FEITIAN

Rockey7.NET Remote Update Tool Help

V2.0

Feitian Technologies Co., Ltd.

Website: www.FTsafe.com

Revision History:

Date	Revision	Description
Sep. 2009	V1.0	1st release of the document
Sep. 2010	V2.0	2nd release of the document

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

Chapter 1. Overview

1.1 Introduction to Rockey7.NET

ROCKEY7.NET is the ideal solution to protect .NET application against piracy. The 32bits high performance smart card chip based hardware with built-in .NET virtual machine allows .NET applet being executed within the device. Software developers can download .NET applet to the device and make it work with outer .NET application. The secure communication technique is applied to protect the data transferred between the device and host machine. Each ROCKEY.NET dongle can run multiple .NET applets simultaneously so as to protect multiple .NET application at the same time. The design of ROCKEY7.NET follows the up-to-date .NET technology. Its stable and effective performance provides excellent protection to Microsoft .NET applications.

With the advent of .NET technology, its simple, powerful and effective features are widely accepted by the users in various fields. The .NET program will be compiled into an IL (Intermediate Language) scripts and being rendered in different .NET runtime environment. The same IL scripts can be used in different platforms, which can significantly reduce the development and maintenance cost. However, the simple structure of IL language makes it too easy to be decompiled into source code. Thus the .NET program is easy to be cracked. How to protect .NET IL scripts is the most important topic of .NET application protection. Normally, the following techniques can be applied to achieve the goal:

- Anti-debugging

  The protected .NET application has the feature that it cannot be debugged or audited by .NET debugger tools.

- JIT runtime decode

  The instructions of .NET application will be decoded before it is rendered by JIT in runtime. The.NET application in memory is not complete.

- Function body encryption

  The body of function will be encrypted with cryptographic algorithm. The .NET application is stored in cipher form.

- Keyword confusion

  The keywords in the .NET application like function name, variable name will be replaced with irrecognizable code. So even if the application is decompiled, it is not easy for cracker to understand the meaning of source code.

- Communication encryption

  For the applications involving communication with hardware, the transfer datagram is encrypted and

protected against interception.

All the above methods can protect the .NET application. But they have a common feature. The protected application is completely stored in the computer, regardless it is stored in cipher or plain format. So it is easy for experienced cracker to obtain the complete original .NET application by using decryption tools. However, ROCKEY7.NET is designed to terminate the risk coming in this situation.

ROCKEY7.NET software protection solution provides a unique “function migration” method to protect the .NET application. It can download a part of the functions in original application to its built-in .NET virtual machine and execute the code in its .NET runtime environment. The internal .NET applet can cooperate with outer application to achieve the same functionality as the unprotected application. The ROCKEY7.NET built-in .NET virtual machine runtime environment makes this innovative design achievable. Worldwide, only a few manufactures can develop .NET virtual machine runtime environment, Feitian is one of them. Feitian .NET virtual machine runtime environment has been certified by Microsoft. Based on 32bits high performance smart card chip, Feitian .NET smart card provides a stable, effective platform for .NET applets being executed onboard. It is the perfect environment for .NET smart card applications. ROCKEY7.NET solution is based on Feitian .NET smart card. The Enveloper can intelligently analysis the target .NET application, migrate the core part of the application to the Feitian .NET card automatically. The protected application is not complete. A core part of the program is protected by the Feitian .NET smart card. The migration concept can guarantee that the outer application can never be fully reversely decom3piled.

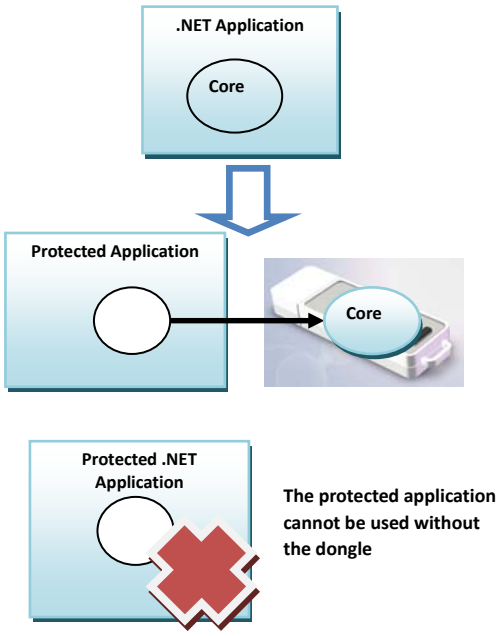

Figure 1.1 ROCKEY7.NET Software Protection Principle

ROCKEY7.NET provides many utilities to help developer maintain the entire software life cycle. The Enveloper, initialization tool, production tool, remote update tool can help developer protect and control the software remotely. Normally, there are several roles in software maintain cycle: administrator, developer, production staff,

sales staff and support staff. For each role, there are according tool to help developer perform the operation. This design can effectually separate the responsibility and task for each different role.

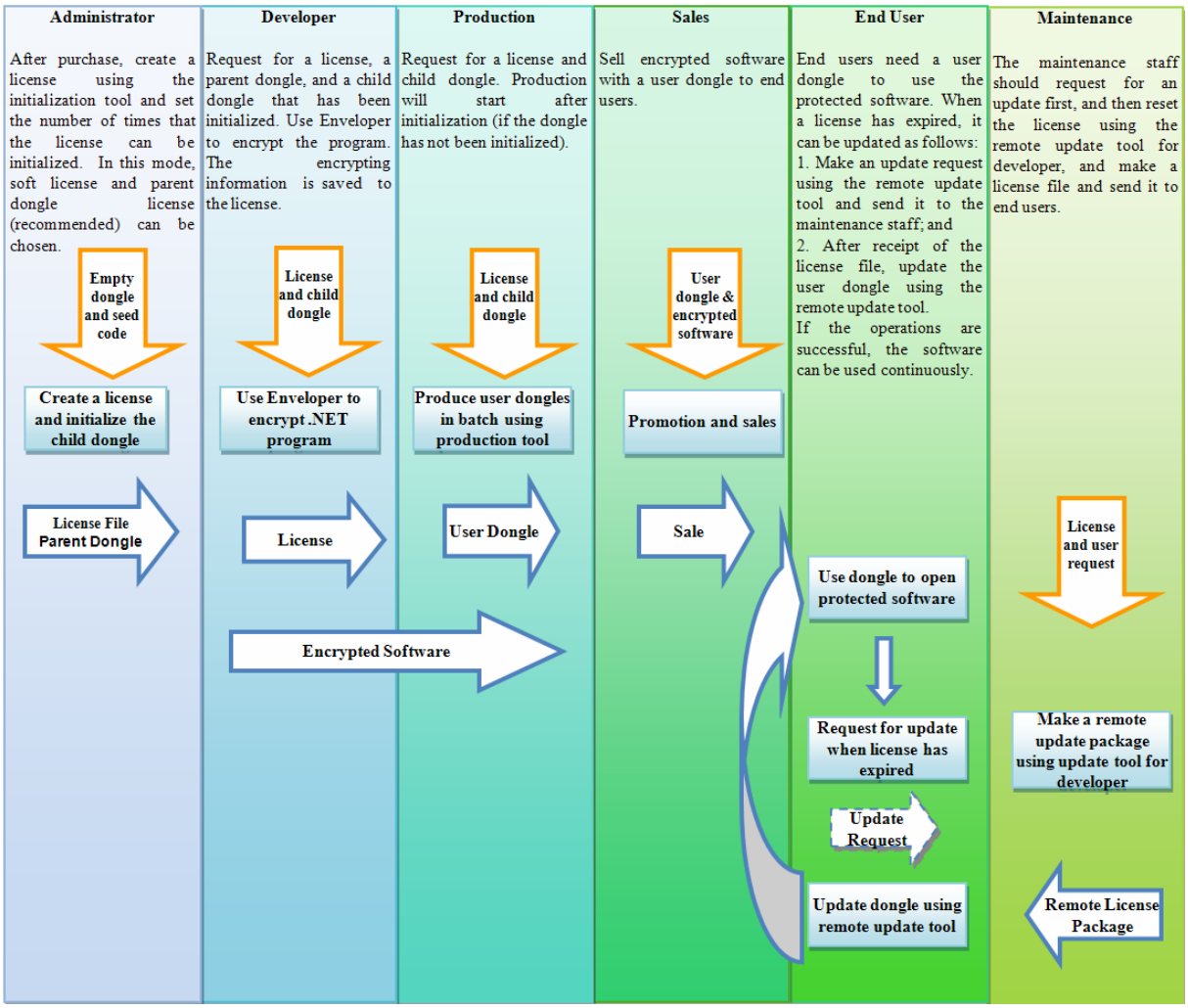

Figure 1.2 ROCKEY7.NET Software Maintenance Flow

1.1.1 ROCKEY7.NET Features

- 32-bit high performance smart card
- Globally unique hardware serial number
- User-defined 4-byte product ID and 8-byte management password
- No user installation of driver needed: CCID driver provided with operating system available or the driver can be installed automatically online
- Communicated packets are encrypted, preventing listening simulation software
- Counting or timing mode for user selection
- Easy and secure remote upgrade

- .NET virtual machine system with Feitian's own IPR
- Smart enveloper, no development work for encrypted product, smart and automatic analysis of .NET code functions of application, automatic migration of resulting algorithms and functions into card to run
- A complete set of easy-to-use tools for controllable license, and role and process-based management of encrypted products

1.1.2 Supported Environments

- Framework: Framework 2.0, Framework 3.0, Framework 3.5, Framework 4.0
- Supported development languages: C#, VB.NET, Delphi.NET, ASP.NET
- Supported .NET application programs: UI, console, service, control, and component programs
- Supported operating systems: Windows 2000, Windows 2003(32/64-bit), Windows XP(32/64-bit), Windows Vista(32/64-bit), Windows 2008 (32/64-bit), and Windows 7 (32/64-bit)

1.2 Introduction to ROCKEY7.NET Remote Update Tool

ROCKEY7.NET solution provides secure remote update plan to enable developers update the content of customer's dongle without physically call back the product. Developer can update the migrated files and the software license information in the dongle. Using the remote update solution can effectually make the software support work simpler and reduce the maintenance cost.

- Onboard AES algorithm based secure update solution

ROCKEY7.NET remote update package is encrypted with high strength AES cryptographic algorithm. The encryption key is stored within the hardware of the dongle. The entire remote update generation at developer site and deployment at client site is performed within the hardware device. The update file is stored in cipher form can effectively prevent the update content being exposed in transmission procedure.

- Fully customizable update content

ROCKEY7.NET remote update solution can update all the content in the dongle device except the PIN, SOPIN and UID, including the migrated functions, timer license and counter license.

The remote update feature enables the "protect once, deliver many" concept. Software developers only need to protect the software once and then, developer can bind the software with different licensing plan. Once the license of the software is expired, customer only needs to request a remote update package from the developer. Once customer wants to use more applications, developer can write more migrated functions to the dongle with remote update solution. In the entire procedure, customer does not need to send back the

hardware dongle to the developer. Developer can control the protection state remotely in the whole maintenance role.

- Once only remote update package

The built-in remote update tag guarantees each remote update package can only be used once at customer site. After a successful update, the update package will become invalid. This design can prevent customer perform the update operation more than one time.

- Bind with multiple feature

The remote package can be bind with different dongle's feature like HID, UID etc. This can guarantee that only specific customer can use the remote package. However, other customers cannot apply the remote package. Moreover, an expiry date is built-in the update package to make sure that customer cannot perform the update operation after the preset expiry date.

1.3 Remote Update Process

There are 4 steps for a remote update operation:

1. Customer uses client remote update tool to generate a remote update request and sent it to developer;
2. Developer use developer remote update tool to browse the customer's licensing state;
3. Developer sets the new software license to generate the remote update file and send it to customer; and
4. Customer uses the remote file to update the content of the dongle.

The entire procedure is clear and simple. The remote update plan is secure and effective.

Chapter 2. Using ROCKEY7.NET Remote Update Tool for Client

2.1 Generating Remote Update Request File

End users can use the remote update tool for client to generate the remote update request without inputting any product information. They need only to attach the ROCKEY7.NET dongle and specify the location of the request file, and then click Generate button to perform the operation. The remote update tool can detect the dongle and generate an encrypted remote update request file automatically.

Make sure that one and only one dongle has been attached to your computer when updating.

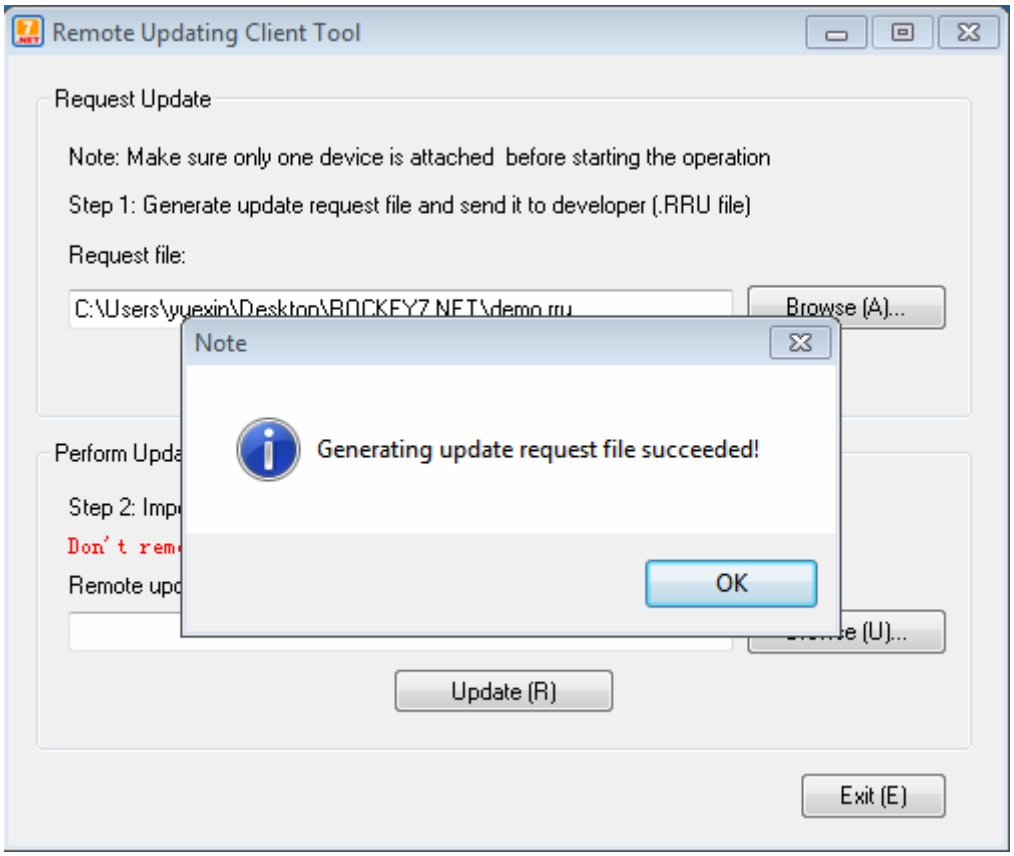

Figure 2.1 Remote Update Tool for Client

2.2 Updating with Remote Update File

After obtaining the remote update file from the developer, end users need to use the remote update tool for client to open the remote update file and click Update button to perform the update operation. After a successful

update, a message will be prompted as shown in the following figure:

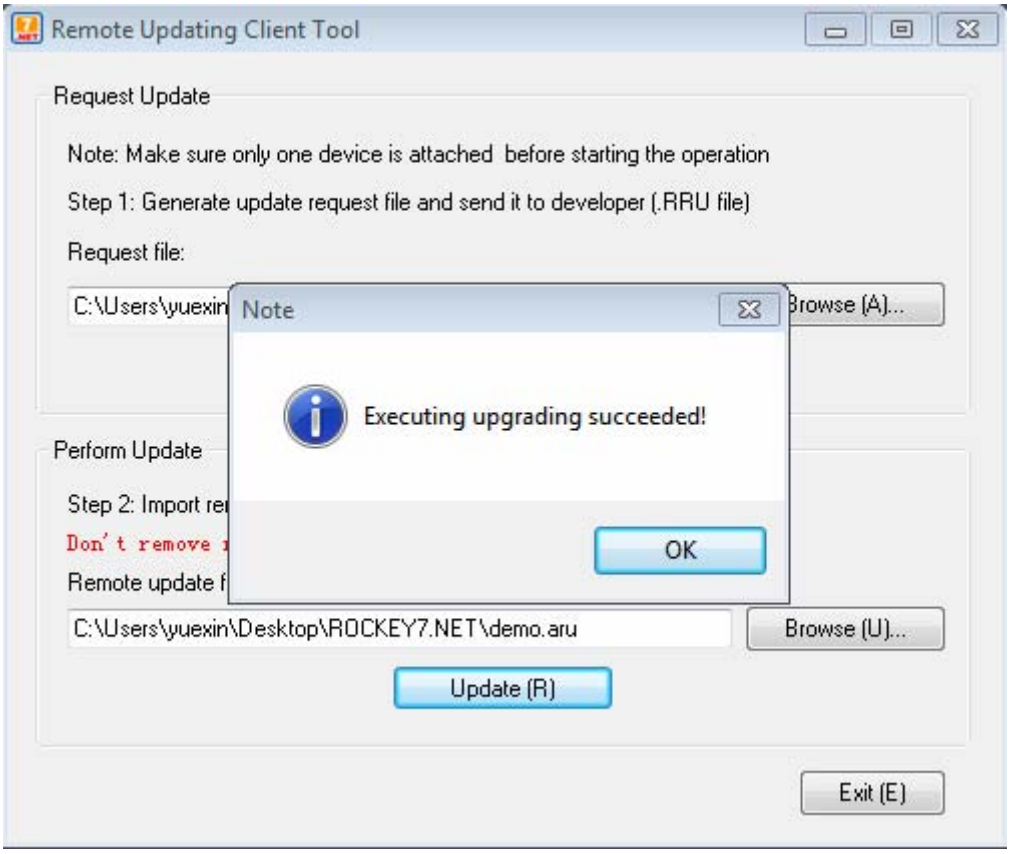

Figure 2.2 Applying Remote Update File

Chapter 3. Using ROCKEY7.NET Remote Update Tool for Developer

The remote update tool for developer is used to generate a remote update license file based on the remote update request from end users. There are three steps to generate the remote update file: open the remote update request from end user; set the binding condition, and set the new software license.

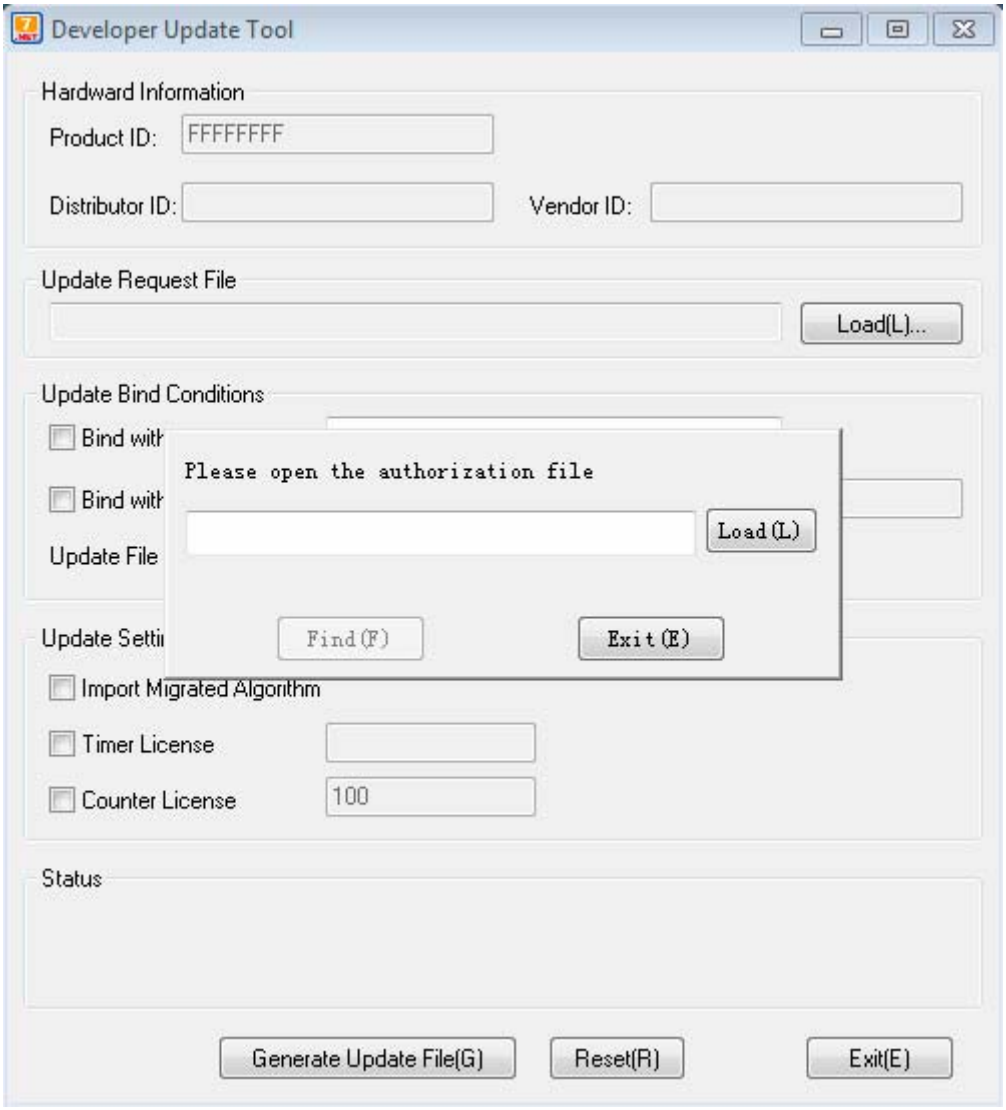

Figure 3.1 Remote Update Tool for Developer Logon

3.1 Opening Update Request

In the remote update tool for developer, choose a valid license file and enter the main interface. Open the update

request file from end user by choosing it and clicking Load button. The current status of license will be displayed in Update Settings area.

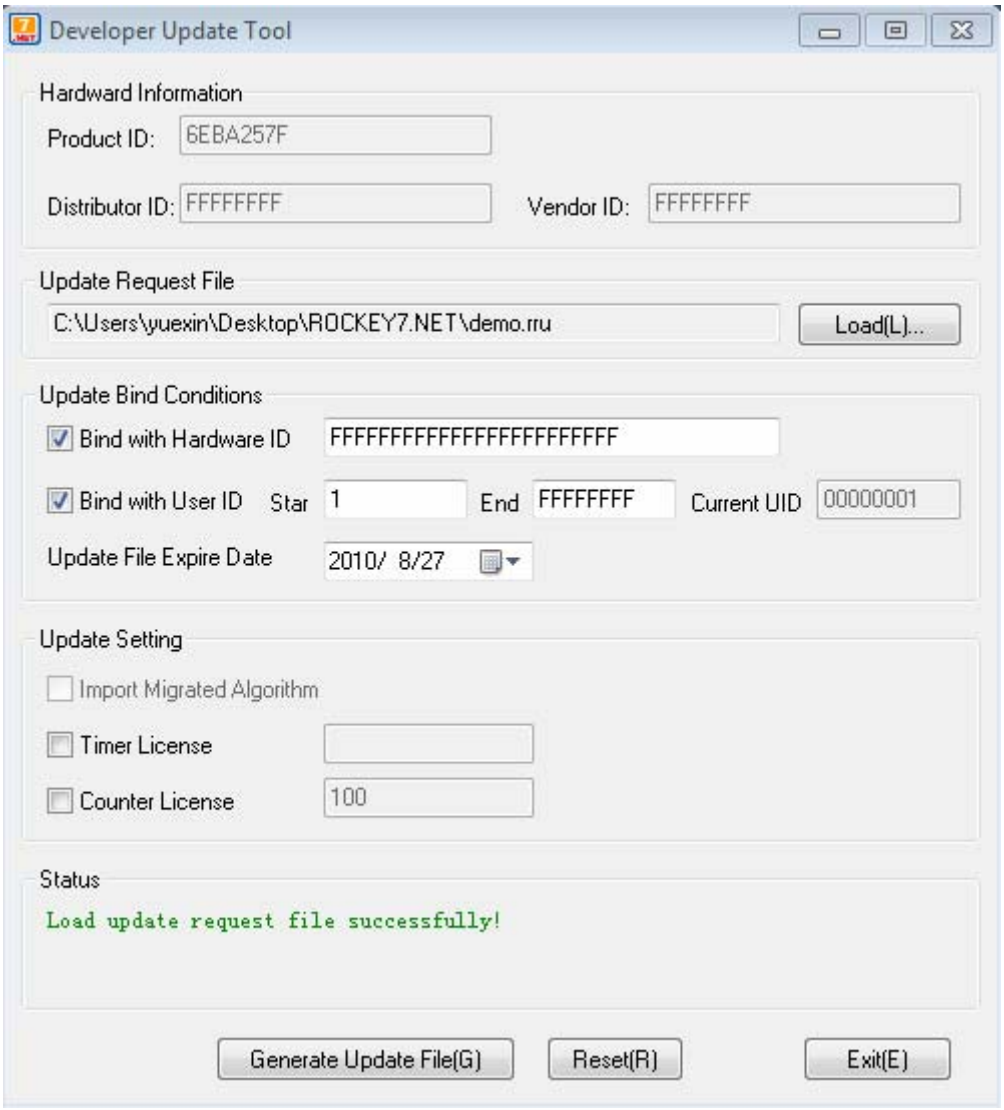

Figure 3.2 Opening Update Request

The hardware ID, user ID, and software license information for current user can also be displayed.

3.2 Setting Update Binding Information

Developers can set the binding condition to the remote update package like the HID, UID and package expiration date.

Binding with specific HID can guarantee that only the desired dongle device can be updated. Other dongles cannot be updated with the remote update file.

Binding with UID range can make sure only a special group of the customers can use the remote update file. Each user can only update the dongle for one time only.

The remote update package expiration date is used to control the time to perform the remote update operation. Once the package is expired, user can no longer use the remote update file.

3.3 Setting Software License

Developers need to open the project file generated by enveloper to set the new software license information. There are three parts of settings can be updated: the algorithm functions, the timer license and the counter license.

1) Algorithm Functions

The algorithm functions are the functions that are migrated to the dongle by the enveloper. When users use the same software as before, there is no need to update the algorithm functions. However, if developers want to allow users to use more application programs, the algorithm functions need to be updated.

2) Timer License

The timer license is used to limit software by time. Developers can set software timer license to an expiration date, or restrict the use of software to a specific number of days or hours.

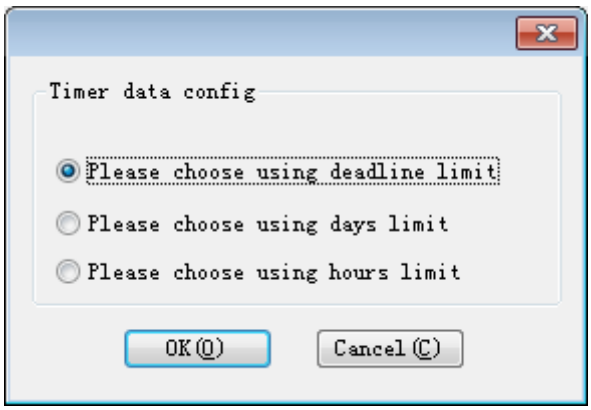

Figure 3.3 Timer License Options

When a deadline is specified, the software can only be used until the expiration date under the license. Users cannot open the program after the preset expiry date. In this case, user must update the timer license remotely by using the remote update tool, or use another valid dongle to continue using the protected program.

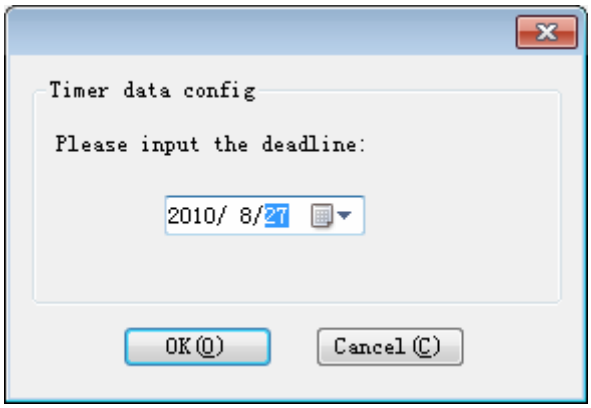

Figure 3.4 Expiration Date Setting

When a number of days is specified, the licensed period of use of the software begins when the user uses the software for the first time. After the preset period of days, the license will expire and the user must update the timer license remotely by using the remote update tool, or the user can use another valid dongle to continue using the protected program.

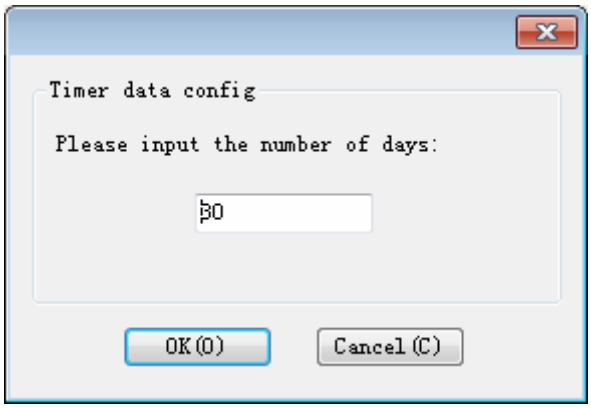

Figure 3.5 Number of Days Setting

When a number of hours is specified, the software can be used within an accumulated period of time. That is, the time is counted from the startup of the software to the closure each time it is used. Finally when the accumulated amount of time reaches the configured number of hours, the user cannot use the software any longer if he/she has not updated the license or changed to use another valid dongle. In this way, the licensed time can be controlled precisely.

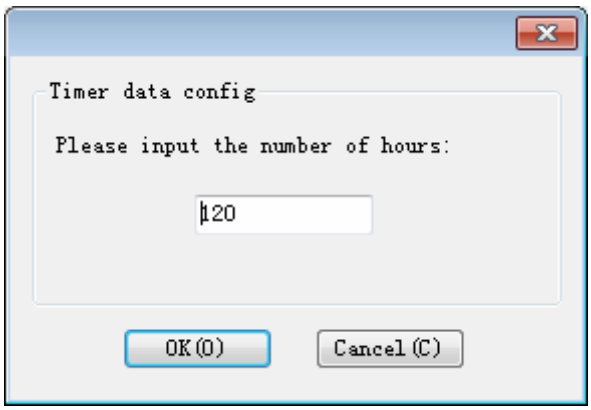

Figure 3.6 Number of Hours Setting

3) Counter License

The counter license is used to control the number of times to use the software. When the number of times for which the software has been used exceeds the limit, the program can no longer be opened. Users must update the counter license remotely by using the remote update tool, or use another valid dongle to continue using the protected program.

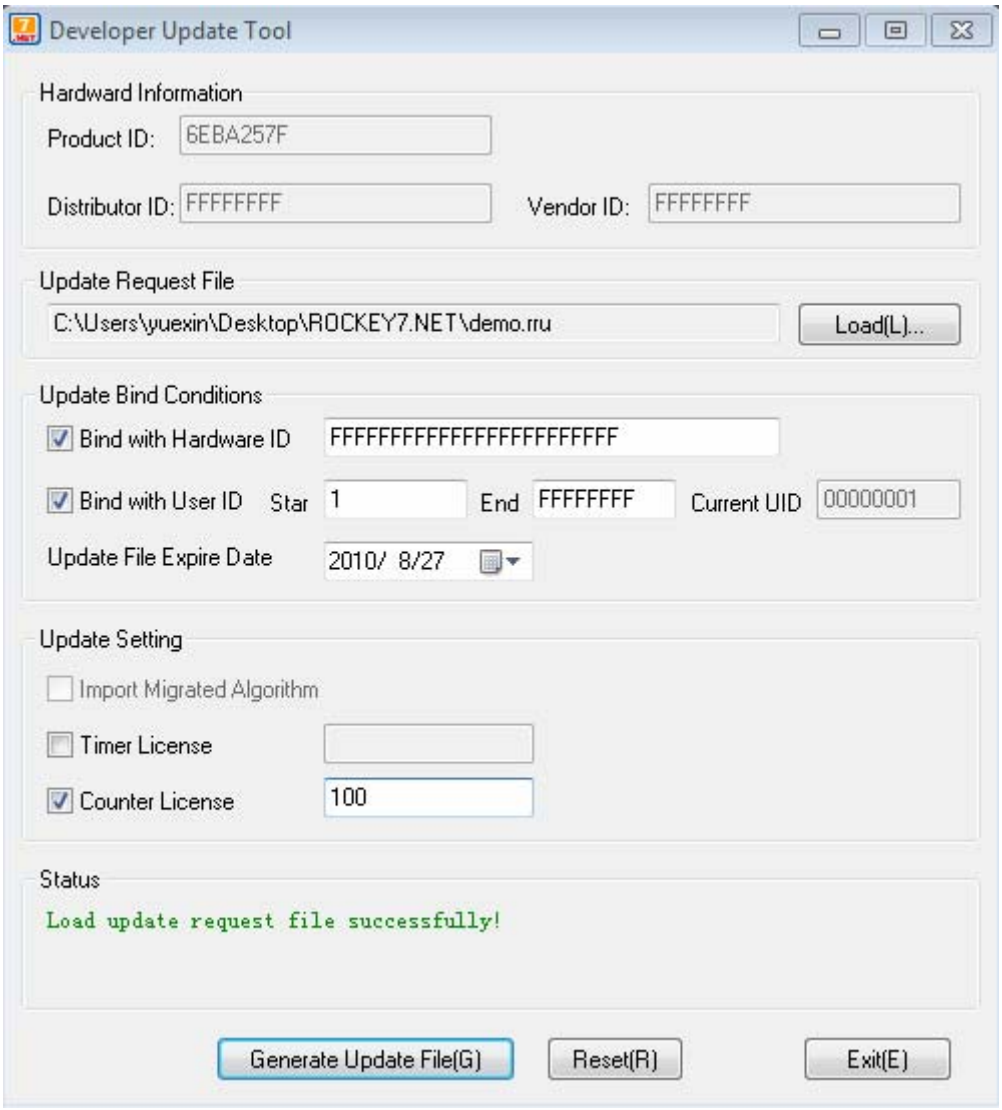

Figure 3.7 Counter License Settings

After setting the software license, click Generate Update File button to generate the remote update file. After the operation, a message will be show as followed. Developers can send the remote update file to end users.