs occasionally. Generally, your device is not attached properly to the computer, or some interference exists. Remove your dongle and try to attach it again.

4.2.10 Why can't I see the USB device in Device Manager when I use the dongle with a Windows 98 computer which has a USB port?

Maybe the USB supporting option is disabled in BIOS.

4.2.11 How can I update the software of the dongle?

If you are a testing user, you will be sent the last-minute updates. Otherwise, you can go to our website (<http://www.FTsafe.com>) to get the latest DK.

4.2.12 I was prompted “Rockey4ND.dll not found” when protecting FoxPro and VB programs by calling APIs. What is the problem?

Although Rocky4ND.dll is present under current directory, you must copy it to a system directory because FoxPro and VB programs find the dynamic-linking libraries only in system directory.

Appendix A: Contents of SDK Directory

Directory	Description
Setup.exe	Installer
FlieList.txt	List of files
Api32	32-bit APIs
Api64	64-bit APIs
Docs	User manual(s)
Driver For Win98	Driver for Windows 98 SE
Include	Header files
NetRockey	Network dongle DK
Samples	Sample programs
Utilities	Dongle Editor and Envelope Encryptor

Appendix B: Performance Comparison of Dongles

Feitian is always dedicated to provide products with high stability, integrity, and quality, and make continuous improvements. Developers can get free trial offerings from us. You are appreciated if you can complete the following form and send it to us.

Performance Comparison of Dongles				
Items for comparison	ROCKEY4ND	Competing Product		
		Y	N	?
USB interface device	✓			
Operating voltage as low as 2.2v	✓			
Passwords and ID number burned into CPU, even manufacturer cannot change them	✓			
Memory read/write unit	✓			
Unique hardware ID for each dongle	✓			
Able to work in parallel with dongles of the same or different kind without any problems	✓			
Able to work in series for same-numbered dongles	✓			
Good adaptability, works normally even when a printer is connected	✓			
No conflicts even when printing	✓			
Support for direct envelope encryption for executable files, without the need of source code of the software	✓			
Able to prevent the track and crack by debugging tools	✓			
Customizable onboard algorithms	✓			
Encrypted software can word under Windows 98 SE/2000/XP/2003	✓			
2-level password control, developer passwords do not appear in user software	✓			
Mass storage CPU program memory	✓			
1000 bytes or more user memory	✓			
Onboard time gate preventing track by software	✓			
Able to encrypt a set of software programs/ modules	✓			