CrypKey™

*BATTLE-PROVEN
SOFTWARE
PROTECTION
AND
LICENSE SECURITY*

Instant
User Manual

CrypKey Instant User Manual

CrypKey (Canada) Inc. License Agreement

Grant Of Rights

In consideration of payment, CrypKey (Canada) Inc. ("CrypKey") grants to the purchasing company (the "Customer") the non-exclusive right to possess, use, and make and distribute unlimited copies of the machine-executable code version of the CrypKey Software Licensing System, including all revisions, modifications, and updates thereto furnished to the customer, together with the written User Manuals in relation thereto (collectively the "Software").

Intended Purpose

The Software is intended to be linked with and incorporated into the product, including, but limited to, the foundation module and installation routines forming a part thereof. No right to distribute the Software on a standalone basis is intended by this License Agreement. Any other use of the Software requires written consent from CrypKey. The customer may not reverse engineer, modify, nor create derivative works based on the Software without written consent from CrypKey, except as permitted by acceptable law.

Ownership

All patents, copyrights, and other proprietary rights in the Software are, and shall remain, the exclusive property of CrypKey or its suppliers. The Customer may not assign nor transfer the rights granted in the License Agreement to any person, except the Customer's subsidiaries and affiliates, without written consent from CrypKey.

Limited Warranty

CrypKey warrants to the Customer that the Software will operate essentially as described in CrypKey brochures and documentation. CrypKey warrants that the media on which the Software is recorded shall be free from defects in materials and workmanship under normal use and service for 60 days from the date of the Customer's invoice. If failure of the media is a result of accident, abuse, or misapplication of the Software, CrypKey shall not be responsible for its replacement. Applicable law may imply warranties that cannot be excluded or can be excluded only to a limited extent. This Agreement shall be reached and construed subject to such laws.

No Other Warranties

THE LIMITED WARRANTY SET FORTH HEREIN IS IN LIEU OF, AND CRYPKEY DISCLAIMS, ANY AND ALL OTHER WARRANTIES (EXPRESS OR IMPLIED) WITH RESPECT TO THE SOFTWARE, INCLUDING ANY AND IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Remedies

Except in connection with a claim for infringement of copyright, patent, or other intellectual property right, the Customer's sole and exclusive remedy for a breach of warranty shall be: (a) the return of the initial fee paid for the rights granted herein or (b) the correction or replacement of defective software or media. Corrected or replaced Software or media will be warranted to the same extent as the original Software or media for the remainder of the original warranty period or 30 days from the date of receipt by the customer, whichever is longer.

Limitation Of Liability

IN NO EVENT SHALL CRYPKEY BE LIABLE TO THE CUSTOMER FOR INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGE. IN NO EVENT SHALL CRYPKEY (CANADA) INC.'S AGGREGATE LIABILITY TO THE CUSTOMER EXCEED THE AMOUNTS PAID TO CRYPKEY BY THE CUSTOMER FOR THE SOFTWARE.

Table of Contents

S E C T I O N   P A G E

List of Tables and Figures

TABLE   PAGE

FIGURE   PAGE

Overview

Welcome to CrypKey Instant and the CrypKey world of software protection.

T rust CrypKey Instant's software security system to protect your software against illegal copying. CrypKey Instant rewrites your executable files, protecting them from illegal duplication.

CrypKey Instant offers the same functionality as CrypKey Software Developer's Kit (SDK), differing only in the way you implement the software protection into your product. CrypKey Instant wraps executable files and requires no source code programming, whereas CrypKey SDK requires you to program function calls into your application.

CrypKey Instant protects your product by writing an invisible signature to your hard drive. Part of the CrypKey Instant advantage stems from its trial period feature, which allows users to try your product for a limited time without authorization.

CrypKey Instant allows developers to:

- protect software products against unauthorized usage on a turnkey basis (this easy-to-use solution requires no associated components)

- limit software use to a number of days or software runs

- communicate authorizations via phone, fax, or email

CrypKey Instant does not use hardware or disk keys and includes a conversion program to protect distributors' executables. Our payment options offer even further flexibility. Depending on your needs, buy the total package, or purchase CrypKey Instant on a per-use basis.

1.1   About CrypKey (Canada) Inc.

The unique CrypKey copy protection and license control software came into being in 1992 with the goal of developing a better way for a large engineering company to protect its own software. CrypKey worked so well that it soon became its own commercial product and quickly outsold the product it was created to protect!

The CrypKey product and service business spun off into CrypKey (Canada) Inc. by its current management in March 2002. The CrypKey team has developed new, ultra-secure, industry-first, CloneBusterTM technology for its version 6.0.

CrypKey has delivered battle-proven software copy and license protection for thousands of companies worldwide since 1992, including: Nokia, Ericson, IBM, Microsoft Caterpillar, Eaton, Dupont, Fujitsu, Minolta, HP, Honeywell, 3M, Lockheed Martin, Mobil, Procter&Gamble, Siemens, Verizon, Sybase, Bell&Howell, Kodak, Allen Bradley, and ABB.

1.2   How to Use This Book

This manual is about two business relationships:

- your relationship, as a software vendor, with CrypKey (Canada) Inc.: how you obtain and utilize CrypKey Instant and the Site Key Generator to protect and license your software as you distribute it to customers

- your relationship with your customers and distributors: how you provide, protect, and license your applications

Following is a summary of the manual's contents, as well as strategies for using it.

1.2.1   Summary of Contents

Chapter 1, *Overview*, contains information about the following topics:

- system requirements
- technical support available at CrypKey (Canada) Inc.
- trial keys and license keys
- general CrypKey licensing process
- new features in CrypKey 6.0
- procedures for upgrading to CrypKey 6.0

Chapter 2, *Authorization and Licensing*, details how to obtain your developer keys and the site key for your copy of the Site Key Generator and explains the process of obtaining, testing, and implementing CrypKey Instant protection for your software.

Chapter 3, *Installation*, focuses on the installation, from CD or downloaded files, and setup of the CrypKey software and associated drivers (Windows 3.1/9x/ME/NT/2000/XP), files, and software.

Chapter 4, *Demonstration Program*, uses an example protected (and unauthorized) application, the Microsoft *Calculator* program, to demonstrate how a site code and site key are generated and how the site key is inserted into the example application to authorize its use.

Chapter 5, *Site Key Generator*, discusses an essential component of the licensing process, the Site Key Generator, and how it is used to configure the protection features for your software and to issue licenses to your customers and distributors. An important element of this chapter is the discussion of options and levels.

Chapter 6, *Using CrypKey Instant*, discusses StealthPlus^{TM} anti-hacking and automatic file-distribution feature, CrypWrap encryption function, use of master and user keys, and procedures for applying CrypKey Instant features to protect your product. These include specifying levels and options, enabling license transfer commands between directories or computers, adjusting license restrictions, and, if required, setting up the interface with CASPER, the CrypKey automated payment, registration and authorization system.

Chapter 7, *Network Licensing*, discusses the operating systems and network platforms that CrypKey Instant supports and procedures for installing CrypKey Instant and associated drivers in these environments.

Chapter 8, *Moving Protected Products*, discusses the CrypKey Instant capabilities for transferring licenses between directories and between computers.

Chapter 9, *Frequently Asked Questions*, discusses general and technical questions that users commonly raise about CrypKey Instant.

Chapter 10, *Troubleshooting*, discusses the most common errors that arise using CrypKey Instant, particularly with the CrypKey License Service, as well as Windows NT diagnostics, NetWare issues, and the general information that you need to provide to CrypKey Support staff if you have a problem requiring their assistance.

Chapter 11, *Appendix*, contains a CrypKey Instant and operating system file matrix, CrypKey program flowchart, and various network configuration diagrams.

At the end of the manual is a *Glossary*.

1.2.2   Strategies for Using This Manual

If you are new to CrypKey, we recommend that you carefully read the *Overview*, *Authorization and Licensing*, *Installation*, and *Demo Programs* chapters, and follow the instructions to try out CrypKey's functionality. After reviewing these chapters and examples, you'll be ready to work with the main procedural chapters of the manual: Chapter 5, *Site Key Generator* and Chapter 6, *Using CrypKey Instant*. These chapters, along with Chapter 7, *Network Licensing*, are your main resources for day-to-day use of CrypKey Instant.

If you are experiencing a problem with CrypKey Instant, we suggest initially reviewing the *Frequently Asked Questions* and *Troubleshooting* chapters, as well as the *Appendix*. If the causes of the problem and possible solutions are not readily apparent at that point, please contact CrypKey Support (see Sec. 1.4: Technical Support).

1.2.3 Special Icons

The following icons are used throughout the manual to convey the meanings shown:

DON'T FORGET

GLAD COMPUTER

WATCH OUT

1.3 **System Requirements**

To use CrypKey Instant, you require:

- 486 (or better) microprocessor, with 64MB RAM and 25MB of free space on your hard drive

- VGA color monitor

- mouse

- Windows 3.1/9x/ME/NT/XP/2000

1.4 **Technical Support**

CrypKey Instant includes 60 days of free technical support, starting from your date of purchase. Our customer service representatives, while always pleased to take your call, ask that you review the following checklist before requesting their assistance:

- read the manual (most problems can be solved by adhering to the specific information contained in this document)

- work through the demo, which provides a basic understanding of CrypKey Instant

- test the sample program within the scenarios you are investigating—again, most questions can be answered using this method; if problems persist, try the same situation with the example.exe

If these alternatives do not satisfy your requirements, please contact us by phone or email. Our business contact information is listed below.

CrypKey (Canada) Inc.

World Headquarters:

Mailing Address	CrypKey (Canada) Inc.
	The Devenish Heritage Building
	908 - 17th Avenue SW
	Suite 208
	Calgary, Alberta
	T2T 0A3 Canada

World HQ Phone:	1-403-398-8011
Regular Business Line:	1-403-258-6274
Fax Line:	1-403-264-8838
Support email	support@crypkey.com
Internet	http://crypkey.com

Pacific Rim Office:

Email	Greg.Wible@crypkey.com
Phone:	1-562-989-8976
eFax:	1-208-978-8503

1.5 Subscription Updates

You can visit the following site for the latest subscription and support news:

http://crypkey.com/support/policy/policy.html

1.6　About Your CrypKey License

CrypKey Instant includes a 30-day trial period that allows you to evaluate the full functionality of the system and then obtain your license only when you are satisfied with its performance. All of the features of CrypKey Instant are available to you during the trial period. Please note that CrypKey cannot be returned once you have been issued the developer keys for your product(s).

For the detailed steps of the CrypKey implementation process, see Sec. 2.3 (p. 37).

CrypKey Instant embeds the CrypKey licensing protection system within your application executable, without requiring any changes to the source code.

CrypKey (Canada) Inc. also offers the CrypKey Software Developer Kit (SDK), a software licensing system with which you can protect your application using library security functions. Using CrypKey SDK, you embed the primary CrypKey functions in the source code. These include initialization, license verification, site code generation, and termination features.

A third CrypKey product is CASPER (CrypKey Automated Software Protection and Electronic Registration), which automates the transmission of payments and authorization requests from your customers to you and of licenses issued by you to your customers.

1.6.1　Using CrypKey—Synopsis

CrypKey Instant enables you to wrap your unprotected executable or DLL into a package that includes copy protection, trial license functions, and a license user interface.

Figure 1 on the next page outlines the process.

Vendor develops application (executable with DLLs).

Vendor uses product keys received from CrypKey Canada Inc. to apply CrypKey Instant protection to application.

Vendor sends application with Trial License to Customer.

Customer opens application on a trial basis.

Customer obtains site code from Licensing Configuration window. (1)

Vendor enters site code into Site Key Generator and produces a site key. (2)

Customer sends site code to Vendor, requesting license authorization to use application.

Vendor sends site key to Customer.

Customer enters site key into application License Configuration window and receives license authorization message. (3)

Figure 1: Overview of Typical CrypKey Licensing Process

Notes on Figure 1

1. A CrypKey license interface appears when the trial license has expired or when invoked by the user. The interface provides the user with a site code, which is based on a special internal hardware signature that is unique to the personal computer on which the application is installed.

2. The vendor enters the site code into the Site Key Generator and specifies the type of license to be provided to the user. A Site Key is generated and sent to the user. The site key contains your specified levels, options, and permissions, collectively called the license, in encrypted form. Any site key you generate works only with the installed application that created the site code provided by the customer. The Site Key Generator automatically verifies that the site code given to it is an authentic one generated by the application running on the customer's computer.

3. CrypKey, running on your customer's computer, automatically tracks restrictions in terms of days or runs and invalidates the license when the time period expires or the number of runs is used. The license is uniquely specific to the computer on which the application runs. If the customer copies the program and its license files to another computer, the license becomes invalid on that machine and does not allow access. This occurs because the CrypKey system is capable of identifying the exact computer for which the license was issued, without requiring an external hardware (dongle) or floppy disk key.

1.6.2   Trial Keys and License Keys

This user manual contains example User and Master Keys (see below) for use during your trial period. These temporary keys **are not** intended for distribution with your product. If you distribute your product with these temporary User and Master Keys, recipients who have CrypKey can to unlock your product. Since all Site Key Generators can create keys for any program that uses the temporary keys, the only keys you should distribute with your product are those specifically created for your product.

Example Keys:

- User Key: D050 815C D1A2 A79D B103

- Master Key (16-bit):

  2A5D 57C4 1B4C 135B F09E 17F7 600B 2D70 79E8 F275 C36A

- Master Key (32-bit):

  F2C938D2D34678D2E9217C18D78EA6A8E466CF49520F92CDD1B6916BD460
  D60E7C7B4CC7CC1750BD7188F90AC132B915E82FC8FA60A1D299DA0F28E
  A3C66BD42DB0BE62149DAAEE4DBA55C0E70CE1C13BD343F8B7573ABC1E
  7DA0695955AB2BD377F50A9BE29A04CF816B30CD171E1509AD65100C999E
  52A35F45A215212A970

CrypKey Instant offers two types of developer keys: those related to the example file and those locking CrypKey to your product. Think of keys as alphanumeric strings of text. Note that you require the following four keys to run CrypKey Instant:

- User Key: created from the password that you set up for your application program

- Master Key: created from the file name of your application program, plus other pertinent information

- Site Key (for the Site Key Generator): enables you to authorize your product using your Site Key Generator

- Site Key (for CrypKey Instant): allows you to run CrypKey Instant without limitations

For instructions for obtaining your permanent CrypKey Instant keys, see Chapter 2: Authorization and Licensing.

1.6.3   Ready-To-Try Licensing

Ready-to-try licensing refers to CrypKey Instant's trial period. This feature allows you to distribute products with an automatic license, meaning users only call for authorization once the time limit expires. Your programmers control the length of the trial period. Once the license expires, you issue users with a new, full license key.

1.6.4   Security of Automatic Licensing

If reinstalling trial periods were possible, ready-to-try licensing would be useless. Users could continue reinstalling your product without authorization, defeating the purpose of CrypKey Instant.

We eliminate this uncertainty by writing an invisible signature to your user's hard drive, which remains on the computer even after your product is uninstalled. The signature is

embedded in an area that users do not typically access. Users can read, write, and delete files on their hard drive without affecting or altering the signature. Signatures are transparent to users and do not affect computer functionality.

Note that if you uninstall an application protected by CrypKey Instant that has already commenced its trial license and then reinstall it, the trial license is longer in effect.

1.7   New Features in Version 6.0

CrypKey, as a concept, has proven itself a hundred times over in the software marketplace. Our next step was to perfect CrypKey's performance. Our goal with the present release is to make CrypKey perform to a very high standard of security and robustness on all the platforms on which it runs. With Version 6.0, we feel we have succeeded in this goal.

CrypKey 6.0 has benefited from the experience of our now-sizable customer base. We have concentrated on tracking down and fixing every known problem on the many platforms CrypKey supports. The result is software that is robust. Before this release, 99% of all support problems were fixed just by sending this software.

In summary, CrypKey Instant has the following capabilities:

- it protects DOS, Win16, and Win32 programs *with no source code changes* in one program

- it does network floating licensing with no source code changes

- it supports international languages and enables you to switch or add languages at runtime

- it encrypts data files

The changes that we've made in CrypKey Instant 6.0 include the following:

- CloneBuster™ technology for hard drive serial number (HDSN) recognition

- EasyLicense

- dynamic multi-key encryption

- enhanced anti-hacking capability (StealthPLUS™)

- CrypWrap, which protects non-executable files

- file auto-distribution

- license directory redirection

These new features are described in more detail below.

1.7.1   CloneBuster^{TM} Technology

Software developers are discovering they are losing billions of dollars in a worldwide massive license theft of large scale. Fuelled by the recent surge in use of very legal low-cost hard drive (HD) cloning, or "ghosting", software, easily-obtained $49 utilities with names like Ghost and XXCopy are rendering once-popular copy protection techniques useless, generating fast lucrative returns for software pirates.

Many popular copy protection technologies that depend on placing some type of simple software footprint are now easily defeated by these new HD cloning techniques, and are no longer an effective option. Many unproven start-up venture-capital backed "rights management platform" providers are not practically viable: they offer grand (and often very expensive) protection schemes that fail to recognize all the numerous firewall, integration, distributed deployment and support issues generated by their "connected" product vision. Hardware dongles provide limited protection against to HD cloning, but are expensive and unpopular with end users.

CrypKey 6.0, which includes CloneBuster^{TM} technology, effectively solves the cloning problem.

Most modern IDE hard drives have burned-in serial numbers (HDSN). Not to be confused with the easily changed volume serial number, the HDSN is a permanent read-only attribute of a personal computer hard drive. The HDSN is very difficult to access, but the new CrypKey SDK 6.0 with CloneBuster^{TM} technology has this ability (patent pending). Leveraging the ten-year battle-proven CrypKey protection architecture, CloneBuster^{TM} detects and logs the HDSN, model number and firmware identifier, and then uses this information in its proprietary licensing algorithms. Although HD cloning programs succeed in breaking other simple copy protection schemes in order to copy an entire hard drive, they cannot achieve this against CrypKey when it is armed with CloneBuster^{TM}.

1.7.2   EasyLicense

Some customers need the simplest possible form of copy protection: a particular application runs only on a particular computer. These customers do not want to deal with any associated issues of transfer, network license, trial period, or number of copies. Whether the software gets offloaded and put back, or is deleted and restored later, or the entire hard drive is erased and restored, the application still runs on the computer.

EasyLicense offers this type of protection coupled with simplicity.

1.7.3   Dynamic Encryption

We have increased the bit size of our Site Code and Site Key encryption. Never satisfied with good enough, we have also created a "dynamic multiple encryption key" scheme, so that encryption keys are constantly changing on the fly, truly a code-breaker's nightmare. This also halts any attempts to create a rogue "key generator."

1.7.4   Enhanced Anti-Hacking

StealthPLUS^{TM}, our anti-hacking layer included with CrypKey, is a critical component, as it stops the hacker from reverse engineering and circumventing the copy protection. StealthPLUS^{TM} encrypts your binary file and guards against program patches while it is in memory. We have enhanced StealthPLUS^{TM} so that it partially unencrypt programs while it runs in memory and re-encrypt the parts that are not running. The program will team up in memory with a special "symbiotic" process that unencrypts parts as needed, dramatically decreasing vulnerability—truly a hacker's nightmare.

1.7.5   Protection of Non-Executable Files

The new CrypWrap function issues licenses to unwrap regular files (i.e., non-executables). CrypWrap works for regular files just as CrypKey does for running executables.

You can use CrypWrap to:

- wrap up multiple files into a single file, and send this protected file safely to its destination

- wrap software updates into a single file and make it available on the Web, while providing customers with limited-duration licenses to access the file

Note that CrypWrap self extracts and installs all the CrypKey runtime files required, including the NT Driver.

To demonstrate CrypWrap, we have protected the CrypKey Instant Help File, found in your directories. In the following procedures, you can use CrypWrap to unwrap the file.

Procedure

1. Run EXAMPLE.EXE. The system displays the following window:
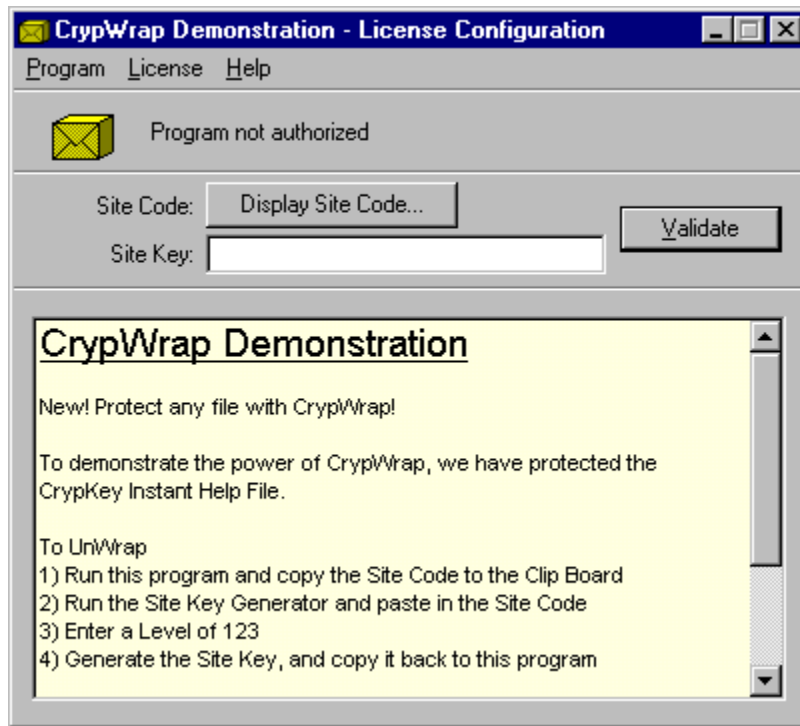
Figure 2: CrypWrap Demo – Opening Window

The simplified steps in the above window are explained in more detail below.

2. Click the **Display Site Code** button. The following popup appears over the above window:
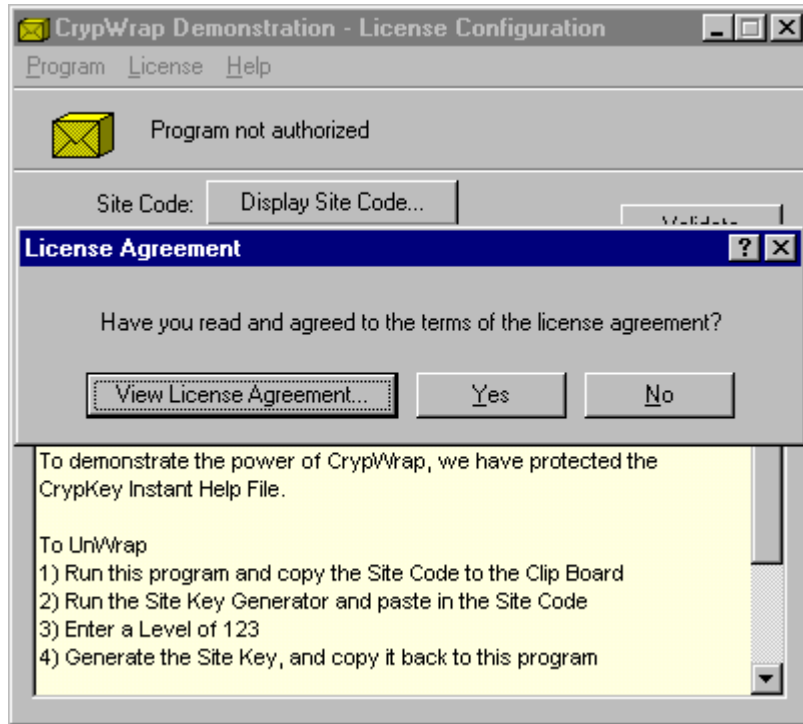
Figure 3: CrypWrap License Agreement Popup Window

3. Click **Yes** or the **View license agreement** button to review the agreement window and then exit the agreement window. In either case, the system now displays the site code.

4. Copy the site code to the clipboard.

5. Open the Site Key Generator. The system displays the following window:

Figure 4: Site Key Generator – Opening Window

6. In the above window, paste the CrypWrap site code into the **Site code** field and then click the **Check** button. The above window appears as follows:
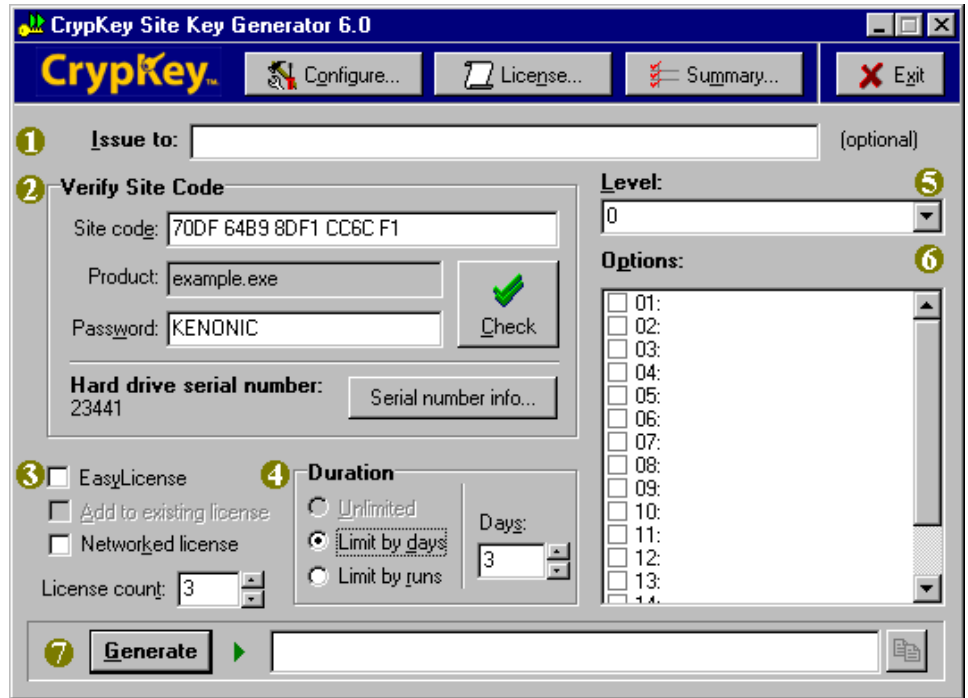
Figure 5: Site Key Generator with Verified CrypWrap Site Code

7. In the above window, enter the value **123** into the **Level** field and then click the **Generate** button. The window appears as follows:
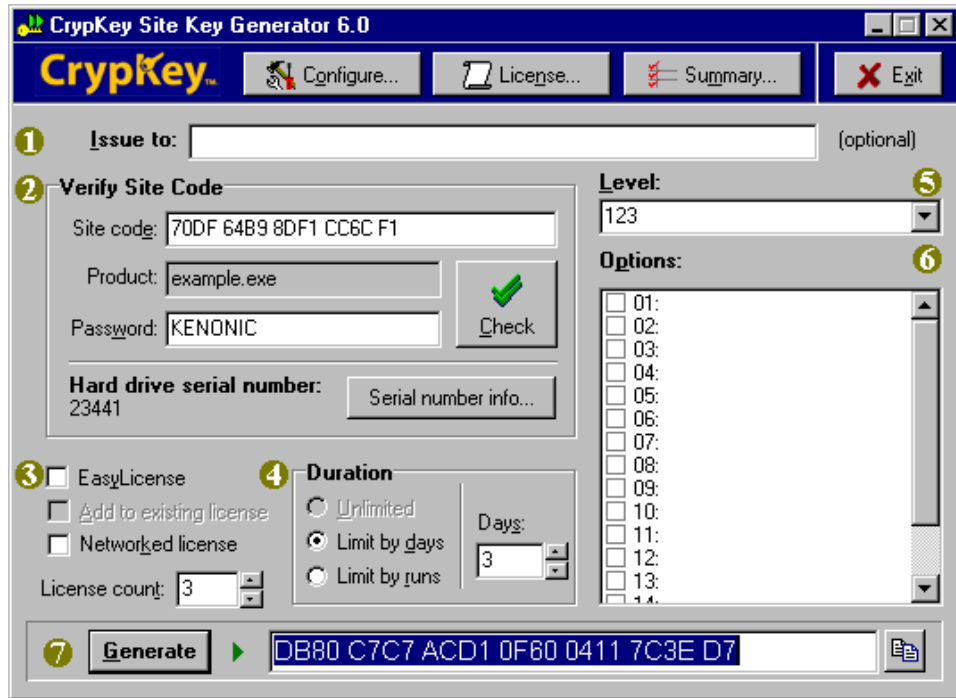
Figure 6: Site Key Generator with Generated CrypWrap Site Key

8. Copy the site key from the above window on to the clipboard.

9. Return to the CrypWrap window and copy the Site Key into the **Site Key** field:
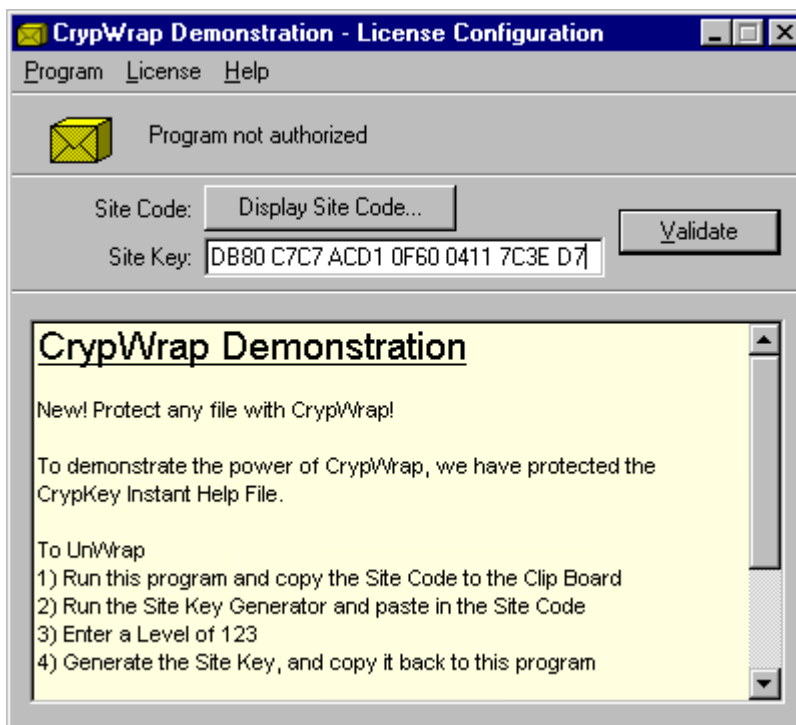
Figure 7: CrypWrap with Site Key Entered

10. Click the **Validate** button. The following popup appears over the window, confirming that your CrypWrap license is authorized:
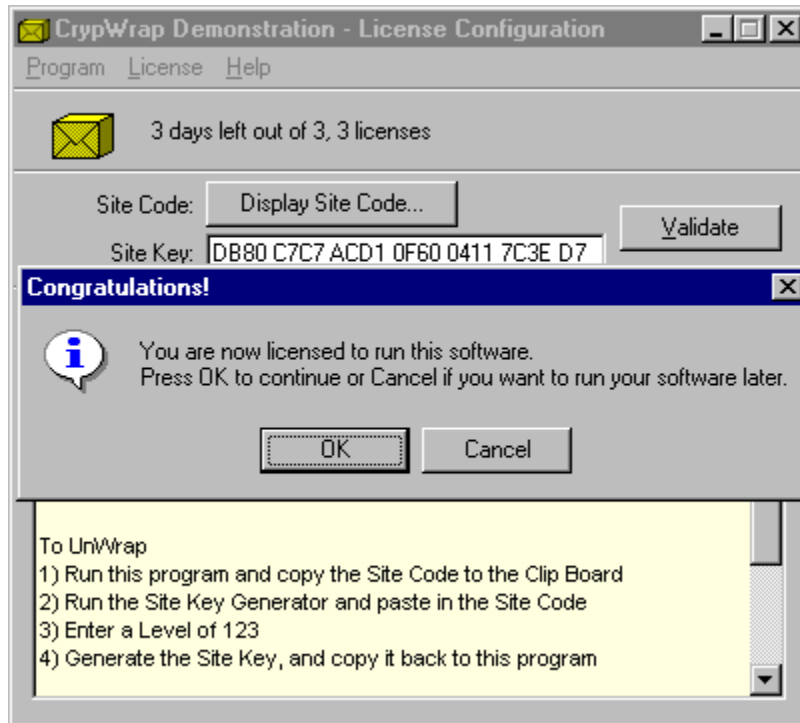
Figure 8: CrypWrap Authorization PopupWindow

11. In the above window, click **OK**. CrypWrap displays the following window:

Pick Extraction Folder

Pick a folder to recieve the files extracted from this archive:

○ Current folder: C:\CKI.311\CRYPWRAP\

○ System temporary folder: C:\WINDOWS\TEMP\

○ Other folder:

C:\CKI.311\CRYPWRAP\

Browse...

OK   Cancel
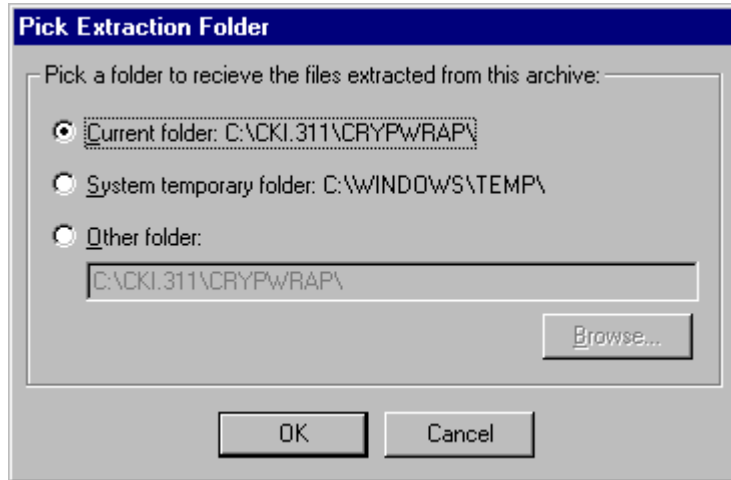
Figure 9: CrypWrap Extraction Folder Selection Window

12. In the above window, click **OK**. The system displays the window below or, if the file to be unwrapped already exists in the specified folder, a popup appears asking if you wish to overwrite the file. When you have responded as needed to the popup, the system displays the window below:

File Extraction

Extraction of "Cki32.hlp" complete.

OK
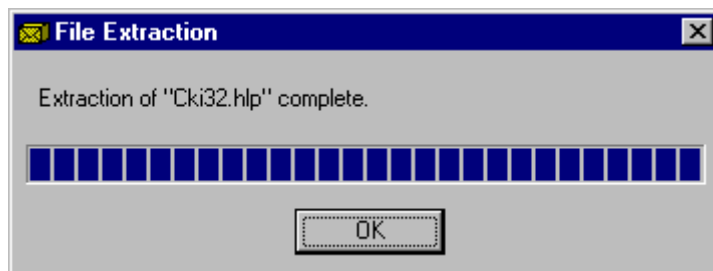
Figure 10: CrypWrap Extraction Complete

This completes the CrypWrap demonstration.

1.7.6   CrypKey File Auto-Distribution

CrypKey Instant can include all CrypKey secondary files in your protected executable. Even the NT driver can be included and automatically installed using StealthPLUS^{TM}. This means that you can distribute one executable file that contains all necessary files that are unzipped as necessary at runtime.

This has some major advantages:

1. Only one file to distribute. It is easy to make a download file for the Internet, or to send updates to customers!

2. You don't have to figure out which files to redistribute.

3. You don't have to install the NT driver; this is taken care of for you.

4. You never again have to be concerned with outdated DLLs; your program carries all the right ones with it.

This protected executable extracts in advance all the CrypKey files it needs to run and if NT is detected, the executable installs the necessary driver.

1.7.7   License Directory Redirection

CrypKey Instant supports placement of your license files in a different directory than your executable. This has some major advantages:

1. The license files can be hidden away so that users are much less likely to delete them.

2. If your executable is in a read-only directory, you can redirect your license files to be put in a read-write directory. The most common example of this is a CD ROM. Using this feature, you can put a protected executable on a CD ROM and have it run from there successfully, as it writes all license files to a directory of your choice on the hard drive.

3. You can make a new version of your software install to a different directory, and it finds and uses any existing license, with no transfer necessary.

1.8   Updating to CrypKey Instant 6.0

Following are actions that are necessary, and information that you need, if you are updating to CrypKey 6.0 from previous versions.

If you encounter any problems during this update procedure, do not hesitate to contact our support department at support@crypkey.com.

Procedures

1. If you have not already done so, install the new version.

    The new version installs into a different directory and does not affect your previous version, so you can put it on the same computer if you wish.

2. Contact us for a new 6.0 SiteKey Generator SiteKey

3. Transfer your CrypKey Instant License.

    This step is necessary only if your CrypKey Instant program starts with shows a license dialog, or shows a message "x days out of x" when it starts.

    The procedure is the similar to the one done in Step 2.

    a) Run your new CrypKey Instant, if necessary hitting a key as it starts to go to the license dialog.

    b) Under the **License** menu, select **Transfer in from another computer**.

        Note: If you have a trial license, you must kill it so that this button becomes active. Select the **Kill License** option from the **License** menu.

    c) Place a blank formatted diskette in Drive A: and click **Next**.

    d) Run your previous version of CrypKey Instant, if necessary hitting a key as it goes to the license dialog box.

    e) Under the **License** menu, select **Transfer out to another Computer**.

f) Put the diskette used in Step (c) into the new host computer's Drive A: and click **Next**.

Note: as mentioned above, the new host computer can be the same one you ran the previous version of CrypKey Instant on.

g) Click **Finished**. You are done with the previous CrypKey Instant.

h) Return to your new Site Key Generator, with transfer already in progress.

i) Put the diskette used in Step (f) into the new host computer's Drive A: and click **Next**.

j) Click **Finished**.

4. Transfer the configuration from your previous version of CrypKey Instant to Version 6.0.

a) If your previous version was 5.x or later:

Copy configuration files SKW.INI and CKI.INI from your previous install directory to your new install directory, overwriting the existing files.

b) If your previous version was 4.x or earlier:

- Copy configuration file CKI.INI from your previous install directory to your new install directory.

- Configure your New Site Key Generator as explained in see Chapter 5.

Authorization and Licensing

Follow our step-by-step instructions to acquire your developer keys, necessary for running CrypKey Instant.

U se our example developer keys while testing CrypKey Instant and your product. On testing completion, obtain your own personalized set of developer keys. It's all part of our master plan to ensure CrypKey Instant is everything you want in a software protection package and more.

In the CrypKey context, "license" refers to the set of levels, options, and permissions that you specify for your product. These data values, embedded and encrypted in your site key, activate and configure your clients' licenses. The site keys that you generate validate your product only on the computer that your client used to create the site code. Your Site Key Generator provides further protection by automatically verifying the authenticity of your client-provided site codes.

2.1   Obtaining Your Developer Keys

Procedure

1. Finish testing CrypKey Instant and your product using the example developer keys.

2. Confirm you have paid for CrypKey Instant. If you selected BillNet30 or Telegraphic Transfer, please ensure your payment has been sent. We can authorize you to use CrypKey Instant on your product only after the payment has cleared.

3. Send us the following information via email, fax, or telephone:

   a) your customer service number (CSN), located on the flap of the box in which the manual was shipped

   b) the file name of your product (maximum 8.3 characters)

   c) the password for your product (maximum 12 characters)

   d) your site code from your Site Key Generator (see Sec. 2.2.1)

   e) your site code from CrypKey Instant (see Sec. 2.2.2)

2.2 Obtaining Your Site Keys

To create site keys for customers, you must first obtain a site key authorizing you to use your copy of the Site Key Generator software. To do this, you need to provide us with the site code from your Site Key Generator. We then generate a site key and send it to you; you insert the key into your copy of the Site Key Generator, thereby authorizing it.

Similarly, in order to protect your software products using CrypKey Instant, you must obtain a site key authorizing you to use your copy of the CrypKey Instant software. To do this, you need to provide us with the site code from CrypKey Instant on your computer. Again, we generate a site key and send it to you; you insert the key into your copy of CrypKey Instant, thereby authorizing it.

These operations are described in the sub sections that follow.

2.2.1 Determining the site code of your Site Key Generator

Procedure

1. Start your Site Key Generator by double clicking its icon in the CrypKey Instant program group.
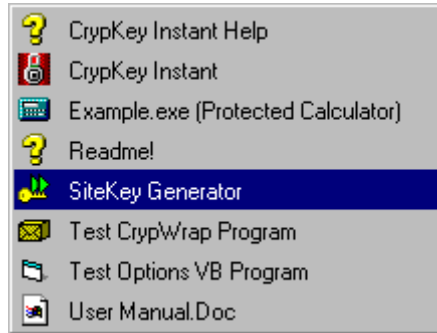
Figure 11: Site Key Generator Start Up

When you make the above selection, the Site Key Generator main window appears as shown below:
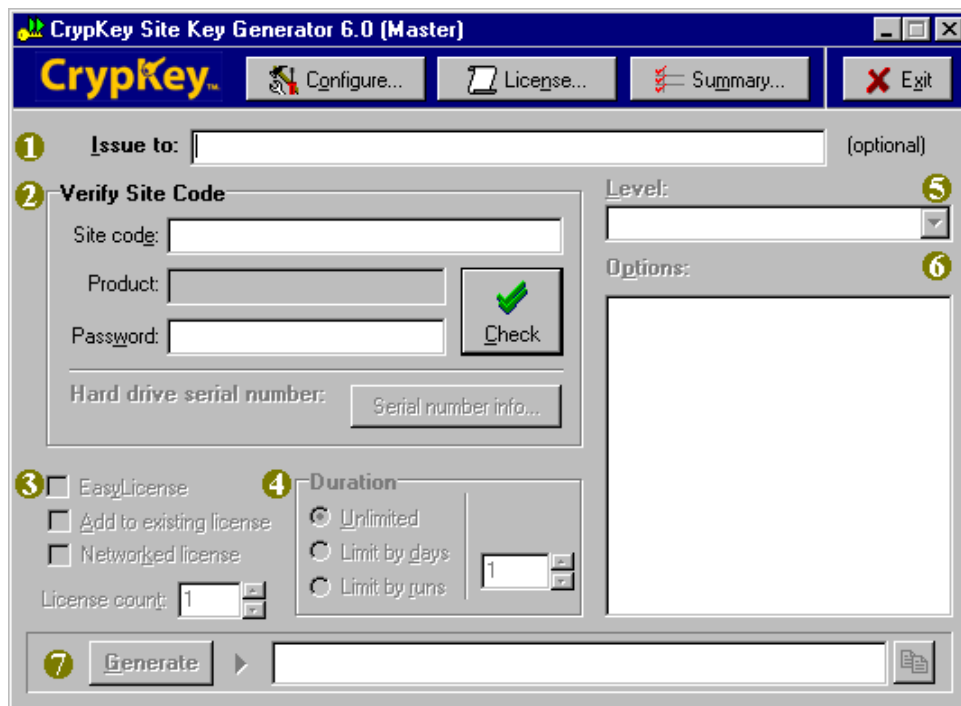
Figure 12: Site Key Generator – Main Window

2. Click the **License** tab in the above window. The License dialog box appears as shown below, with the site code displayed:
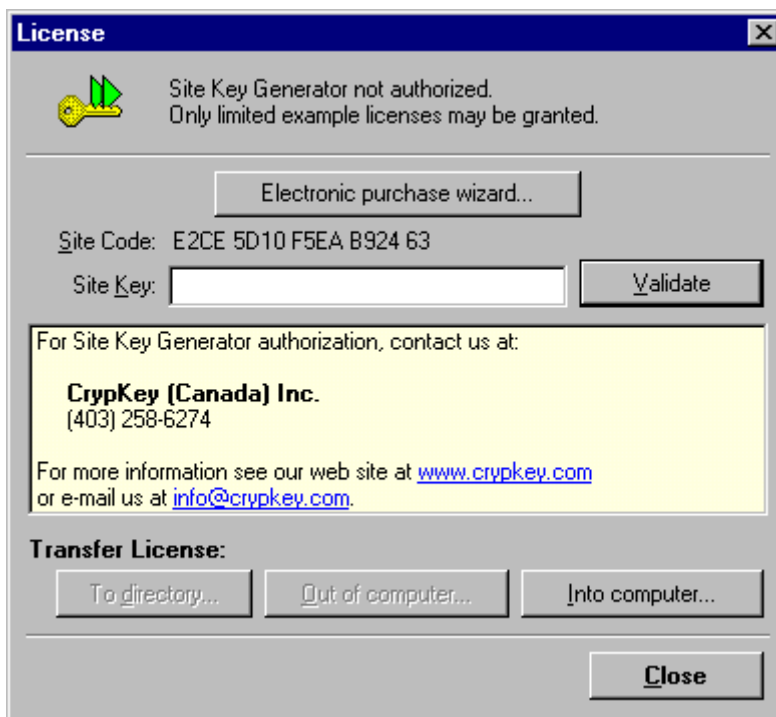
Figure 13: License – Unauthorized

2.2.2   Determining the site code of your CrypKey Instant program

Procedure

1. Select the CrypKey Instant icon in the CrypKey Instant program group.
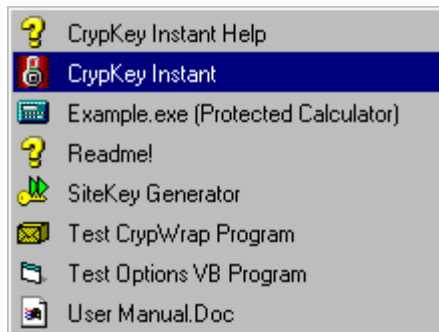
Figure 14: CrypKey Instant Start Up

2. Double click the above selection to display the CrypKey Instant License Configuration window:
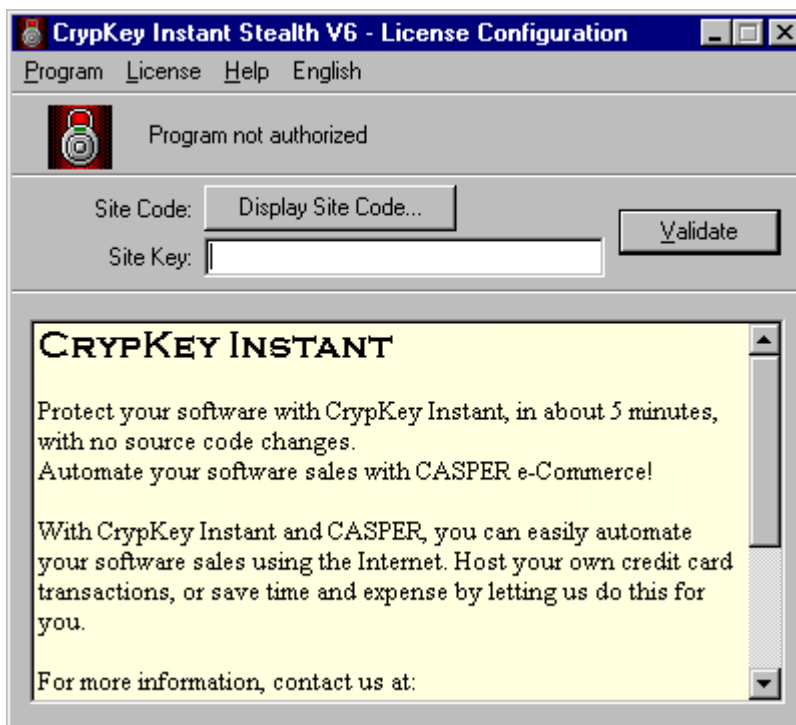
Figure 15: CrypKey Instant License Configuration Window

3. In the above window, click the **Display Site Code** button. The system displays the following popup window:
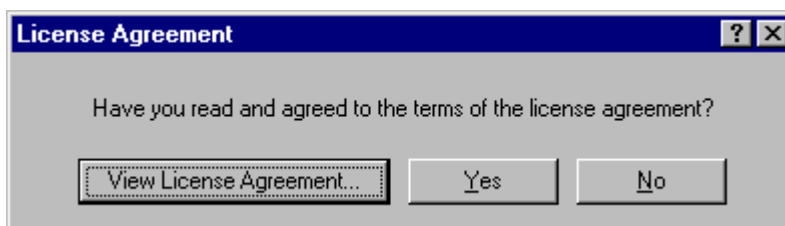
Figure 16: License Agreement Popup Window

If you haven't seen the license agreement yet, now is a good time to do so by clicking the **View License Agreement** button. When you have viewed and exited the agreement window, the above popup remains on the screen.

4. Click **Yes** in response to the license agreement prompt. The site code appears in place of the **Display Site Code** button.

2.2.3   Obtaining your site key for the Site Key Generator or CrypKey Instant

Procedure

1. Send us your site code via email, fax, or phone, along with the other information outlined in Section 2.1: Obtaining Your Developer Keys.

2. Once you receive your site key, type it (or cut and paste it from our email) into the **Site Key** field in the applicable window.

    For the Site Key Generator, the **Site Key** field is in the License dialog box, as shown below:
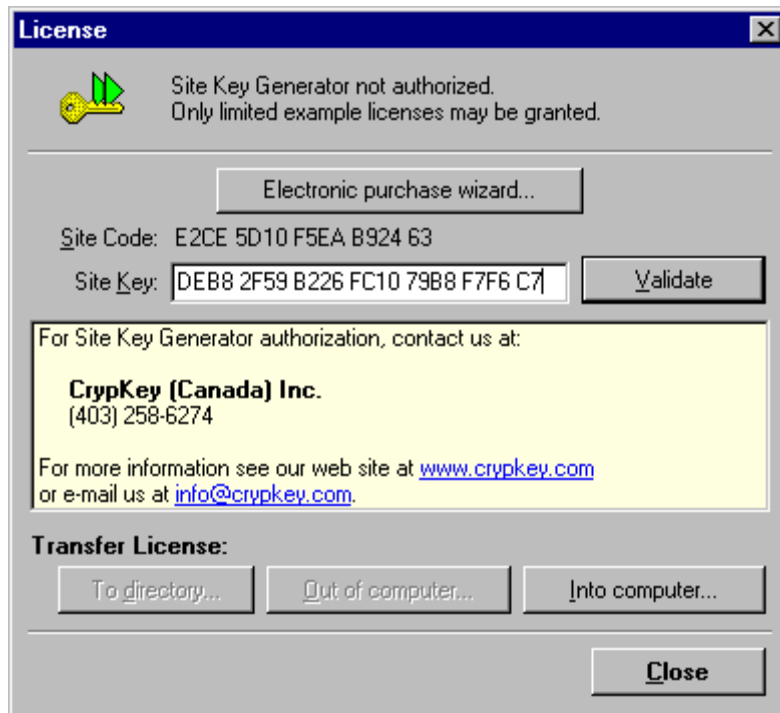
Figure 17: Site Key Generator – License Window, with Site Key Inserted

For CrypKey Instant, the Site Key field is in the Configuration window (see Figure 15: CrypKey Instant License Configuration Window).

Click the **Validate** button. If the site key is correctly generated and entered, you are authorized to use the Site Key Generator and/or CrypKey Instant on your computer.

In the case of the Site Key Generator, the License window appears as follows:
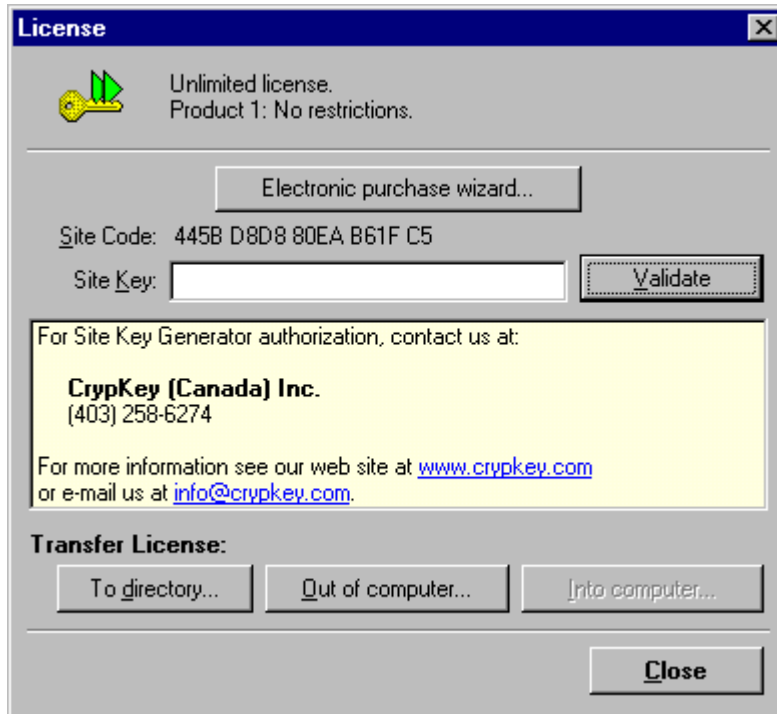
Figure 18: Site Key Generator License – Authorized

In the case of CrypKey Instant, a popup message appears in front of the License Configuration window, which shows that CrypKey Instant is licensed:
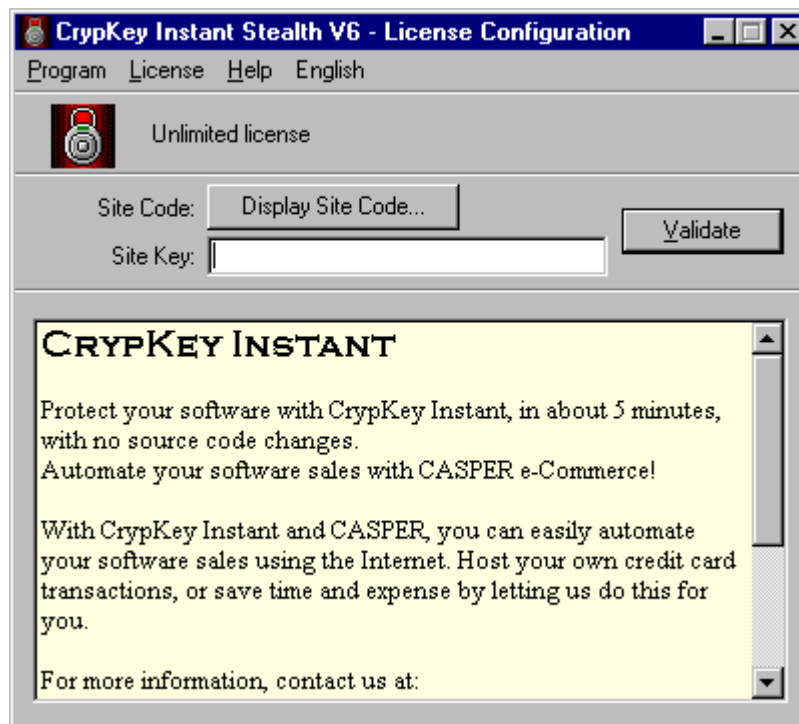
Figure 19: CrypKey Instant License – Authorized

You can click **Program > Resume program execution** in the menu bar in the above window, to display the opening CrypKey Instant window:
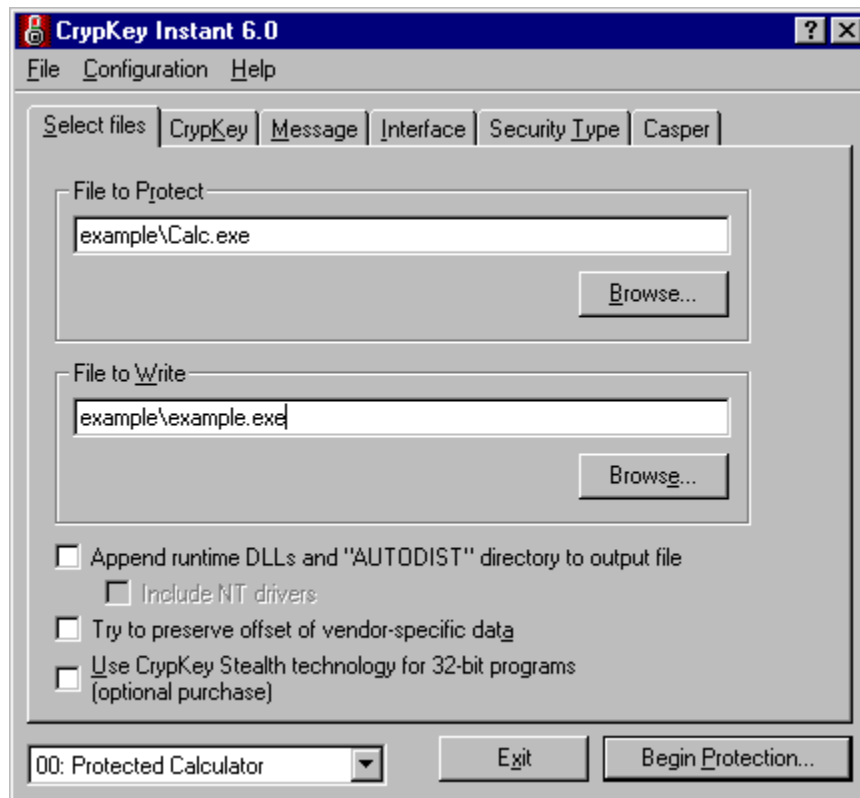
Figure 20: CrypKey Instant – Opening Window

2.3   CrypKey Implementation Process

Following are the steps that generally take place in the acquisition and implementation of CrypKey Instant:

1. You purchase CrypKey Instant, and test your software via the object code wrapping method.

2. You use CrypKey Instant to embed the protection object code in your target executable file within your application executable without requiring any changes to the source code. CrypKey Instant provides initialization, license verification, site code generation, and termination features.

3. Using CrypKey Instant, you organize (optionally) the features of your application in terms of specific "levels" and "options" that are available in the CrypKey system. We recommend that you do this if it is appropriate for the application, since applying levels and options allows you to use the full feature set that CrypKey provides for licensing. In cases where detailed control over product licensing is regularly required, we recommend purchasing the standard CrypKey SDK to meet your needs.

4. You experiment with CrypKey Instant by testing your product with the temporary license provided. CrypKey Instant is accompanied by a 30-day, money-back guarantee to ensure you can fully test the software without risk. All of the features of CrypKey Instant are available to you during this trial period.

5. If you are satisfied with CrypKey Instant's performance, you fax the information outlined in Section 2.1: Obtaining Your Developer Keys to CrypKey (Canada) Inc. We, in turn, fax you your developer keys, which are required to activate your distributor's license for your product. With these in place, you use your Site Key Generator to license clients to use your product.

    Please note that once you have been issued the developer keys for your product(s), CrypKey cannot be returned for a refund.

6. You distribute your product to prospective clients. To ensure clients can experiment with your product to determine the level of functionality and options they require, we suggest that you configure your product to function initially in demonstration mode.

7. You configure your product with a limited license (we recommend a 30-day license). When the time limit expires, your product ceases to run on clients' machines.

8. When a client is satisfied with your product, the client obtains a site code from the protected application running on the client's computer, and sends the code to you by email or fax, together with a request for authorization. The client should also indicate the desired license permissions and payment arrangements at this time.

9. You enter your client's site code into your Site Key Generator and set the license configuration. CrypKey Instant then generates a site key, which provides the specified access to your product. You send the site key to your client (an action referred to in this document as "authorization") once you have received payment.

   Note that CrypKey licensing is PC-specific, meaning that a client cannot copy your product and its license files to another PC for valid operation. CrypKey identifies the exact PC to which the license was issued —without requiring external hardware (dongle) or floppy disk keys.

10. Your client unlocks your product using the site key that you issued. CrypKey Instant, operating within your product on the client's computer, automatically tracks the number of runs or days over which the product is used, and invalidates the client's license at the appropriate time. In addition, CrypKey Instant verifies that the site code/site key combination is valid each time the client attempts to access the product.

11. You achieve fame and fortune once clients spread word of your product and the clean, unobtrusive CrypKey Instant licensing system that you have chosen to provide.

Besides protecting your own product, you can use CrypKey Instant to protect unique programs acquired from developers around the world. Regardless of coding method or development environment, most Windows-based executables can be redistributed with CrypKey Instant protection.

We are pleased to provide you with technical assistance through the contact numbers listed in Section 1.4: Technical Support.

Installation

This "how to" section outlines the CrypKey Instant installation procedures.

I f you are using a Windows NT operating system, you must install NT drivers to run CrypKey Instant even if the product is installed on a standalone computer (see Section 7: Network Licensing for further details).

3.1   Getting Started

You can install CrypKey Instant from a CD provided by CrypKey (Canada) Inc., or, if you are a CrypKey subscriber, by downloading the installation files from the CrypKey website. As you will see in Sections 3.1.1 and 3.1.2, the sequences of windows for the two types of installation are quite similar.

Whether run from a CD or from downloaded files, the installation program creates the following CrypKey group in your Start menu (Windows 95/98/ME/NT/XP/2000), or in Program Manager (Windows 3.1):
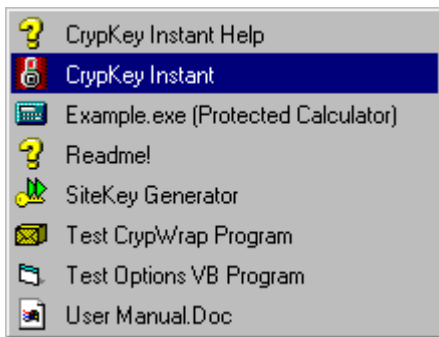
Figure 21: CrypKey Instant Program Group

3.1.1 Installing CrypKey Instant from CD

Procedure

1. Ensure Windows is running on your computer.

2. Insert the CrypKey CD-ROM into your CD-ROM drive. CrypKey automatically starts up, displaying the following window:

Figure 22: Opening CrypKey CD Installation Window

3. Click the **Install** button. The system displays the following window:

Figure 23: CD Installation Screen 1

4. Choose **Install CrypKey Instant.** The system displays the InstallShield Wizard, shown below. In this window, and the others in the sequence, simply press the **Next** or **Yes** key, whichever is presented, after you respond to the prompts, if any, shown in the windows.
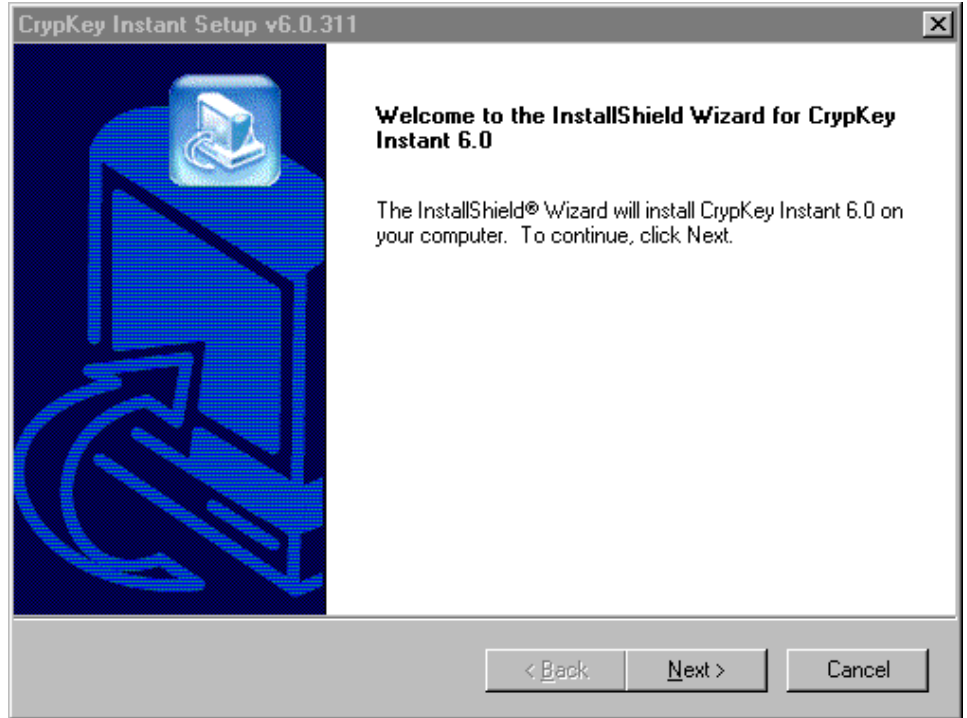
Figure 24: CD Installation Screen 2
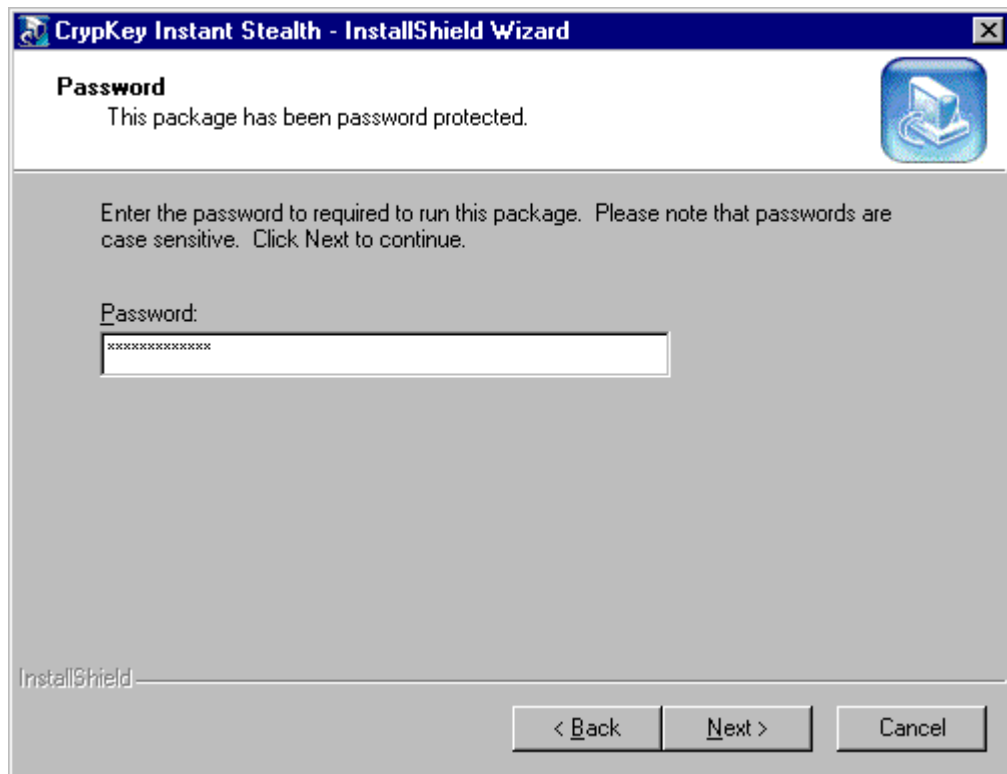
Figure 25: CD Installation Screen 3

5. In the above window, type the password provided by CrypKey (Canada) Inc. When you have correctly entered the entire password, the **Next** button is enabled, as shown above. Click the **Next** button to display the following window:
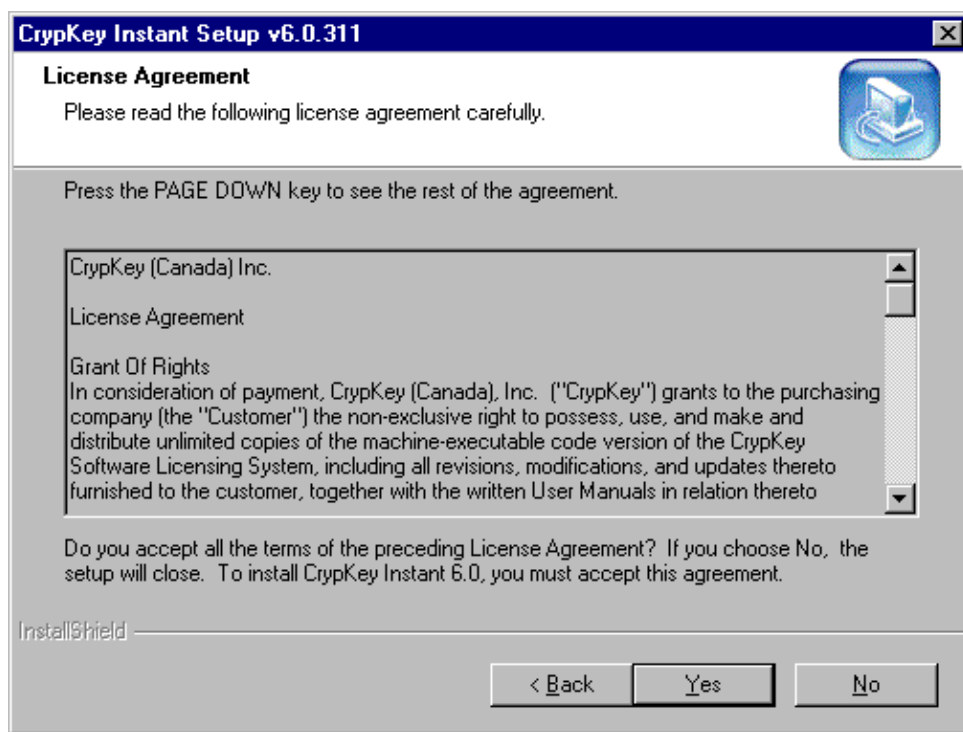
Figure 26: CD Installation Screen 4
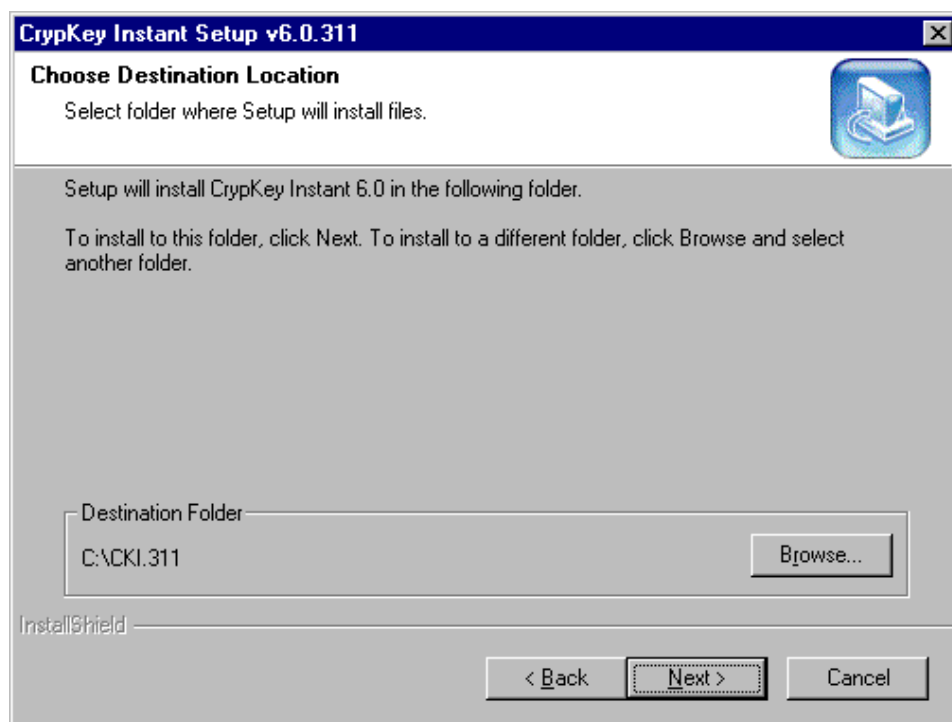
Figure 27: CD Installation Screen 5

6. In the above window, specify where you want CrypKey Instant installed by accepting the default directory provided by the installation program, or by typing in a path for it to use. If the directory does not already exist, the installation program creates it for you.
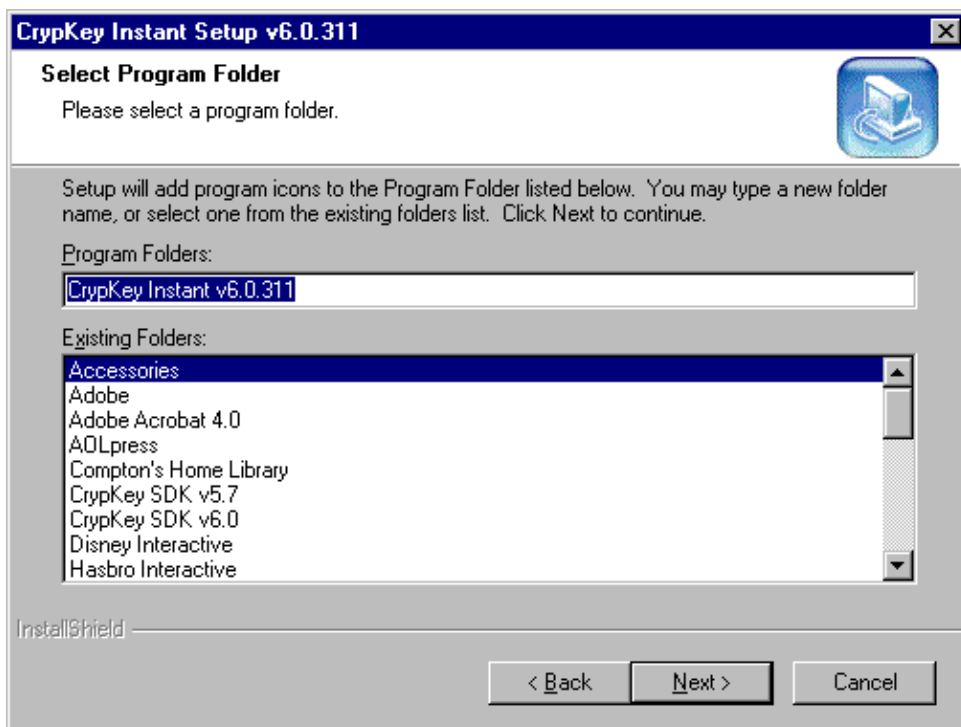
Figure 28: CD Installation Screen 6
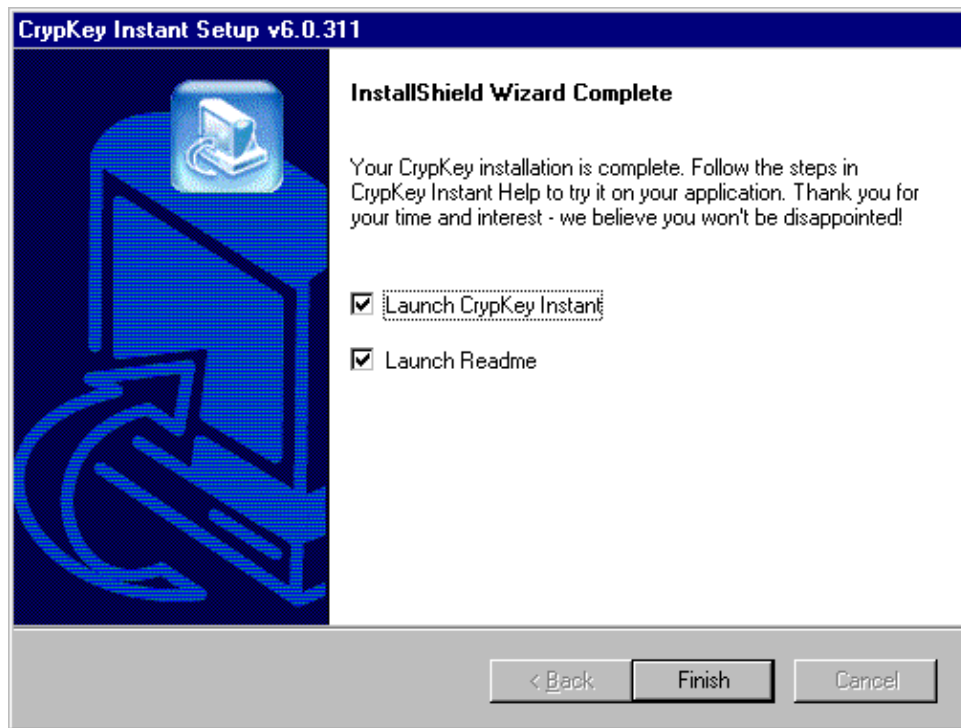
Figure 29: CD Installation Screen 7

7. In the above window, the options **Launch CrypKey Instant** and **Launch Readme** are pre-selected. You can click either checkbox to deselect it.

We strongly recommend that you read the **Readme** file immediately, because it may contain last-minute details that were not available in time to be included in this manual.

3.1.2   Downloading and Installing CrypKey Instant

Procedure

1. When you have completed the download of the installation files to your computer, double-click the file **CrypKeyInstant311$[1]**.

    The system displays the following window. This is the first of a sequence of standard installation windows. In each one, simply press **Next** after you have responded to the prompts, if any, in that window.

Figure 30: Download Installation Screen 1
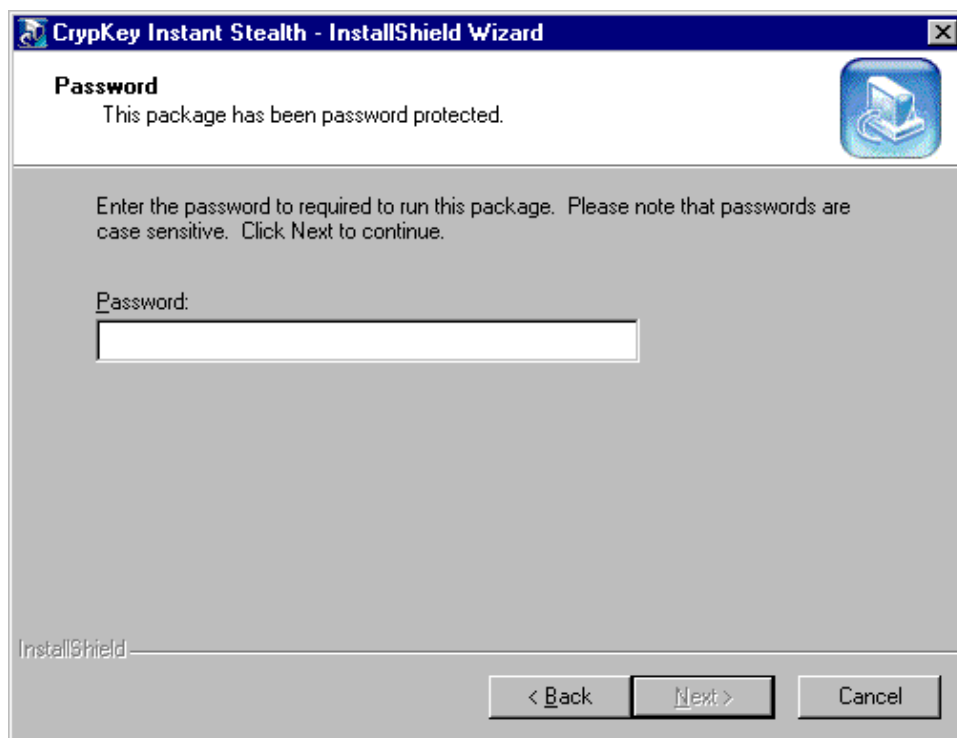
Figure 31: Download Installation Screen 2
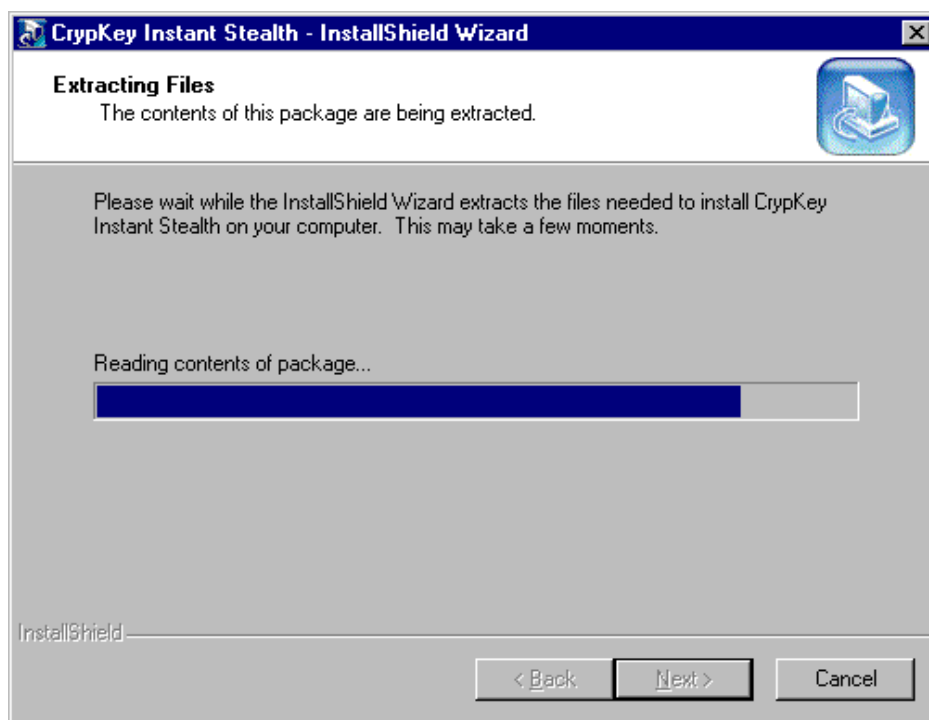
Figure 32: Download Installation Screen 3
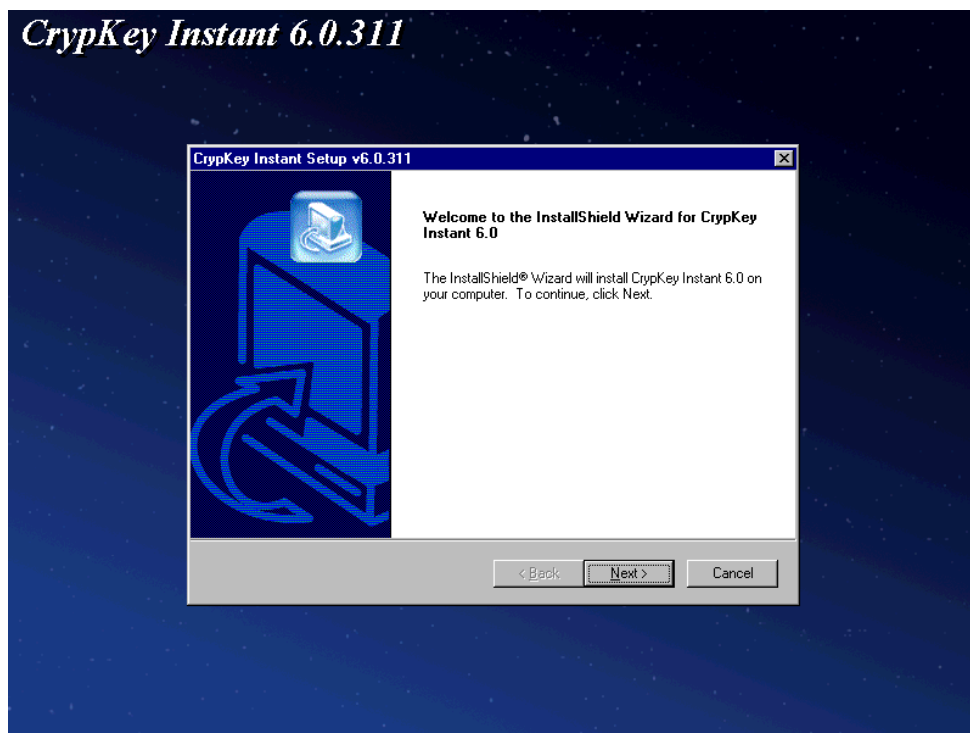
Figure 33: Download Installation Screen 4
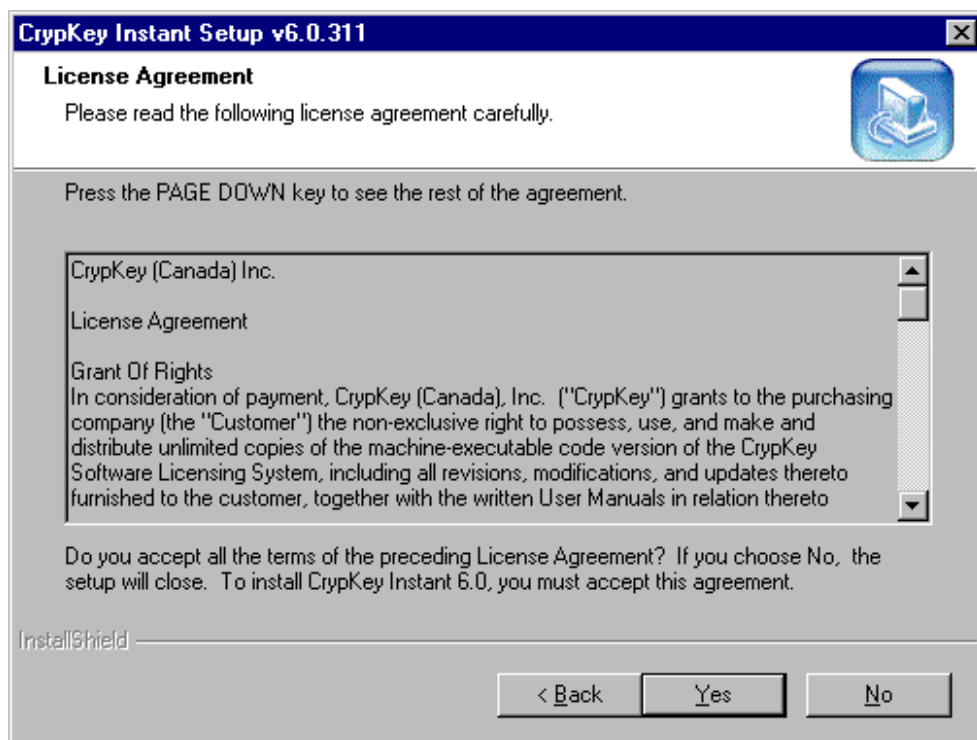
Figure 34: Download Installation Screen 5
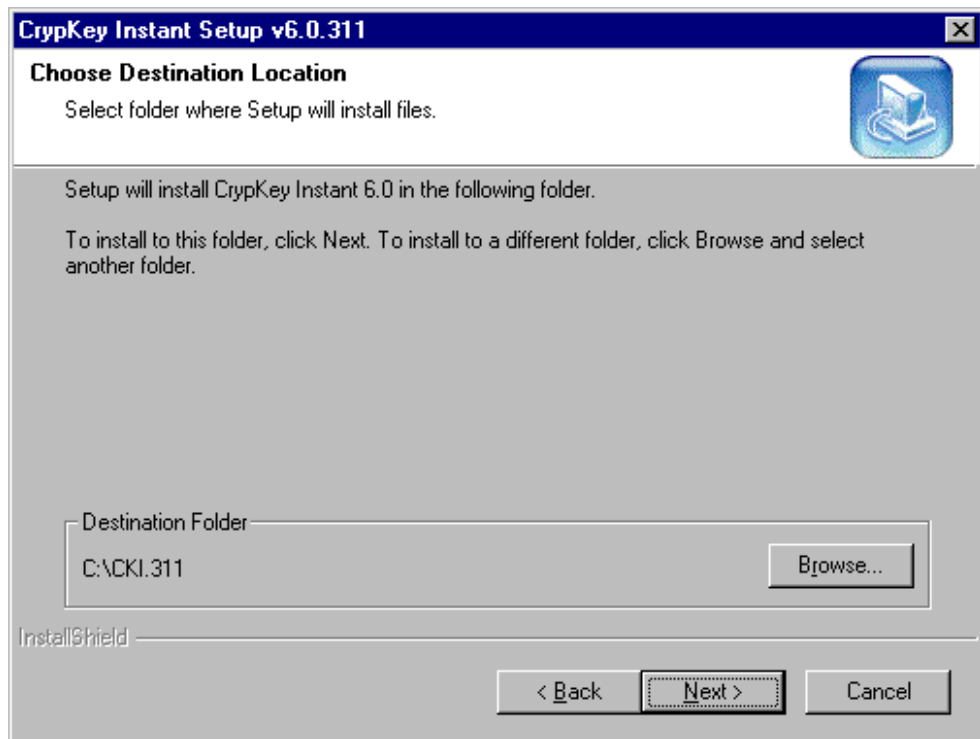
Figure 35: Download Installation Screen 6

2. In the above window, specify where you want CrypKey Instant installed by accepting the default directory provided by the installation program or by typing in a path for it to use. If the directory does not already exist, the installation program creates it for you.

3. Once the drive and directory are correct, click **OK** to continue the installation process with the following window:
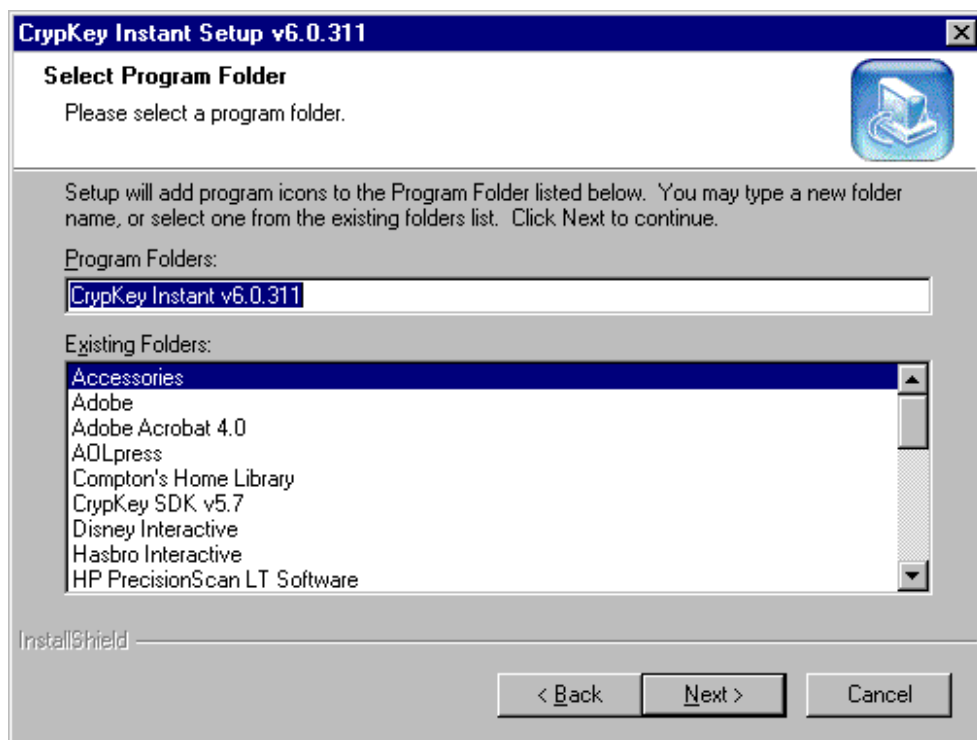
Figure 36: Download Installation Screen 7
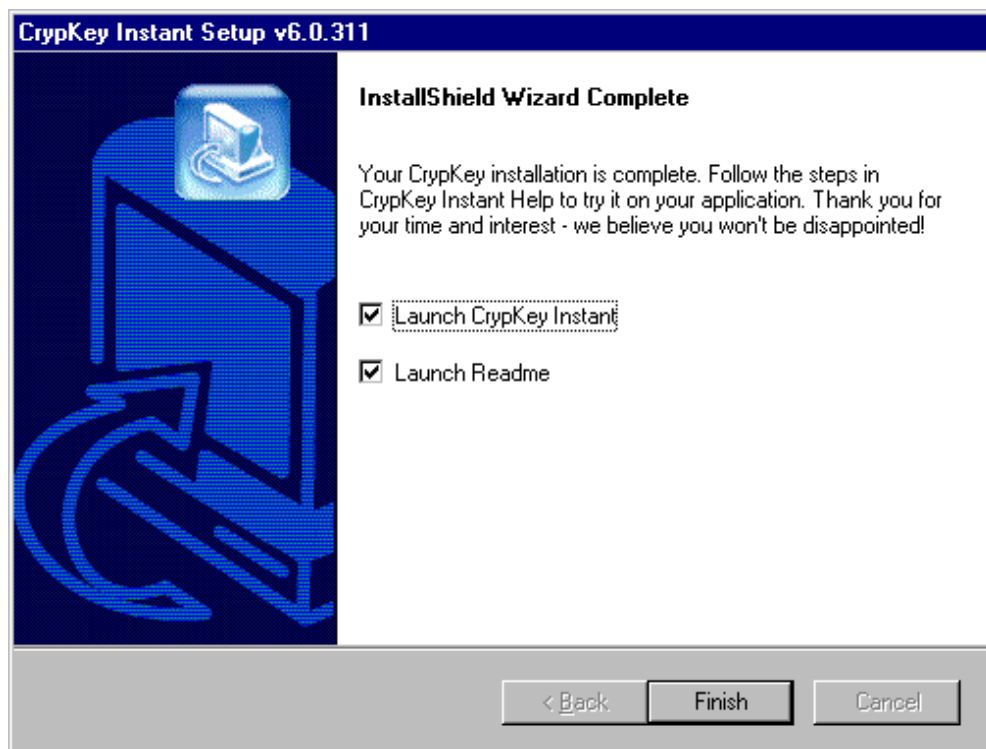
Figure 37: Download Installation Screen 8

4. In the above window, the options **Launch CrypKey Instant** and **Launch Readme** are pre-selected. You can click either checkbox to deselect it.

We strongly recommend that you read the **Readme.hlp** file immediately, because it may contain last-minute details that were not available in time to be included in this manual.

3.2 CrypKey License Service Installation

This section pertains to all programs running under the NT File System (NTFS), including MS-DOS and Win16 as well as native Win32 programs. The CrypKey License Service (CLS) needs to be installed on Windows NT/2000/XP operating systems.

CLS manages licenses. In NT environments, it is required for either standalone or network installations.

To run a CrypKey-protected MS-DOS, Win16 , or Win32 program from a local drive on a Windows NT platform, you must install CLS on that machine. CLS is required because Windows NT does not allow programs to directly access the computer hardware, which CrypKey needs to do. For details and instructions for installing CLS, see Sec. 7.1: CrypKey Network Drivers.

If you are currently running CrypKey Instant on a Windows NT personal computer, you already have CLS installed and running on that PC. If you would like to use CLS with the installation of your application, you can find it in C:\CrypKey.60\Stealth.

StealthPLUS™ can install CLS automatically for you. For details on utilizing StealthPLUS™ to do this as well as protect your software, see Sec. 6.3: StealthPLUS™.

We no longer support custom installations for the Windows NT drivers.

3.3   Windows 9x/ME Network Installation

The file wckserve.exe is the Windows 3.1, Windows 95, and Windows 98 CrypKey network communications driver. It is a Windows program that can be run in any Windows environment to allow the computer to act as a server for CrypKey-protected programs. Wckserve.exe runs in the background and is transparent to the operation of the computer.

Before running wckserve.exe, an environment variable must be set to tell it where the CrypKey-protected program is. The best way to do this is to put a command in the autoexec.bat file as follows:

```
SET CKSERVE=dir; [dir2;] [dir3;]
```

where `dir`, `dir2`, `dir3`, etc. are paths to the directories that hold CrypKey-protected programs. If there is more than one CrypKey-protected program on the computer, a path must be given for each directory, ending with a semicolon. When the computer is rebooted, the SET command takes effect with the parameters specified.

Alternatively, wckserve.exe accepts the directory string normally in the WCKSERVE environment as a command line variable:

```
WCKSERVE.EXE C:\MYAPP1;C:\MYAPP2
```

where MYAPP1 and MYAPP2 are directories containing CrypKey-protected applications

To configure wckserve.exe to automatically start and run in the background, just add wckserve.exe to the Startup group. When Windows is restarted, the driver runs.

Note: the server must give read and write permission to its clients for the directory where the CrypKey-protected software resides. If write permission is not given, all network access requests are denied.

Example: Running CrypKey on a Win9X/ME peer to peer network

WIN9X/ME Server
Name = APPSERVER

WIN9X/ME Client

This System is acting as the server. Other clients will connect to this computer to run the application:

C:\APP\EXAMPLE.EXE

1. Load the WCKSERVE driver on the system by placing the following lines in the autoexec.bat file:

SET WCKSERVE= C:\APP
C:\APP\WCKSERVE.EXE

or you can have one line instead of the two above by using the following statement:

C:\APP\WCKSERVE.EXE C:\APP

Note: The wckserve.exe file must exist in the directory specified.

2. You must share the directory C:\APP so that other users on the network will have FULL access to it.

3. Reboot the computer for the changes to take effect.

This is a client that will run the application form the server. It also requires some configuration:

1. Load the WCKSERVE driver on the system by placing the following lines in the autoexec.bat file:

SET WCKSERVE=\\APPSERVER\C\APP
\\APPSERVER\C\APP\WCKSERVE.EXE

or you can have one line instead of the two above by using the following statement:

\\APPSERVER\C\APP\WCKSERVE.EXE \\APPSERVER\C\APP

Note: The wckserve.exe file must exist in the directory specified.

2. Reboot the computer for the changes to take effect.

3. Create a shortcut to the executable on APPSERVER.

Figure 38: Example WCKSERVE.EXE Configuration

3.4   MS-DOS Network Driver Installation

Ckserve.exe is a terminate and stay resident (TSR) driver program that must be run on any networked MS-DOS computer that makes a CrypKey-protected program available to other computers. This driver is intended for MS-DOS servers and cannot be run on a

Windows server. Ckserve.exe runs in the background and is transparent to the operation of the computer.

Before running ckserve.exe, an environment variable must be set to tell it where the CrypKey-protected program is. The best way to do this is to define an environment variable in the autoexec.bat file as follows:

```
SET CKSERVE=C\:MYAPP1; C\:MYAPP2; ...
```

where MYAPP1, MYAPP2, etc. are directories containing CrypKey-protected applications. If there is more than one CrypKey-protected program on the computer, a path must be given for each directory, ending with a semicolon. When the computer is rebooted, the SET command takes effect.

Alternatively, ckserve.exe accepts the directory string normally in the CKSERVE environment as a command line variable:

```
CKSERVE.EXE C:\MYAPP1;C:\MYAPP2; ...
```

where MYAPP1, MYAPP1, etc. are directories containing CrypKey-protected applications.

To start ckserve.exe, ensure the program is loaded on the computer. Type the program name from the MS-DOS command line, with no options. This command can and should be put into the autoexec.bat file. You can put ckserve.exe in any directory, as long as you name the full path when you start it.

This program must be run from MS-DOS (version 3.1 or higher). It cannot be run with Windows on the same computer (check with us if you need this ability).

The server must give read and write permission to its clients for any directories where CrypKey-protected software resides. If write permission is not given, all network access requests are denied.

3.4.1   Example

Consider an example where there are CrypKey-protected programs in the following directories:

```
C:\APPS\BINGO
```

```
E:\WINDOWS\WHIZBANG
```

```
D:\TEMP
```

If you want your users to be able to operate the first two programs from other computers that are linked by a network and you have ckserve.exe loaded into the directory C:\util, you should put the following commands in the autoexec.bat file to make it run properly:

```
SET CKSERVE=C:\APPS\BINGO;E:\WINDOWS\WHIZBANG;D:\TEMP

C:\UTIL\CKSERVE.EXE
```

Reboot the computer to put these commands into effect.

3.5   Novell NetWare Installation

The CrypKey system includes one Novell NetWare Loadable Module (NLM) , which must be loaded into a NetWare server machine that is hosting CrypKey-protected programs with floating licenses.

Ckserver.nlm is used for all NetWare servers. It must be given read, write, filescan, modify, and delete permissions for the server machine that it services. Ckserver.nlm can service only the local file server that it is installed on; this includes the SYS volume and all other volumes on the server.

Ckserver.nlm should be installed in the SYS:SYSTEM directory and loaded from the autoexec.ncf file. Ckserver.nlm is self-configuring and it detects any CrypKey-protected program on the server on which it runs. It does not require any interaction or configuration from the administrator once it is loaded.

3.6   Distributing Your Protected Application

When distributing your product, remember that your clients are not be running the same platforms. Each platform requires different files to run your product, as detailed below. For a quick reference to the information detailed in Table 1 and Table 2 below, see Table 8: File Distribution Matrix, which is found in the Appendix (Sec. 11).

3.6.1   Files Used in 32-Bit Windows Applications

Table 1 describes the CrypKey files that are required to be in the same directory as a CrypKey Instant protected.32-bit application. "?" represents the language identifier for language files shipped with the product.

Table 1: Files Used in 32-Bit Windows Applications

File	Description
Required Files	
crp32001.ngn	CrypKey DLL (always required). The values for "?"vary depending on the version of Instant used.
cki32j.dll	CrypKey Instant DLL (required for all 32-bit applications). The "j" refers to Version 6.0 of CrypKey Instant.
cks.exe setup.exe	Files used to install the Crypkey License Service required on all NT systems, whether networked or standalone.
cryp95f.dll	CrypKey DLL (required for Windows 95/98/ME programs).
crp9516f.dll	CrypKey thunk DLL (required for Windows 95/98/ME programs).
ck16rmv.exe	Executable file (required for all 32-bit applications running under Windows 95/98/ME; ensures thunk libraries are removed from memory)
hdsn1.dll	Used to access and read the hard drive serial number.
Files Required for Specific Functions	
cki32.hlp	Help file, accessible if you have not disabled the help menu. If this file is not distributed, context-sensitive help does not work.
cki32j_?.dll	Language resource file (required for non-English versions only). The "?" vary depending on the language used.
cki_?.msg	Text file message (required if you select **Use File** in the **Message** tab page). The "?" vary depending on the language used.
cki_?.bmp	Bitmap message (required if you select **Use Bitmap** in the **Message** tab page). The "?" vary depending on the language used.
cklicens.hlp	License agreement help file (required if you select **Require License Agreement** in the **Interface** tab page).
Optional Files	

File	Description
splash.int	Standard Windows bitmap that is displayed in the splash screen.
Files used if you have enabled the CASPER feature	
casper.dll	Required for all CASPER transactions.
inetcli.dll	Required if you are using CASPER's direct Internet communication.
pub.key	Required public encryption key.
casintro.txt	Optional text, displayed in the first screen of the CASPER wizard.
casfinal.txt	Optional text, displayed in the final screen of the CASPER wizard.

If you note discrepancies in the above list, please refer to CrypKey Instant's online help for current information

3.6.2   Files Used in 16-Bit Windows Applications

Table 2 describes the CrypKey files that are required to be in the same directory as a CrypKey Instant protected.16-bit application. "?" represents the language identifier for language files shipped with the product.

Table 2: Files Used in 16-Bit Applications

File	Description
cki16j.dll	Main DLL and English-language resource file (always required).
cki16j_?.dll	Language resource file for languages other than English. The "?" vary depending on the version of Instant used.
cki16.hlp	Help file; accessible if you have not disabled the help menu.

File	Description
cks.exe setup.exe	Files used to install the Crypkey License Service required on all NT systems, whether networked or standalone.
hdsn1.dll	Used to access and read the hard drive serial number.
cki_?.msg	Text file message (required if you select **Use File** in the **Message** tab page). The "?" vary depending on the language used.
cki_?.bmp	Bitmap message (required if you select **Use Bitmap** in the **Message** tab page). The "?" vary depending on the language used.
cknetwk.exe	Network supported (required if you want to use floating licenses).
cklicens.hlp	License agreement help file (required if you select **Require License Agreement** in the **Interface** tab page).
splash.int	Standard Windows bitmap that is displayed in the splash screen.

If you note discrepancies in the above list, please refer to CrypKey Instant's online help for current information.

3.6.3   Required Files For DOS Programs

DOS programs protected by CrypKey Instant do not support multiple languages, networking, or message files. The only necessary files are those created at protection time: programname.exe, programname.ex^, and programname.ex_.

3.6.4   Storing License Files and the Protected Program in Separate Locations

You may want to separate license files from your protected program for the following reasons:

- You want your program to reside on a client machine and the license to reside on a server.

- You want your program to reside on a CD-ROM or other read-only source, and the license to reside on your hard drive. If you implement this approach in a Win9x/ME environment, ensure that no CrypKey DLLs are located in the read-only location. They should be located with the license file. This prevents thunk errors.

In these system configurations, the license directory requires full permissions.

Procedure

Building Your Protected Program

1. Determine a file, other than your program file, to which to tag the license. CrypKey Instant uses any file you specify to locate and name its license files. This file need not be the protected executable; it can be any file you want. CrypKey Instant only checks for the existence of this file; it does not read it.

   For example, you may decide to specify a dummy file called DATA.LIC. We call this the license tag file.

2. Obtain your master key from CrypKey for the license tag file rather than the protected execution file. Insert your master key in the **Master Key** field of CrypKey Instant.

3. Since the license tag file is not in the same location as your protected executable, you must tell CrypKey Instant where to find the license tag file by using an environmental variable in the computer the program runs on. This variable contains a path to the license tag file. Determine the name of the environmental variable you use (for example, LICENSE_PATH).

4. Enter the selected name of your environmental variable in the **Filename** field of the **CrypKey** tab page. To ensure CrypKey Instant recognizes you entered an environmental variable name rather than a file name, prefix and append a " % " character to the name. (For the example name specified above, enter %LICENSE_PATH%.)

5. Protect your program as usual.

Installing Your Protected Program

6. Install the license tag file in the computer and directory where you want it to reside. If the license tag file resides on a server computer, you must also install the appropriate network driver.

7 . In the computer your program runs on, configure your selected environmental variable to hold a path to the license tag file. For example, to run your program on Windows 95, where the license resides in the server directory of X:\Programs\ MyProgram, you would enter the following in the AUTOEXEC.BAT file (using the example names specified above):

```
Set LICENSE_PATH= X:\Programs\MyProgram\data.lic
```

8. Reboot if necessary.

3.7 Creating Your Splash Screen

You can create a graphic popup screen that appears when your authorized customer launches your application.

Procedure

1. Use a program such as Windows PaintBrush to create a graphic of any size (typical dimensions are 300 x 150 pixels). At runtime, the splash screen resizes itself to fit the defined graphic.

2. Save the file in bmp format.

3. Rename the file to splash.int.

4. Copy the file to your application directory.

Demonstration Program

With CrypKey Instant installed, now comes the fun part:
testing how the software functions in relation to your product.

W e suggest that you use the trial version of CrypKey Instant to test its protection value, using the example keys contained in this document. Once satisfied with CrypKey Instant's performance, use the software with your own keys, distributing your product to users and authorizing their use of it.

The CrypKey Instant package consists of the following two components:

- CrypKey Instant, to protect your executable and DLL files

- Site Key Generator, to create keys for the protected product

This section briefly describes the procedures for opening your CrypKey Instant example program (example.exe) and authorizing your license for it using the Site Key Generator. In this context, you are acting as your customer when you open the example program, and as yourself when you use the Site Key Generator to issue a site key for the example program.

After you have installed CrypKey Instant, your Windows Program Manager/Start Menu contains a new program group for CrypKey Instant, with several new icons.

For this demonstration, you need only focus on:

- the example.exe (illustrates what your users see when they use your protected product)

- the Site Key Generator (the same as the one you use to authorize your product for your clients once you have received your developer keys)
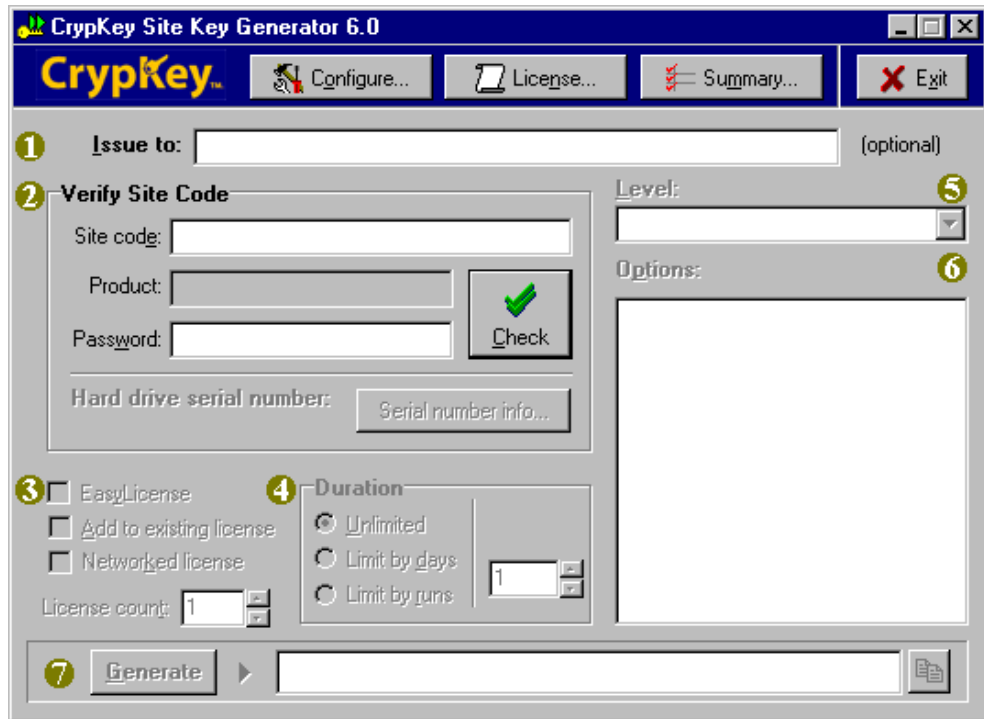
Figure 39: CrypKey Site Key Generator – Main Window

4.1   Producing a Site Code

The purpose of this demonstration is to show you how the authorization process works. When you start the demonstration program (Calculator), you initially have a three-run RTT license. After the three runs, you must obtain the site key for it using your copy of the Site Key Generator.

Procedure

1. Start the demonstration program (Calculator) by double clicking **Example.exe** in the CrypKey Instant program group.
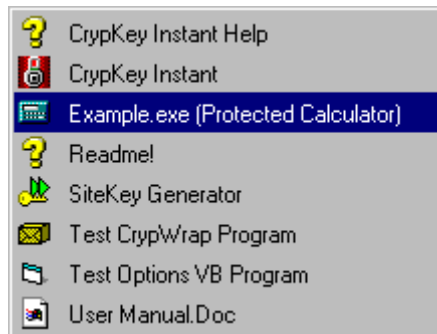
Figure 40: Example.exe Start-up

When you first open this example, the system displays the following window, showing that you are not authorized to use the Calculator program:
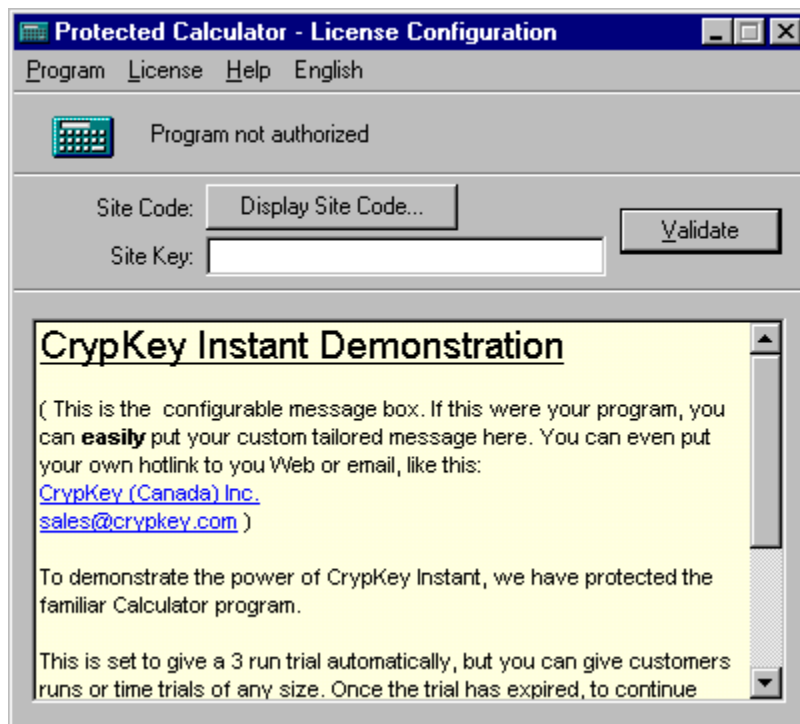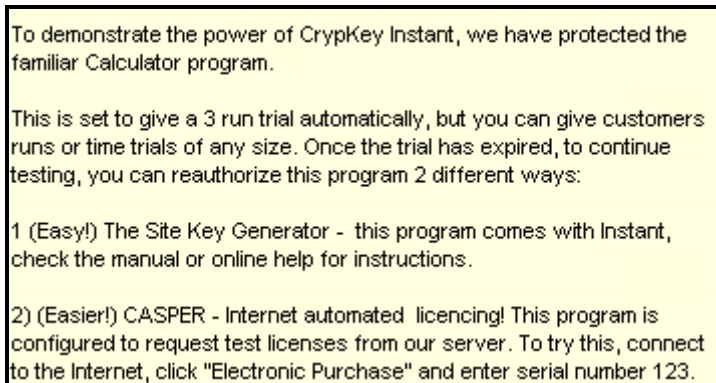
Figure 41: CrypKey Instant Example – Unauthorized License

Scrolling down the text panel in the above window displays the following information:

To demonstrate the power of CrypKey Instant, we have protected the familiar Calculator program.

This is set to give a 3 run trial automatically, but you can give customers runs or time trials of any size. Once the trial has expired, to continue testing, you can reauthorize this program 2 different ways:

1 (Easy!) The Site Key Generator - this program comes with Instant, check the manual or online help for instructions.

2) (Easier!) CASPER - Internet automated licencing! This program is configured to request test licenses from our server. To try this, connect to the Internet, click "Electronic Purchase" and enter serial number 123.

Figure 42: Example – Opening Instruction Panel

Later, when you have obtained authorization (in the procedures explained below), a different popup window appears when you open the example—see Sec. 4.3: Authorizing Your Example Program.

2. In the License Configuration window, click the **Display Site Code** button. The **License Agreement** popup window appears as shown below:
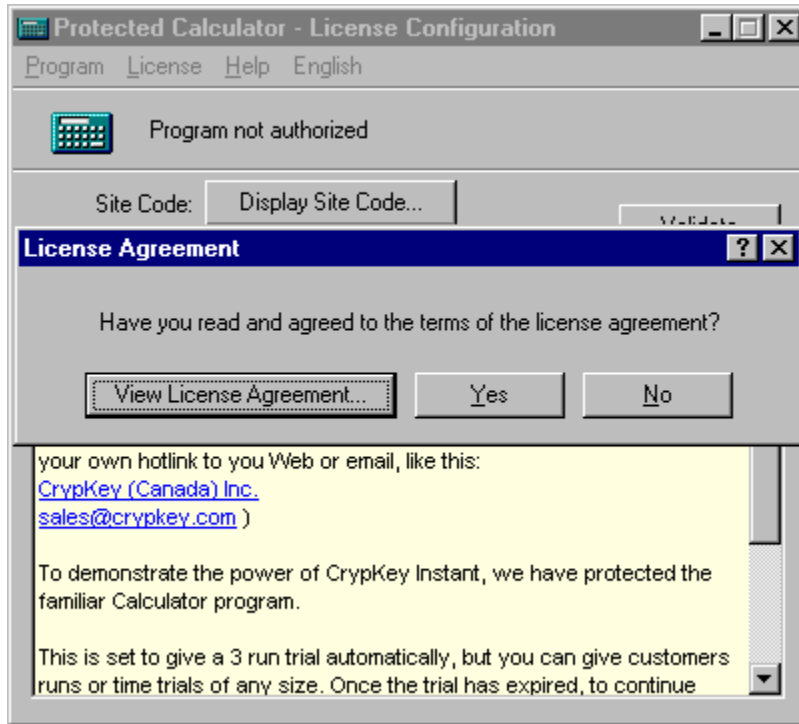
Figure 43: License Agreement Popup

3. Click **View Agreement** or **Yes** to display the site code in the License Configuration window:
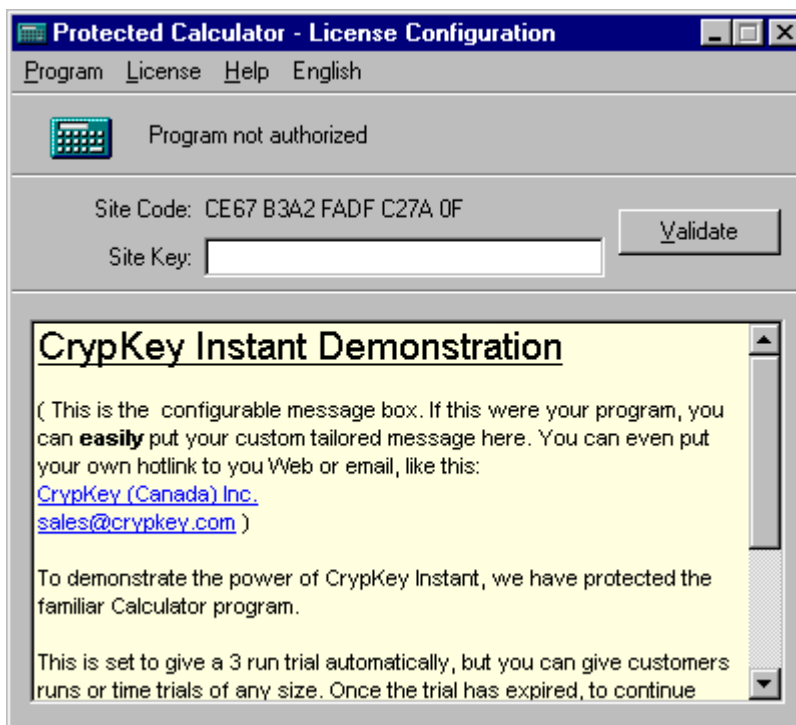
Figure 44: Software Opening Window (CrypKey Instant Protected)

4. Select the site code and copy it to the clipboard, so that you can use it to generate a site key from the Site Key Generator (see the next section).

4.2   Generating a Site Key

In the preceding section, you opened the example Calculator program and found that you were not authorized to use it. You displayed the site code from the License Configuration window. Now you are ready to type the site code into your Site Key Generator program. You can generate a site key that you then use to gain access to the example Calculator program.

Procedure

1. Start the Site Key Generator by double clicking its icon in the CrypKey Instant program group.
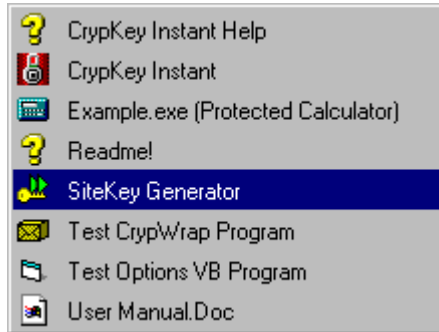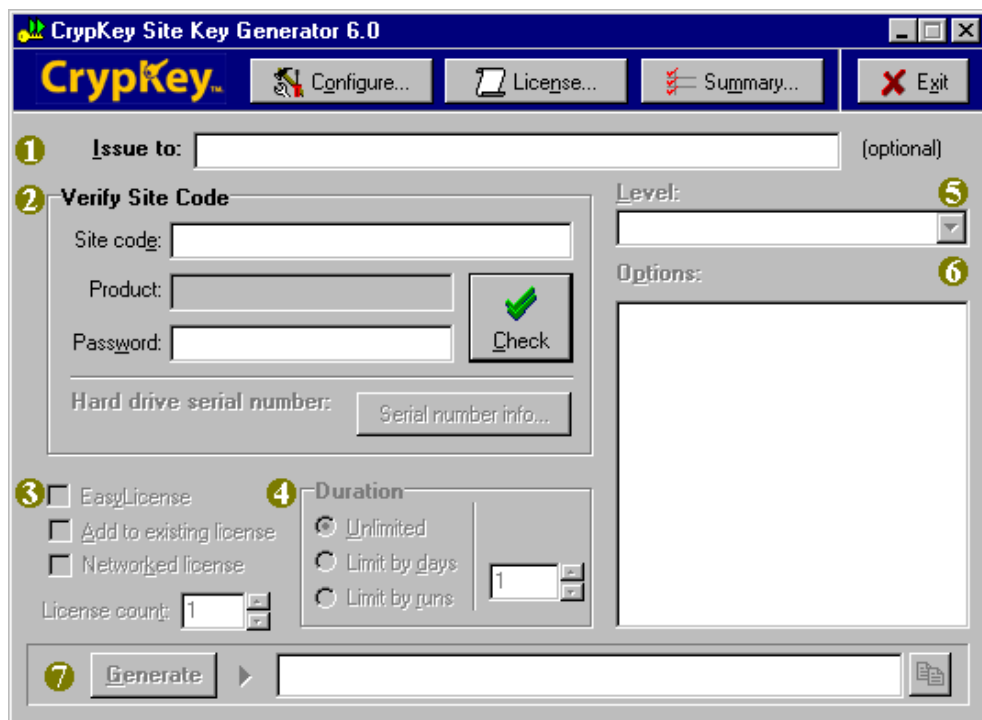
Figure 45: Site Key Generator Start Up

2. The CrypKey Site Key Generator dialog box appears as shown below:

Figure 46: CrypKey Site Key Generator

3. From your clipboard, paste the site code that you obtained from the example Calculator program (see Section 4.1: Producing a Site Code) into the Site Code field. Click **Check.** Ensure the product field reads "example.exe" and the password field reads "KENONIC".
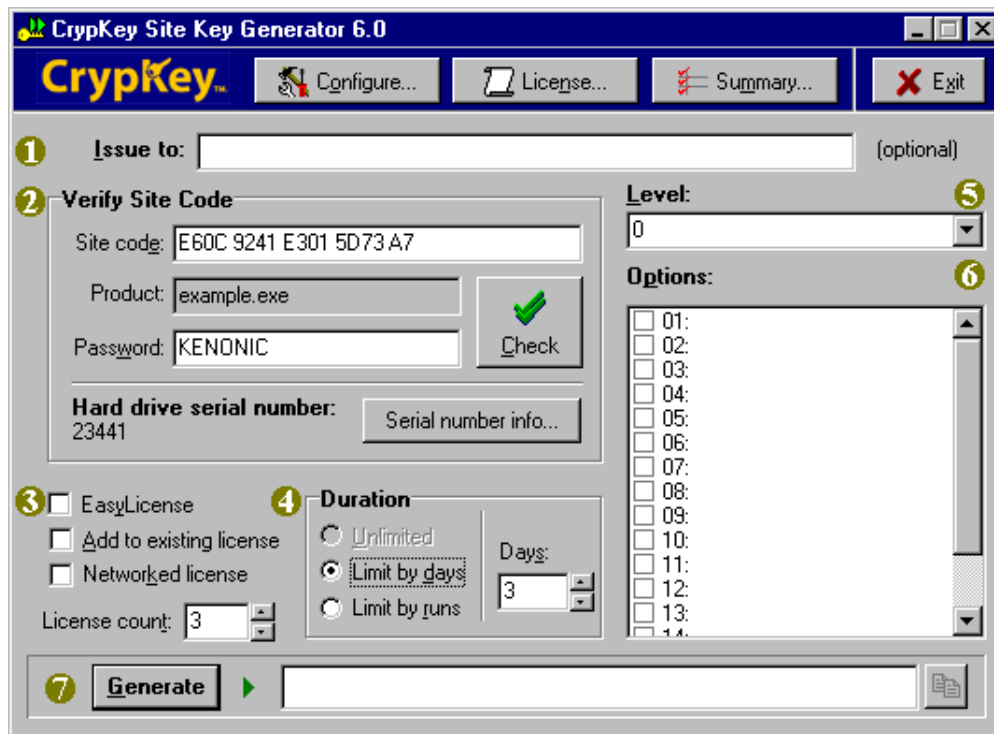
Figure 47: CrypKey Site Key Generator

4. Complete the remaining fields in the CrypKey Site Key Generator dialog box. As indicated in the above figure, you must enter such information as:

- the number of days/runs you want clients to use your product (for demonstration purposes, you are limited to choosing up to three days, or up to three runs).

- the defaults you want the Site Key Generator to use when creating keys (click the **Configure** tab to specify) once you are authorized

- the levels or options you want clients to have (again, click the **Configure** tab to specify)

   Note: using an active but unlicensed copy of the Site Key Generator, you can generate licenses of up to three days or runs.

5. Click **Generate.** The Site Key Generator produces a site key:
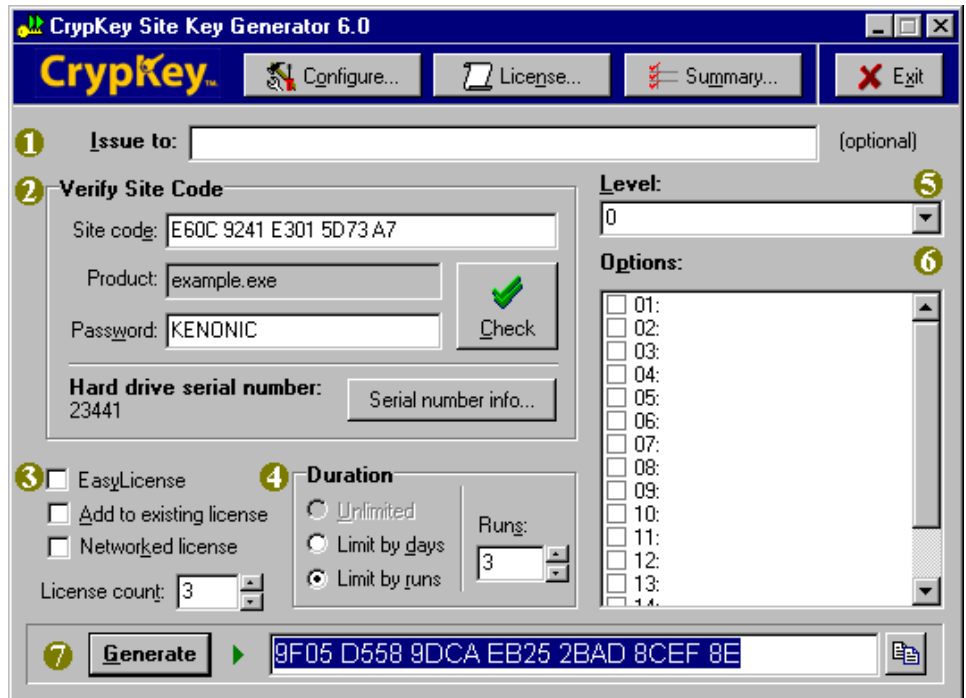
Figure 48: CrypKey Site Key Generator

6. Copy the site key to your clipboard, so that you can use it to authorize your license to use the sample Calculator program (see the next section).

4.3   Authorizing Your Example Program

In the preceding section, you generated a site key using your Site Key Generator program. Now you are ready to use this site key to gain access to your example Calculator program. In this context, you are playing the role of your hypothetical customer.

If you exited the demonstration program before running the Site Key Generator, you'll need to start the demonstration program again by double clicking Example.exe in the CrypKey Instant program group, in order to display the opening License Configuration window:
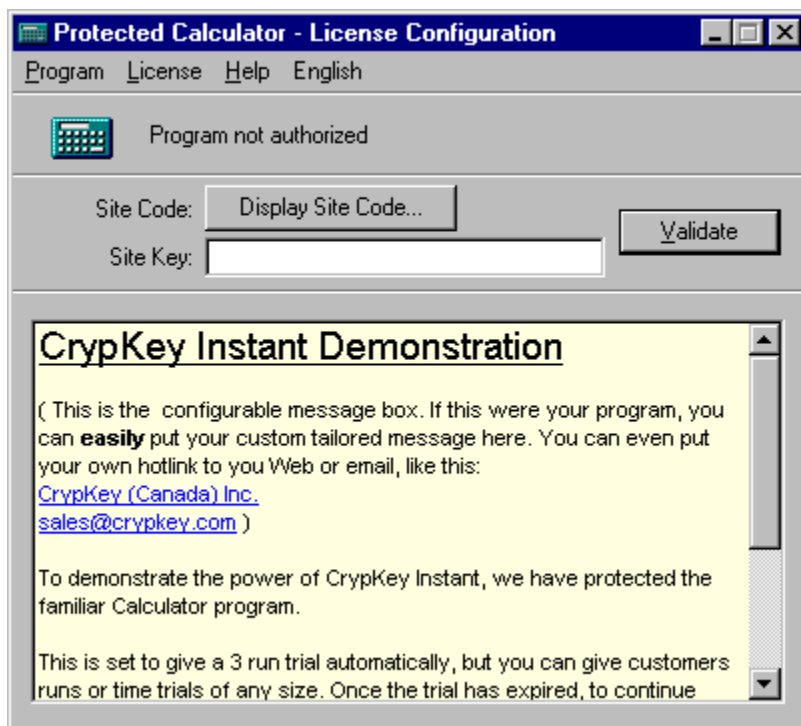
Figure 49: CrypKey Instant Example – Unauthorized License

Procedure

1. In the above window, paste the site key that you have generated (see Section 4.2) into the Site Key field, as shown below:
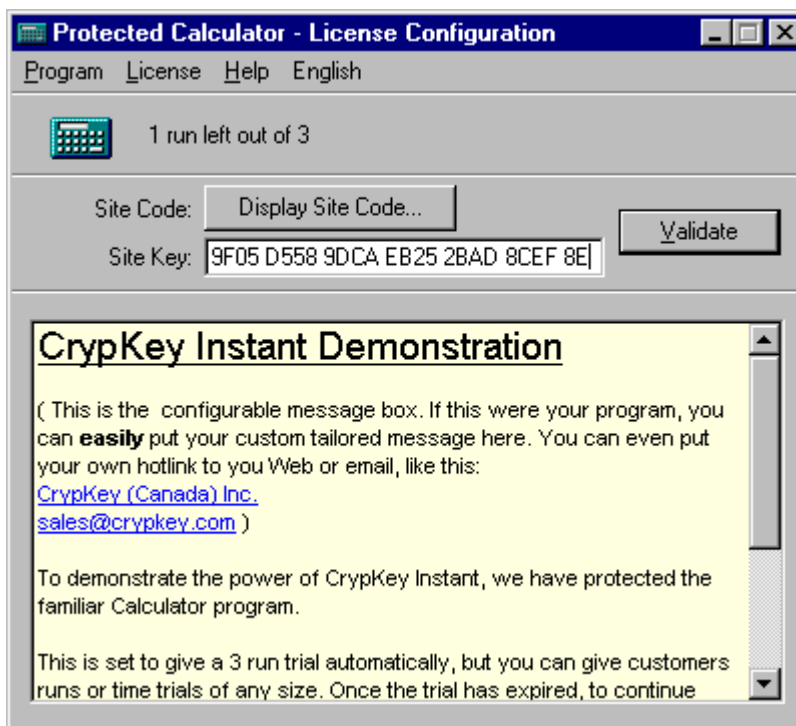
Figure 50: Example License – Site Key Inserted

2. In the above window, click the **Validate** button. The system displays the following popup, confirming that you are now licensed to run the program:
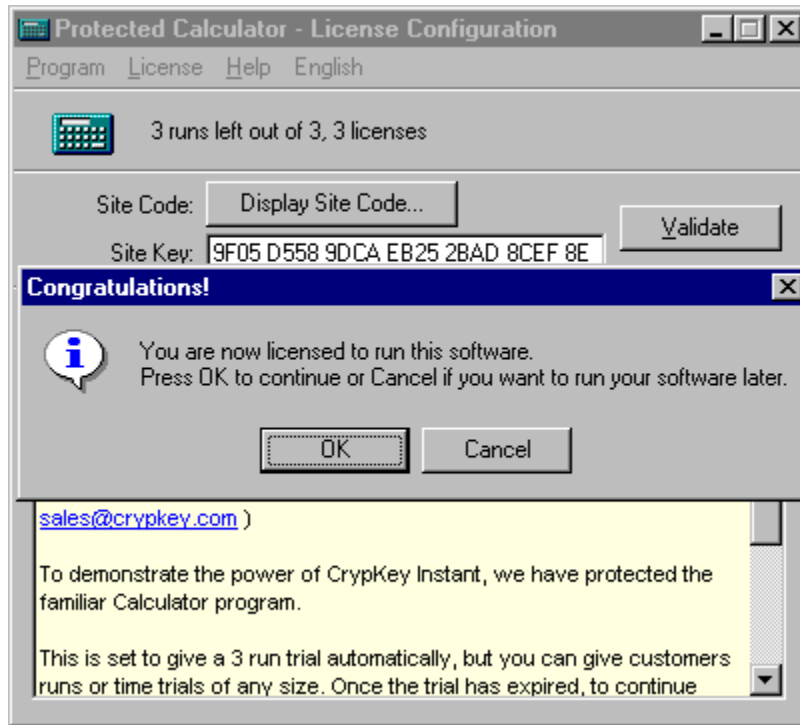
Figure 51: Example License – Confirmation Popup

The above popup confirms that the demonstration program now contains the privileges assigned in the CrypKey Site Key Generator dialog box (see Section 4.2).

Once you have you entered a valid site key into the License Configuration window, the site code automatically changes, indicating that the new information is received. The changed site code appears the next time you click the **Display Site Code** button. This feature ensures your clients cannot enter the same site key twice, which provides you additional security.

3. When you again open the example program, the following splash screen popup window appears:
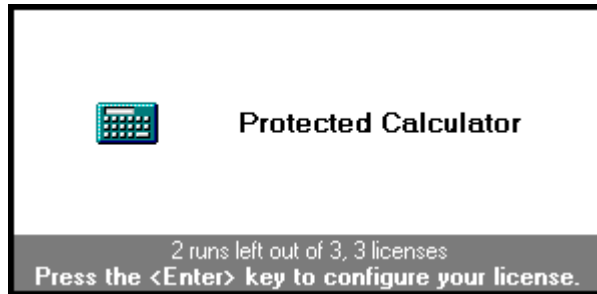
Figure 52: Protected Application Splash Screen

4. You can either do nothing, or click **Enter** within a few seconds of the appearance of the above popup. The results of both of these choices are described below:

- If you do nothing, the above popup disappears and is replaced by the Calculator window, ready for you to use:
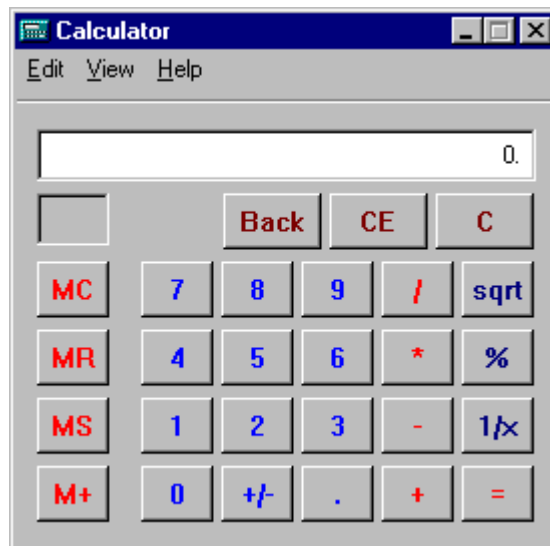
Figure 53: Calculator Program Window

- If you click **Enter**, in response to the CrypKey Instant popup, the following window appears:
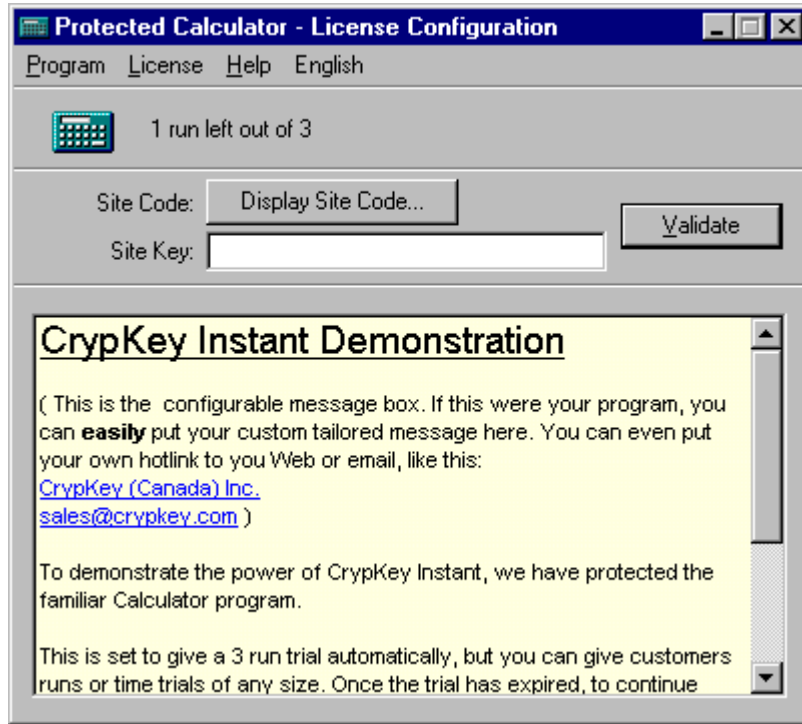
Figure 54: License Configuration Window (Authorized)

The above window gives you (as your hypothetical customer) the ability to transfer the example license between computers, or to "kill" the license. The window provides your customer with the following menu options:

- **Program**

    - **Close** — close the program

    - **Resume program execution** — return to the regular Calculator program operation

- **License**

- **Transfer to directory** — see Chapter 8: Moving Protected Products.

  - **Transfer in from another computer** — see Chapter 8: Moving Protected Products.

  - **Transfer out to another computer** — see Chapter 8: Moving Protected Products.

  - **Kill license** — delete the license for the application acquired from the vendor. The **Kill license** function generates a "kill" code, which the customer can send to you as verification after deleting a license for your software. You can use the Site Key Generator to verify this code.

- **Help** — online help

- **English** — selection of language used for the application interface.

Site Key Generator

CrypKey Instant's Site Key Generator allows you to authorize clients to use your product.

I ntegral to CrypKey protection, the Site Key Generator creates the keys that unlock your product. You can limit the number of days or runs over which clients can use your product, or implement the unlimited usage option. You can also specify the number of program copies that can be made and the number of concurrent network users that are allowed. In addition, you can review previous transactions and sort them by date, customer name or product name, and you can review archived log files.

5.1   Levels and Options

CrypKey levels and options allow you to authorize different features of your product. For example, if your product has multiple components and you want your clients to pay by component, you would select only those components your clients want when you issue their site key.

CrypKey levels and options are defined within a single 32-bit programming "word"; the combined total number of bits that can be used for levels and options is therefore 32. You control which portions of this total are assigned to levels and to options. For example, you could implement 28 options (note that each option uses one bit) for your product — keeping in mind that only four bits would now remain, out of the original 32, for implementing levels. The maximum number of possible levels in this case would be 2^4, or 16.

Within the above framework, you set up a range of levels and options for each product, using the Site Key Generator **Configure** tab page (see Sec. 5.3.2: Configuring Your Products). While you can assign multiple options to a product, you cannot assign more than one level for any given license for that product.

The wrapping function sets decimal-format values for the option and level information in the **CKLEVEL** and **CKOPTION** environment variables. Your application code typically converts the **CKOPTION** value into a binary number. Your CrypKey Instant-protected application then uses the position of the bits, starting with the least significant bit, to identify enabled and disabled options. Enabled options have the value 1, and disabled options, 0. For example:

CKOPTION = 1235

1235 converted to binary = 10011010011

Counting from the right-most digit, the value 10011010011 means that options 1, 2, 5, 7, 8, and 11 have the value 1 and are therefore enabled

In the case of the **CKLEVEL** decimal value, that value is the number assigned to the level. For example, a value of 12 denotes Level #12.

When your customer requests a license authorization for a product, you use the Site Key Generator to:

- select a level (only one of the available levels) and options specifying what access you are providing to the customer for that product.

- issue a site key to the customer. The site key incorporates the selected level and options.

A further refinement is provided in the CrypKey Instant protection bundled into your application: namely, how the privileges and restrictions configured using the Site Key Generator are implemented with the application. These specifications can be applied as defined in the Site Key Generator, or on a module-by-module basis — see Chapter 6: Using CrypKey Instant.

When you issue a site key to the customer, the customer enters the site key into your protected application on his or her computer. The levels and options information, encoded into the site key, becomes a permanent part of the customer's license, defining the customer's usage privileges for the application.

5.1.1   Levels

With levels, you can choose one feature or style you want your clients to have. For example, you can divide your software into beginner, intermediate, and expert levels.

A level is an integer that controls a variety of features in your product. For example, you might devise the following definitions:

- Level 0: no additional modules can be used

- Level 1: the graphic module can be used

- Level 2: the graphic and printing modules can be used

Levels can also be used for version control. For example, you might decide that the first version (v1) of your software runs regardless of level, while v1.1 requires Level 1 and v1.3 requires Level 2. Level strategies relating to versions are numerous, but you can choose only one level for any given license. Levels are configured using the **Configure** tab page of the Site Key Generator.

5.1.2   Options

With options, you can toggle on or off one or more different features of your product.

- An option is a single bit used like an on/off switch. For example, if you want to offer clients, for extra cost, a module that allows your product to perform printouts, you could make this, say, the fifth option. If the value assigned to this option is 1, the module can be run. If the assigned value is 0, the module cannot be run, and a message appears noting that the option has not been purchased.

CrypKey Instant transmits level and option information to your product. Note, however, that **source code changes are required** for your program to use this information.

Options are configured using the **Configure** tab page of the Site Key Generator.

5.1.3   Configuring Levels and Options

Following is the general process of assigning levels and options for a product and specifying which of these are included in a given customer license. For detailed procedures, see Sec. 5.3: Using the Site Key Generator, as well as Chapter 6: Using CrypKey Instant.

Procedure

1. Determine and design the levels and/or options your product has. You may decide to use only levels or options, or use both together.

2. Reconfigure your product to run according to your levels and options design (i.e., program your product to execute the action associated with each specified level and option). For example, if you decide that when Option 5 is enabled, your product allows clients to run the compression module, so you must implement this logic in your product.

3. Modify your product's source code to receive the levels and options information transmitted by CrypKey Instant.

4. Open CrypKey Instant and specify the name of the application that you are protecting.

5. In the CrypKey tab page of CrypKey Instant, shown below, click one of the following checkboxes:

    - **Pass option and level information**

    - **Allow modules to run based on options**
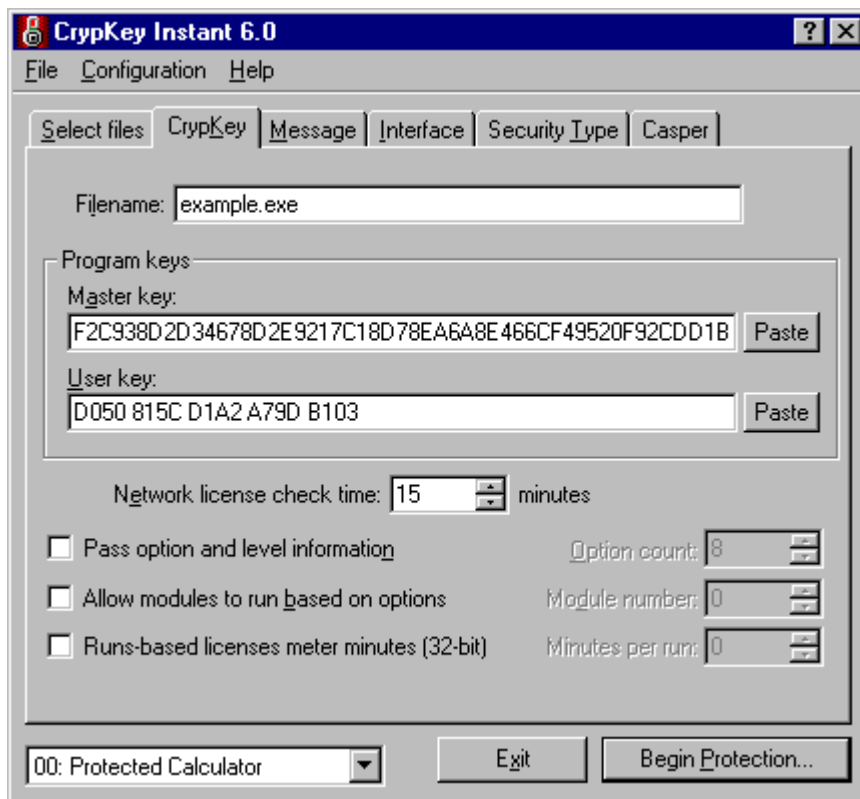
Figure 55: CrypKey Instant – CrypKey tab page

For more information on the above window, and specifically concerning the functions **Pass option and level information** and **Allow modules to run based on options**, see Sec. 6.6.4: CrypKey tab page.

6. Configure your levels and options for the product, using the **Configure** tab page of the Site Key Generator — see Sec. 5.3.

5.1.4   Internal Handling of Levels and Options

The following mechanisms are used to transmit level and option values to your application. These mechanisms apply for any settings that you make via the Site Key Generator and CrypKey Instant interfaces.

For 16-bit Windows or DOS Applications

If your product is a 16-bit Windows or DOS program, CrypKey Instant transmits your levels and options information to your application by appending the following command line arguments:

```
/LEVEL=PassedLevel
```

and

```
/OPTIONS=PassedOptions
```

where

- *PassedLevel* is replaced by the integer at which the level is currently set

- *PassedOptions* is an integer where each bit represents an option. The lowest bit is Option 1, the next lowest bit is Option 2, etc., as explained below.

For example, if your program file name is PROG1.EXE, and your license offers 23 levels and no options, CrypKey Instant makes your software appear to run as if this information was entered into the command line as follows:

```
PROG1.EXE /LEVEL=23 /OPTIONS=0
```

The commands CrypKey Instant appends to the command line always occupy the last two fields. To prevent attempts to enter these parameters manually with a view to deceiving the protection program, ensure that you verify values in these last fields when checking the command line levels and options.

For 32-bit Windows Applications

If your product is a 32-bit Windows program, CrypKey Instant transmits your levels and options information to your application by adding the following to the environment variables:

```
CKLEVEL=PassedLevel
```

and

```
CKOPTIONS=PassedOptions
```

where

- *PassedLevel* is replaced by the integer at which the level is currently set

- *PassedOptions* is an integer where each bit represents an option (the lowest bit is Option 1, the next lowest bit is Option 2, etc.)

If you are using Visual Basic, note that you must call a Windows API function to process these environment variables, since Visual Basic functions cannot obtain variables created by CrypKey Instant. The function you need to use is **ExpandEnvironmentStrings**.

Although your programming language defines your work path, you must process the PassedOptions integer to obtain from it the value of each option. In general, if you convert this value to a binary number, each bit in the binary number represents an option, with the lowest bit representing the lowest option.

For example, if Options 1, 2, and 5 are on, the representative binary number is 10011. Converted to decimal, this number is: $1x1 + 1x2 + 0x4 + 0x8 + 1x16 = 19$.

Following is one possible algorithm for converting the decimal number to options:

```
declare integer OptionArray [1 to 32], initialize all to zero
declare integer i
declare integer Options = PassedOptions
for i = 1 to 32
if Options is an ODD number, OptionArray[i] = 1
Options = Options/2 (integer division rounds down (i.e.
19/2=9))
```

Let's explore how this works on our decimal example of 19 above:

- iteration 1: i = 1, Options = 19, this is ODD, OptionArray[1] = 1

- iteration 2: i = 2, Options = 9, this is ODD, OptionArray[2] = 1

- iteration 3: i = 3, Options = 4, this is not ODD, OptionArray[3] = 0

- iteration 4: i = 4, Options = 2, this is not ODD, OptionArray[4] = 0

- iteration 5: i = 5, Options = 1, this is ODD, OptionArray[5] = 1

- iteration 6: i = 6, Options = 0, this is not ODD, OptionArray[6] = 0

- the rest of the iteration also produces 0

We see that we obtain the correct answer by following this procedure, which is easy to implement in programming languages such as Visual Basic.

5.2 Additional Features of the Site Key Generator

Besides Levels and Options, the Site Key Generator offers flexible restrictions on licenses, EasyLicense for the user's convenience, CloneBuster[TM] technology to prevent hard drive cloning or "ghosting", and a summary view of your licensing transactions.

5.2.1 License Duration Settings

You can create three types of licenses for your clients, all of which can be transferred directly via direct transfer or by floppy disk:

- Runs: allow clients to run your product for a specific number of runs (maximum: 32,768)

- Days: allows clients to run your product for a specific number of days (maximum: 32,768)

- Unlimited: allows clients to run your product without restrictions

When you are authorizing distributors (see Sec. 5.5.1), the RUNS_ONLY and DAYS_ONLY options are available . When you enable RUNS_ONLY and select the runs license, the slave Site Key Generator can only create runs licenses. In addition, the total number of runs the generator grants a product is decremented from its own license count. Therefore, if a slave Site Key Generator is awarded a runs license with 1,000 runs, and the RUNS_ONLY option is enabled, the generator has 800 runs left if it issues 200 runs to a product. The same theory holds true for the DAYS_ONLY option and days license.

Clock Manipulation Checks

Programs available on the market are designed to try to deceive time-restricted software protection systems. These programs automate the process of changing a computer's clock in order to bypass time-restricted protection. These programs change the time registered by the protected program. For example, if the registered time never extends beyond your program's trial period, a user can in theory run your program indefinitely.

CrypKey Instant safeguards against clock manipulations by monitoring your customers' computers for the inconsistencies generated by such an attack. CrypKey Instant detects when time is falsely reported to your program, and prevents your program from running. All times reported by CrypKey are the server's, adjusted to the local time zone of the computer.

CrypKey Instant may also detect clock manipulation if users adjust their computer clock by more than several hours, even for benign purposes such as testing. If your program is prevented from running in these situations, your customers can correct the situation by rebooting their computer.

5.2.2   EasyLicense

Some customers need the simplest possible form of copy protection: a particular application runs only on a particular computer. These customers do not want to deal with any associated issues of transfer, network license, trial period, or number of copies. Whether the software gets offloaded and put back, or is deleted and restored later, or the *entire* hard drive gets erased and restored... the application must *still* run on the computer.

EasyLicense meets these requirements. The features of EasyLicense can be summarized as follows:

- Clients can back up their licenses and restore them later.

- The license files can be moved without affecting the license itself.

- The license transfer ability is disabled to prevent abuse.

- The only license type available for EasyLicense is an unlimited license.

EasyLicense works on any system that supports CrypKey's HDSN technology.

EasyLicense Backup and Restore

Apart from the EasyLicense type of license, it is not possible to back up or restore CrypKey licenses. The reason for this is that the other types of CrypKey licenses, i.e. those with time or run restrictions, are transferable by the user, and the availability of backup-restore would allow the user to duplicate these licenses. However, by design, the EasyLicense is not transferable — and, consequently, it can be backed up and restored. You can think of EasyLicense as a permanent authorization of a program for a particular hard drive.

Procedures

It is simple to back up and restore a valid Easy License.

To back up EasyLicense:

Copy to a safe place, such as a floppy disk or another computer, the following license files:

- *yourfilename.key*

- *yourfilename.rst*

To restore EasyLicense:

Install the software if it is not already present, and simply copy the above two files back to the directory where they came from. If the software is on the same hard drive as it was when the license was backed up, the license is restored.
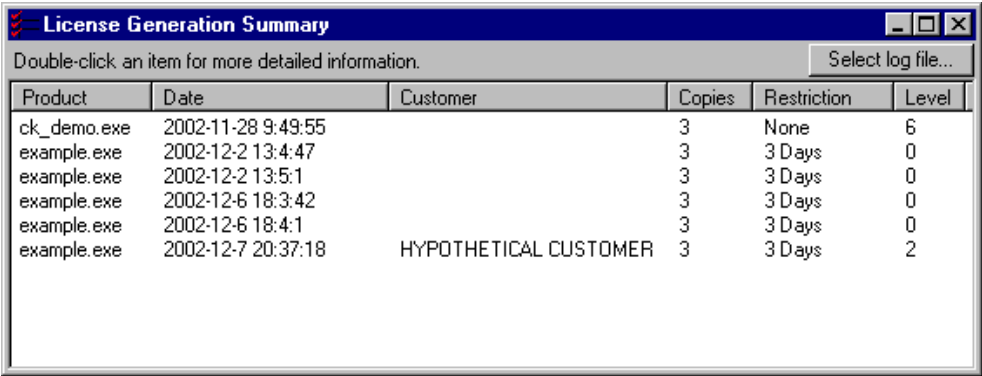
5.2.3   CloneBuster^{TM} Technology

CrypKey 6.0, with the new patent-pending **CloneBuster^{TM}** technology, effectively solves the problem created by the upsurge in software products that clone hard drives. Many popular copy protection technologies that depend on placing some type of simple software footprint are now easily defeated by these products, and are no longer an effective option. Hardware dongles provide limited protection against to HD cloning, but are expensive and somewhat unpopular.

Most modern IDE hard drives have burned-in serial numbers (HDSN). The HDSN is a permanent read-only attribute of a personal computer hard drive (rather than the easily changed "Volume" serial number). The HDSN is very difficult to access, but the new CrypKey Instant 6.0 with CloneBuster^{TM} technology has this ability. Utilizing CloneBuster^{TM}, CrypKey detects and logs the HDSN, model number and firmware identifier, and then uses this information in its proprietary licensing algorithms. This ensures that your CrypKey-protected applications are not fraudulently transferred to unauthorized computers.

5.2.4   Transaction Summary

The Site Key Generator includes a **Summary** button that you can use to view license activity. When you click this button, the system displays the following window:

Figure 56: License Generation Summary Window

5.3   Using the Site Key Generator

To start the Site Key Generator, you must first have obtained the license to use it from CrypKey (Canada) Inc. For details on obtaining the license, see Sec. 2.1: Obtaining Your Developer Keys.

Once you have obtained your Site Key Generator license, the main Site Key Generator window appears when you select the SKW icon:
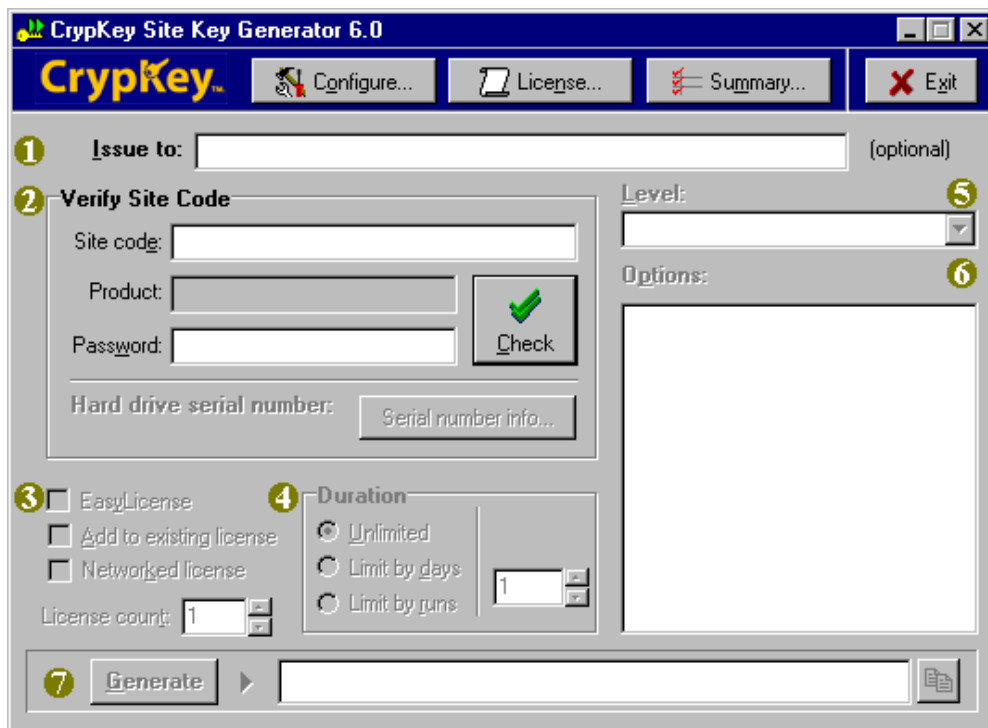
Figure 57: CrypKey Site Key Generator 6.0 Window

The Site Key Generator function handles the identification and general authorization of your clients, as well as the definition of your products and associated license terms, options and levels. CrypKey Instant adds some refinements to these elements (see Chapter 6: Using CrypKey Instant).

5.3.1   Generating Site Keys

The CrypKey Site Key Generator 6.0 Window enables you to authorize your customers to use your product. When a customer loads your CrypKey-protected application on his or her computer, the application generates a site code. The customer sends you the site code, which you use in the Site Key Generator to produce a site key. You send this site key to the customer, who uses it to unlock your application under the terms you have defined in the Site Key Generator.

When you issue a site key to a customer, you are authorizing that customer to use your product. This is a different operation from that of configuring the restrictions on the

product itself, which you do using the **Configure** tab page of the Site Key Generator (see Sec. 5.3.2).

Procedure

1. Receive the customer's site code generated from your installed application.

2. Start the Site Key Generator, using the **SKW** ⚔️ icon. The system displays the CrypKey Site Key Generator 6.0 Window.

3. Optionally, type the customer name into the **Issue to** field.

4. In the **Site code** field, type in the site code provided by the customer, then click the **Check** button. The window appears as follows:
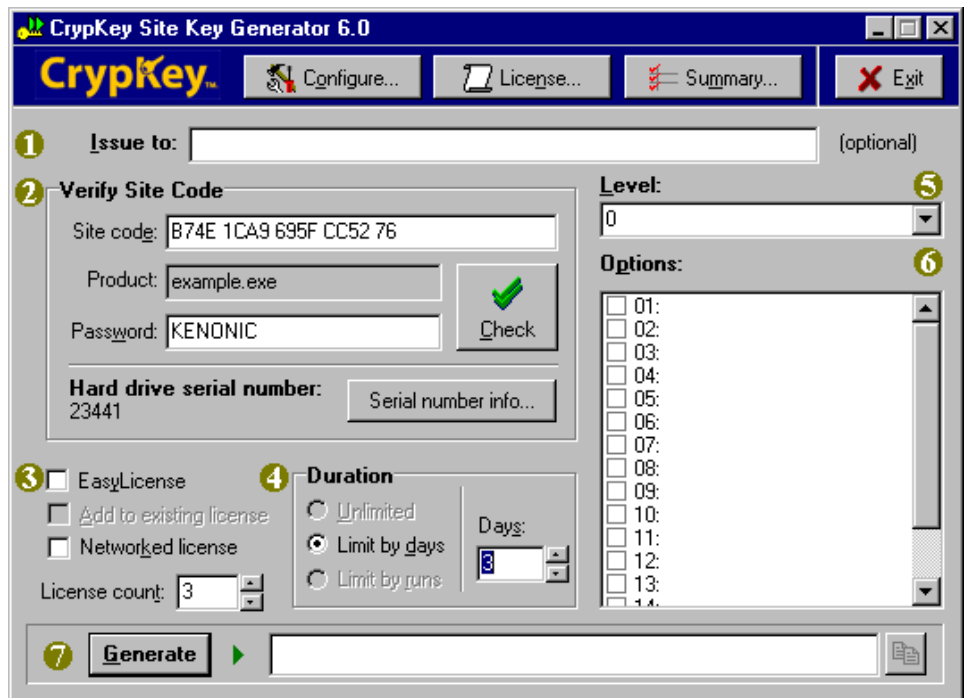
Figure 58: Site Key Generator – Starting Authorization

If CrypKey Instant encounters a problem finding or reading the hard drive serial number (HDSN), it displays an error message.

5. Optionally, click the serial number info button to display the customer's hard drive serial number (HDSN) information, if available:
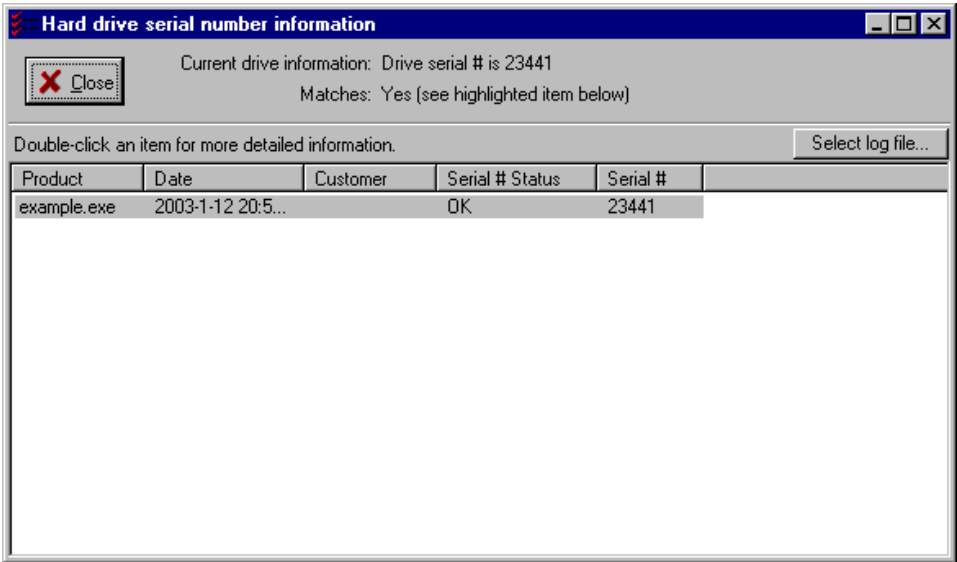
Figure 59: Hard Drive Serial Number Information Window

The HDSN exists on most computers currently manufactured. If CrypKey has a problem finding or reading the HDSN, the serial number is shown as unavailable in the HDSN information window above.

You can double-click any information entry line in the above window to display the License Details window shown below:
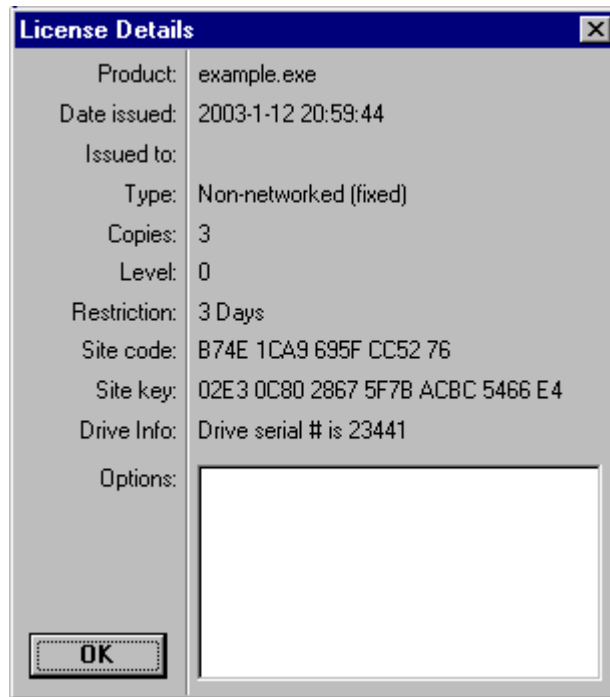
Figure 60: HDSN License Details Window

You should record the HDSN information for future reference. For example, it is helpful for verification purposes in the event that your customer asks you for re-authorization following a computer crash.

6. Verify the license terms generated from your application at your customer's computer. You can change the license duration, expressed as **unlimited**, **days**, or **runs** (for details, see the next section, Configuring Products).

7. In the **Level** box, click the drop down arrow to assign one of the levels (if any) that were pre-defined during the product configuration.

Note: There is a special requirement here, if you are using the CrypWrap feature of CrypKey Instant for the same product (see Sec. 6.6.7: Security Type tab page). If you are enabling CrypWrap encryption, you must enter the same encryption key into the **Level** box that you specify in the **Security Type** window of CrypKey Instant.

8. In the **Options** box, click the checkboxes beside the product options that you wish to activate for the customer.

9. Click the **Generate** button.

The system generates a 26-character alphanumeric value and places it in the box beside the **Generate** button. This is the site key that you send to your customer. It contains all of the specifications you have entered concerning license terms, level, and options.

When your customer receives the site key and enters it into the CrypKey window of the installed application, the customer is authorized to use that application under the license terms defined and with the restrictions that you specify in the CrypKey Instant protection (see Chapter 6: Using CrypKey Instant).

5.3.2   Configuring Your Products

To specify the products that your clients are authorized to use, use the **Configure** window of your Site Key Generator. This is a separate operation from that of generating Site Keys (see Sec. 5.3.1).

Procedure

1. In the CrypKey Site Key Generator 6.0 Window, click the **Configure** button.

The system displays the **Configure** window:
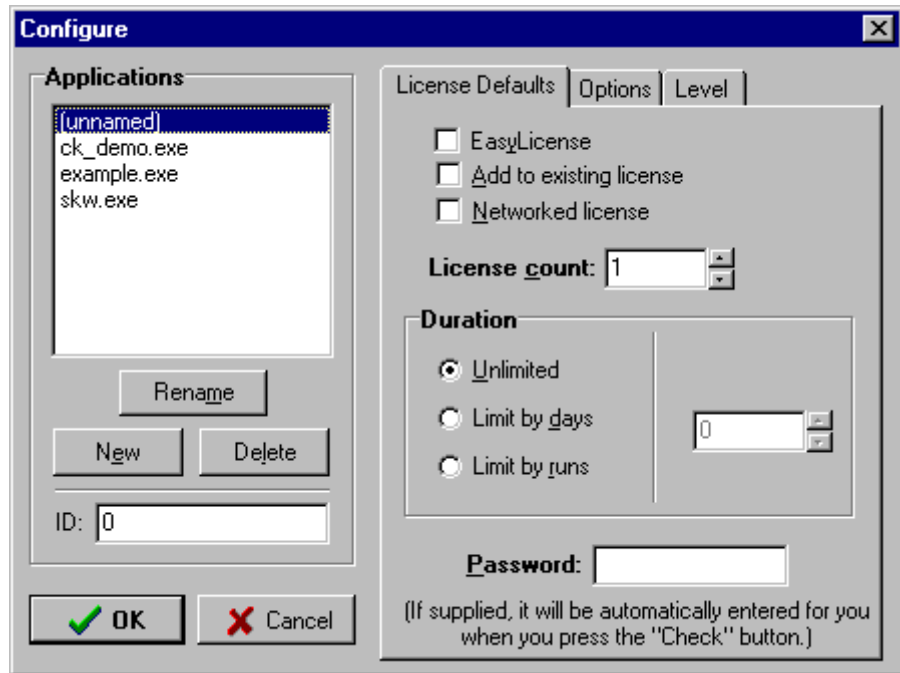
Figure 61: Configure Window

2. If you are editing an existing product file, click the applicable name in the Applications list. Proceed to **Step 4**, below.

If you are configuring a new product, click **New** in the above window. The system displays the **Configure** window with the **New Application** popup superimposed onto it:
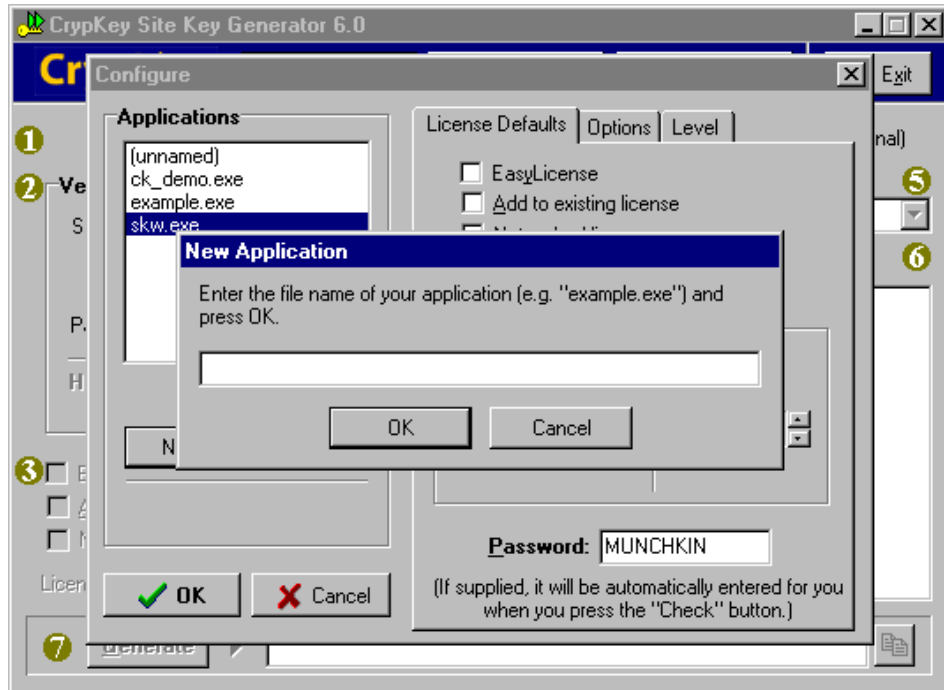
Figure 62: Site Key Generator with New Application Popup Window

3. Type the product's file name into the blank field and click **OK**. The popup window disappears, and the name you have typed is displayed in the **Applications** list, as shown below:
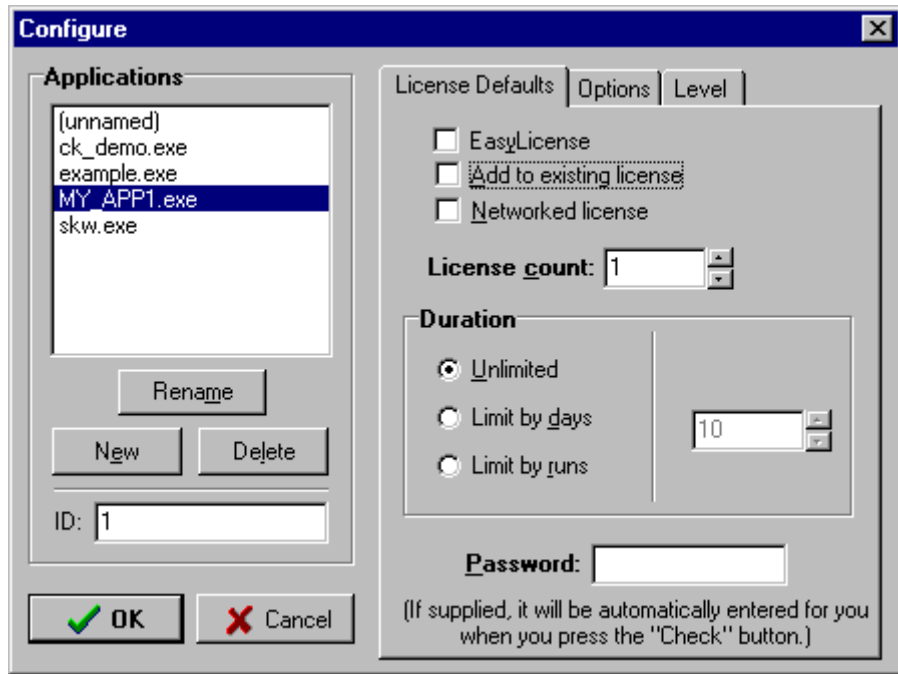
Figure 63: Configuration Window with New Application

You can rename or delete the new entry, or any existing entry, by clicking the name in the list, then clicking the **Rename** or **Delete** button.

4. In the **ID** field, enter a unique product identifier — for example, enter 1 if you are configuring your first product.

5. In the **License Defaults** tab page, set the default restrictions for the product. Note that the license automatically defaults to "Fixed" if you do not specify a network license. The checkbox choices are as follows. Note that these are defaults for the specified product, and can be changed as needed for specific customers.

    EasyLicense — unlimited license with no restrictions

    Add to existing license — used if a customer with an existing license is specified in the CrypKey Site Key Generator 6.0 Window

    Networked license — used if the application is to be run by one or more users connected to a server.

    License count — maximum number of seats that a customer can have for the specified product.

    Duration — amount of usage allowed under the license. This can be unlimited (the default), or can be expressed in number of days or runs. If you select days or runs, the number box to the right becomes active, and you can enter the number of days or runs allowed for the license.

    Password—the password that must be referenced in the site code returned to you by your customer. A password specified here is automatically entered into the **CrypKey Site Key Generator 6.0** Window when you click the **Check** button to verify a customer's site code.

6. Click the **Options** tab to display the Options tab page:
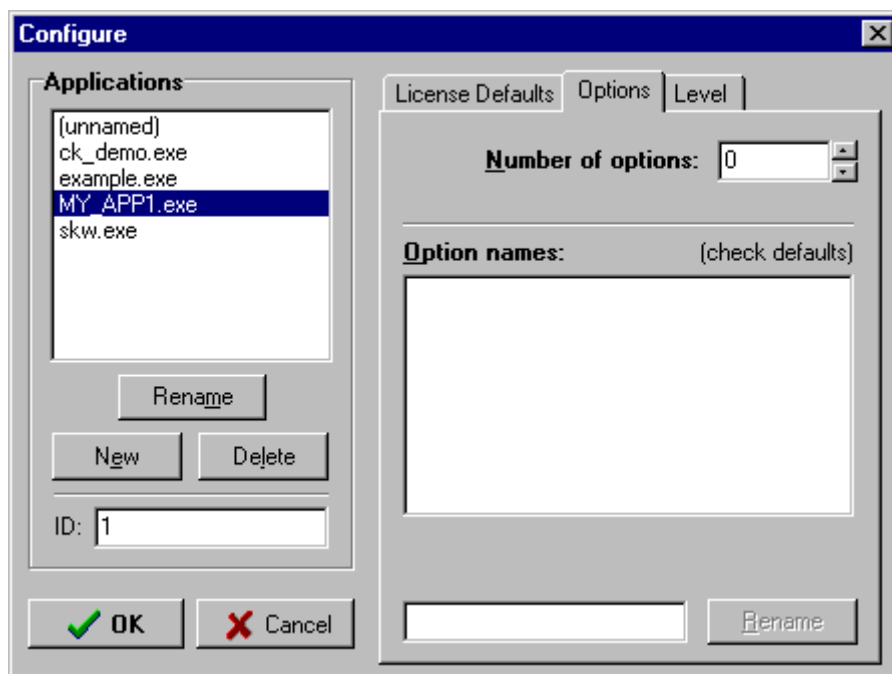
Figure 64: Site Key Generator – Options Tab Page

7. In the above window, click the combo box arrows to increase or decrease the number of options to be assigned to the product. As you increase the number, undefined option entries with checkboxes appear in the **Option names** sub window, as shown below:
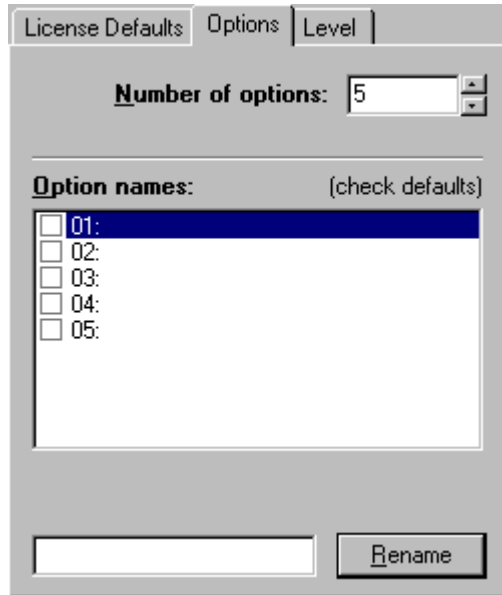
Figure 65: Site Key Generator – Options Combo Box

If you click on an entry number, such as 01, the cursor moves to the name box at the bottom of the Options sub window and you can assign a name to the option.

8. Click the checkboxes beside the options that you wish to assign as defaults for the product.

9. Click the **Level** tab to display the **Level** tab page:
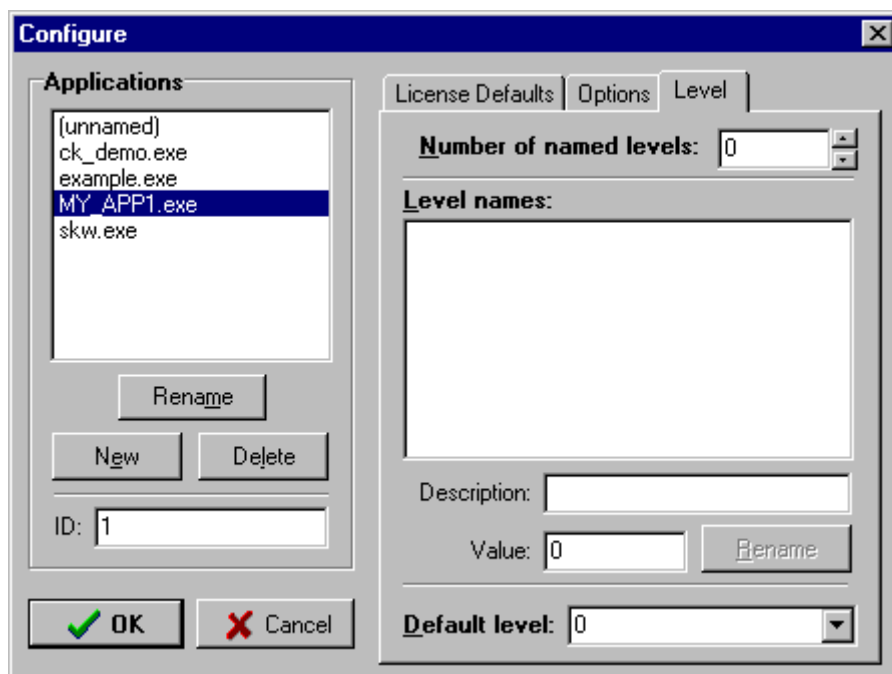
Figure 66: Site Key Generator – Levels Tab Page

10. In the above window, click the combo box arrows to increase or decrease the number of levels available to be assigned to the product. As you increase the number, undefined level entries appear in the **Level names** sub window, as shown below:
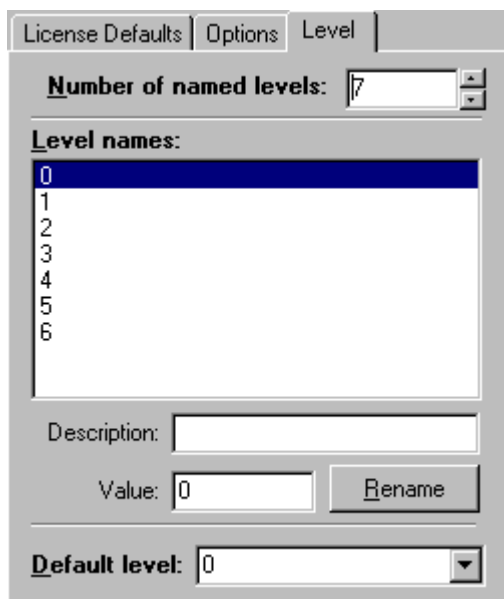
Figure 67: Site Key Generator – Levels Combo Box

If you click on an entry number, such as 1, the system places that number in the **Value** field and you can assign a name to the level.

11. In the **Default level** field, type in the value (or use the arrow to select the value) representing the level that you wish to assign as a default for the product.

5.4   Incrementing Existing Licenses

The Site Key Generator allows you to change the levels, options, type, and restriction of an existing client license. You can do this only if you have a valid site code from an authorized copy of CrypKey-protected software. You cannot toggle this option using your site code from the trial period

Procedure

1. Click the SKW icon in the CrypKey program group to display the Site Key Generator main window.

2. Enter a valid site code into the **Site Code** field.

3. Click the **Add to Existing License** checkbox in the Site Key Generator dialog box, as shown below:
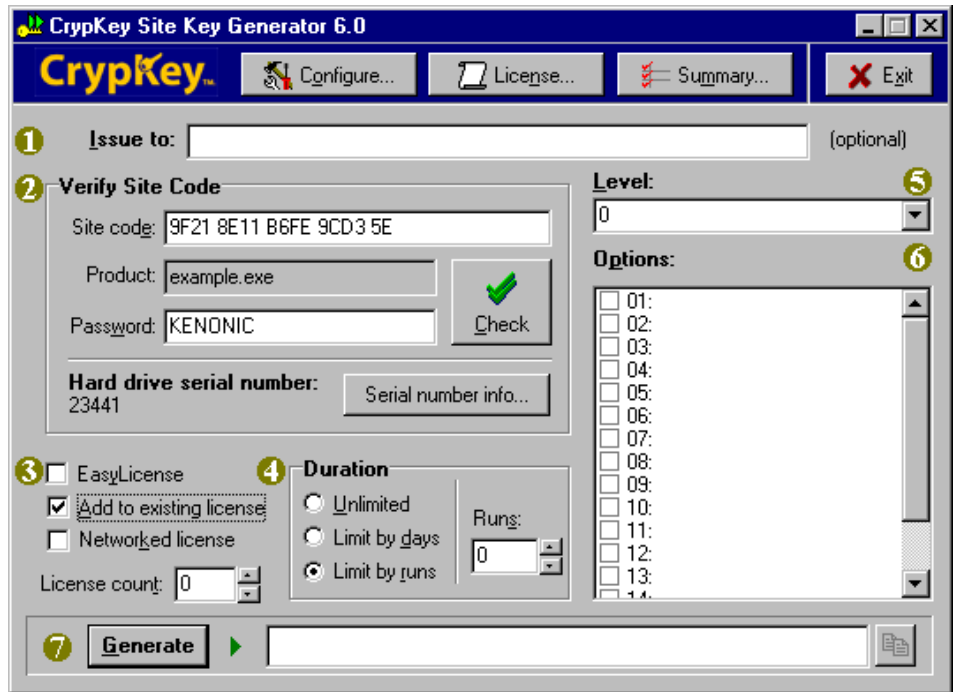
Figure 68: Site Key Generator Window

4. Specify levels, options, and duration of the license. These changes are added to the license for the customer who provided the site code.

5. Click the **Generate** button to produce a new site key for the customer.

5.5 Distributor Authorizing License

The Distributor Authorizing License (DAL) enables you to authorize your customers to act as distributors, using copies of the Site Key Generator — provided by you — to authorize your product. You hold the **master** Site Key Generator and each of your distributors holds a **slave** Site Key Generator.

The benefit of bringing distributors into your business plan comes from increased distribution and sales of your product. Distributors authorize **their** clients to run **your** product — based on the number of runs, days, or copies that you specify — thereby expanding your worldwide market base, hassle-free.

To obtain authorization for the DAL, send us the site key from your Site Key Generator once you have paid for this feature.

5.5.1 Authorizing Distributors

Your master Site Key Generator (SKG) can apply the following constraints to licenses assigned to a slave SKG:

- It can limit the number of licenses that the slave SKG can generate.

- It can limit the number of days during which the slave SKG can be used to distribute licenses.

- It can restrict the total limitation of days or runs that the slave SKG can apply to licenses issued by it.

  Note: A single slave SKG can issue only one type of license, i.e. either runs-based or days-based but not both. If you want your distributor to issue, say, 10 day-type licenses and 10 run-type licenses, then you need to have them install copies of the skw.exe and skw.ini files into separate directories, licensing each slave SKG for a specific license type.

The number of licenses that a slave SKG can issue is based on the usage count. Each time the slave SKG generates a key, it decrements its usage count. The usage count of a slave SKG is regulated by the Duration setting in the master SKG. The effects of various duration settings and the usage count are detailed in Table 3, below.

The License Count should be set in the Master SKG to the value 1, unless you are issuing a network license for the SKG slave. The license count is the number of users who can simultaneously run the licensed application.

If your application has a non-network license, then the License Count represents the number of licenses available to be transferred out. For example, if you license Product X as a non-network application with a License Count of 3, the user could make a copy of the program on two other computers and transfer a license to each of them, making a total of three licensed copies.

Table 3: Effects of Duration Settings for Slave Site Key Generator

Duration Setting	Option Setting	Effect
Unlimited		Slave SKG can generate an unlimited number of licenses for the specified product.
days = 10		Slave SGK can generate an unlimited number of licenses for the specified product, but stops functioning after 10 days.
runs = 15		Slave SGK can generate up to 15 licenses for the specified product.
Unlimited	Days Only	Slave SGK can generate an unlimited number of Day-type licenses (but not Run-type licenses) for the specified product.
days = 10	Days Only	Slave SGK can generate an unlimited number of Day-type licenses (but not Run-type licenses) for the specified product, but stops functioning after 10 days.
runs = 15	Days Only	Slave SGK can generate up to 15 days of total license time. In this case you could issue one 15 day license or three 5-day licenses for the specified product.
Unlimited	Runs Only	Slave SGK can generate an unlimited number of Run type licenses (but not Day-type licenses) for the specified product.
days = 10	Runs Only	Slave SGK can generate an unlimited number of Run type licenses (but not Day-type licenses) for the specified product, but stop functioning after 10 days.
runs = 15	Runs Only	Slave SGK can generate up to 15 runs of total

Duration Setting	Option Setting	Effect
		license run time.
		In this case the slave could issue one 15-run license or two 6-run and one 3-run license, for the specific product.

Procedure

1. Send your distributor a copy of the Site Key Generator. This copy of the Site Key Generator is unauthorized at this stage.

2. Tell your distributor to:

   a) Run the unauthorized copy of your Site Key Generator.

b) Click **License** in the Site Key Generator License Authorization dialog box to display the following dialog box showing the site code:
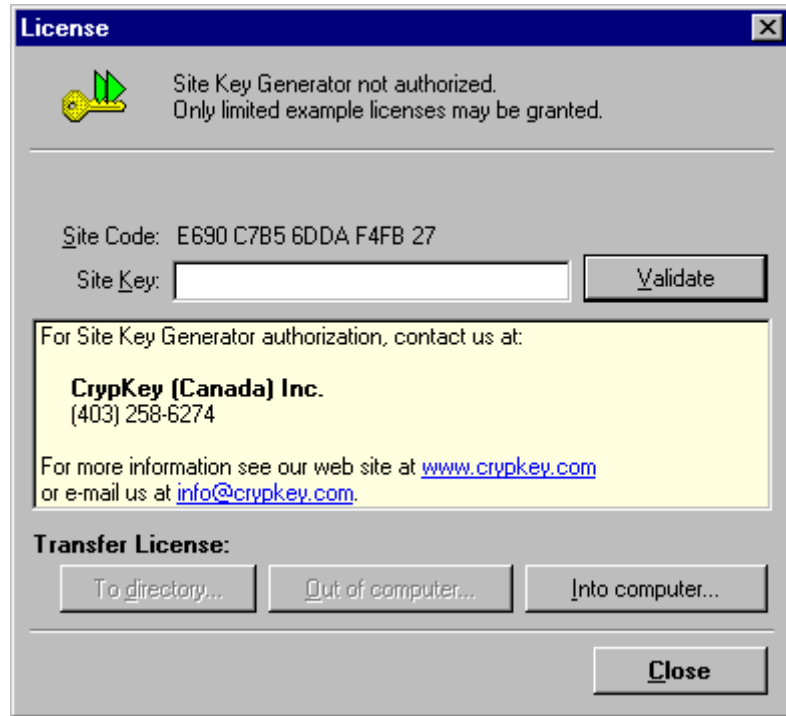
**Figure 69: Distributor's Unauthorized SKG
License Window with Site Code**

c) Provide you (via email or telephone) with the site code.

3. Type the site code from your distributor's slave Site Key Generator into the Site Code field in your master copy of the Site Key Generator.

4. If the word MUNCHKIN doesn't already appear in the Password field, then type it in.

5. Click the **Check** button in your Master SKG, which after a few seconds appears as follows:
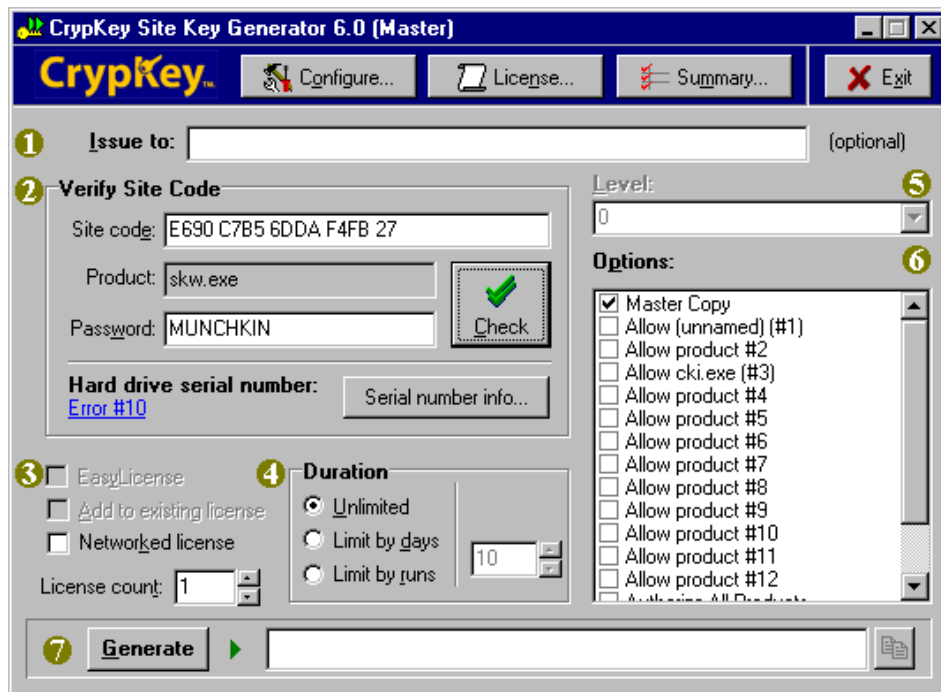
Figure 70: Master Site Key Generator with Distributor's Site Code

In the above window, the **Product** field should read `skw.exe`, which is the Site Key Generator executable file. Note that the **Master Copy** option is selected by default in the **Options** panel.

6. In the **Options** panel of the above window, select the products that you want to enable. You must enable at least one product, keeping in mind that the available options should already have been set up in the **Configure** tab page.

Note: when licensing a slave SKG, you should deselect the **Master Copy** option. If you leave it selected, you are authorizing a Master SKG, thereby allowing a distributor to create their own Site Key Generators with the capability of issuing licenses to distributors.

7. Click **Generate** to create the site key. Your Master Site Key Generator appears as follows (example selected options are shown):
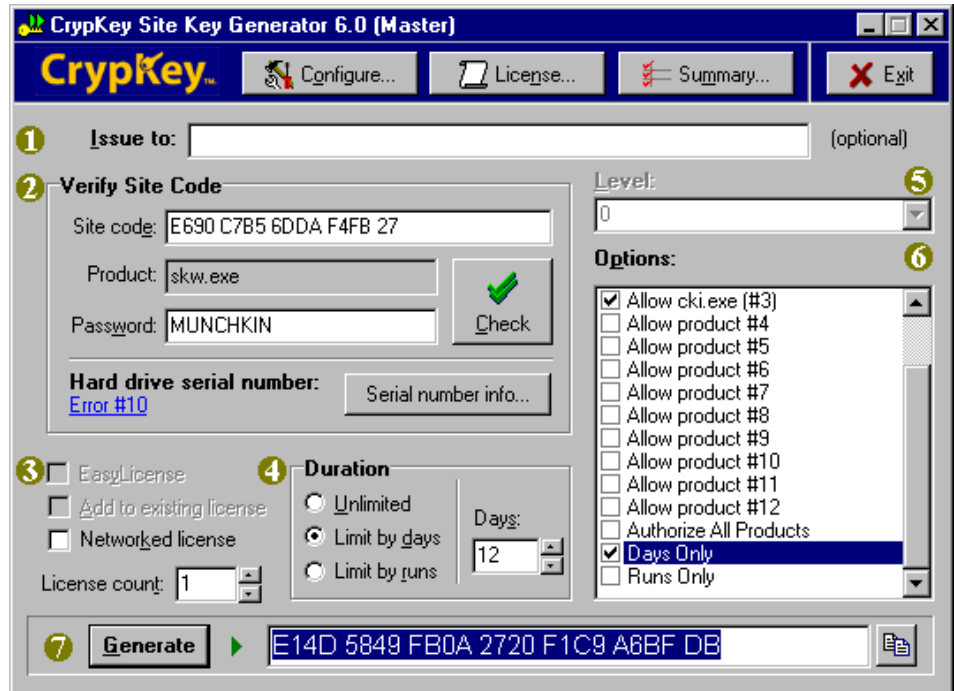
Figure 71: Master Site Key Generator with Slave Site Key and Selected Options

Note: the **Days Only** and **Runs Only** options, shown above, appear only when you authorize a slave Site Key Generator. They are used as special license restrictions for a slave SKG. When you enable **Runs Only**, and select the runs license, the slave Site Key Generator can only create runs licenses. In addition, the total number of runs the generator grants for a product is decremented from its own license count. Therefore, if a slave Site Key Generator is awarded a runs license with 1,000 runs, and the **Runs Only** option is enabled, the generator has 800 runs left after it has issued 200 runs to a product.

These rules apply in the same way to the **Days Only** option and days license.

8. Send the generated site key to your distributor.

9. Your distributor enters the site key into the License window of his or her Site Key Generator:
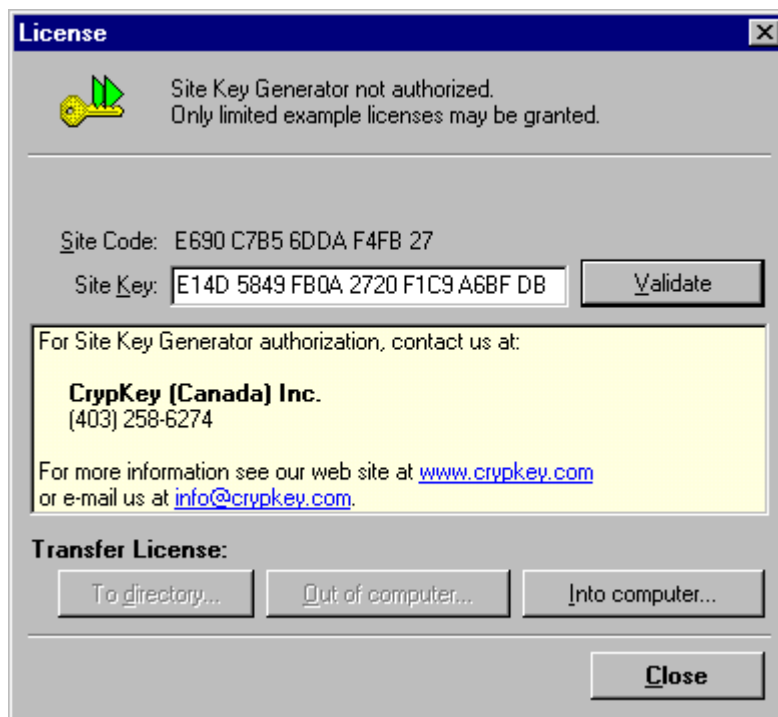
Figure 72: Site Key Generator License Authorization

10. Your distributor clicks the **Validate** button in the above window, resulting in authorization of the slave SKG as shown below:
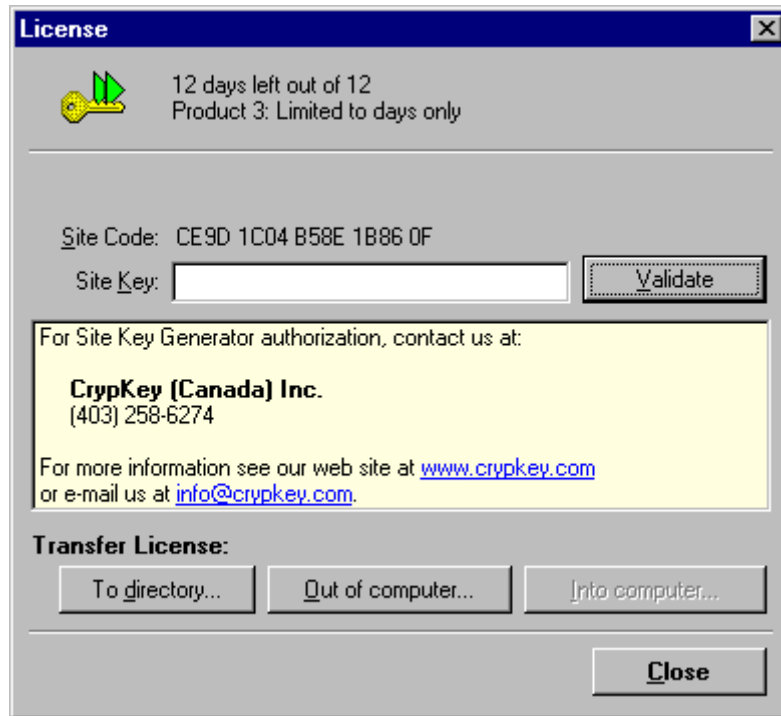
Figure 73: Slave SKG License Window – Authorized

Your distributor is now authorized to use the Site Key Generator to issue customer licenses for his or her products. Note that the license duration is the same as specified in the Master SKG (Figure 71).

You shouldn't need to contact your distributor again concerning issues of license validation, unless the distributor's hard drive crashes or they lose authorization.

Using CrypKey Instant

Learn how CrypKey Instant works by exploring the details of each program button, field, and check box.

F ollow the instructions outlined in this section to prove CrypKey Instant's value to your product. During your trial period, CrypKey Instant protects your product using the example keys, generating a wrapped .exe file of your product.

The action of protecting your files begins with the main CrypKey Instant window, shown below, which the system displays when you click the CrypKey Instant icon.
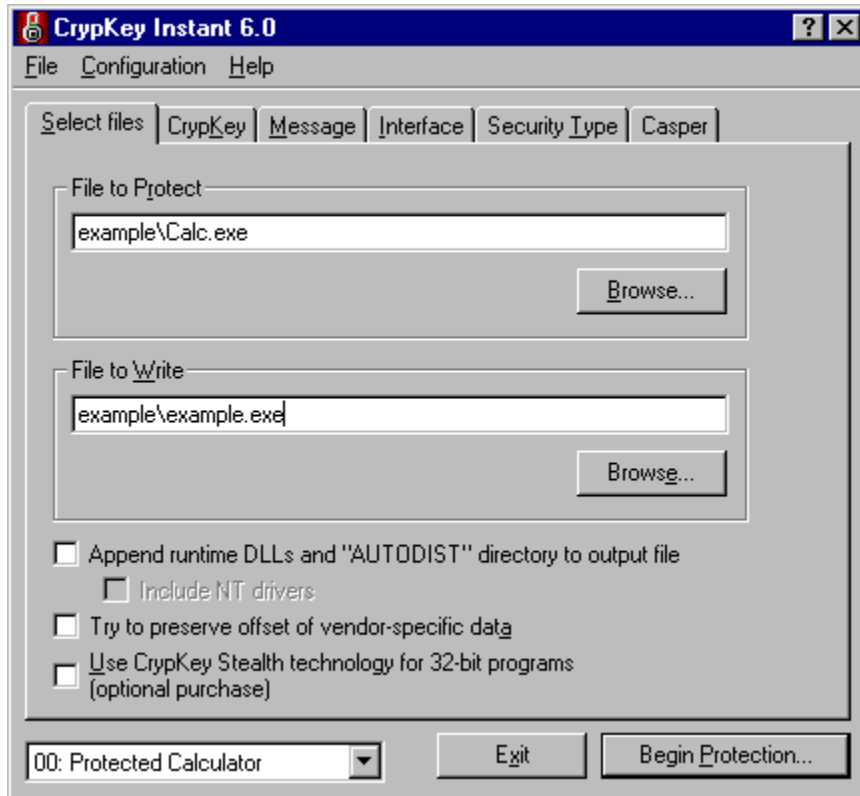
Figure 74: CrypKey Instant – Opening Window

Before describing the procedures for using CrypKey Instant, we'll discuss some of its essential features, including:

- Options and Levels

- Messages

- StealthPLUS™ anti-hacker technology

- CrypWrap, for encrypting both executable and non-executable files

For the procedures for protecting your application using CrypKey Instant, see Section 6.6 (p. 126).

6.1   Levels and Options

Level and option information relating to your product enables or disables features for your clients based on their purchased license type. Your computer platform dictates how these values are stored, as follows:

- 32-bit Windows applications: options are stored in the environment variable CKOPTIONS; levels are stored in the environment variable CKLEVEL.

- 16-bit Windows and DOS applications: options are appended to the command line as `/OPTIONS=PassedOptions`; levels are appended (one at a time) as `/LEVEL=PassedLevel.`

Refer to Section 5.1.4: Internal Handling of Levels and Options for details on implementing levels and options. Note that you control how your product's options and levels operate. Since 32 bits are available for this information, if for example you assigned 20 options at one option per bit, 12 bits would remain for the assignment of levels.

6.2   Messages

The message you enter in the **Message** tab of the CrypKey Instant main dialog box appears in your product's License Configuration dialog box. The message should explain how clients can contact you to obtain a site key, and may also include information on license options, license transfers, and other details you feel are necessary.

CrypKey Instant offers the following message types:

- **built-in text**: Text entered in the edit field of CrypKey Instant's Message tab (Use Default Message) is included in your product. No other files are necessary for this message, of which the maximum size is 1024 characters. A warning notifies you if your message length exceeds this limit.

- **file text (default)**: Text appearing in your product's License Configuration dialog box is derived from your specified text file at run time. Although the text body can exceed 1,024 characters, brevity is important to facilitate the user's search for information. Place text file messages in the same directory as your executable program and `cki_?.msg`, where ? is replaced by a single-character language identifier. For example, the English-language identifier is "a", and the corresponding filename would be `cki_a.msg.`

- **bitmap**: A 16-color bitmap is displayed in your product's License Configuration dialog box. The bitmap used depends on the language your clients select. Place bitmap file messages in the same directory as your executable program and `cki_?.bmp`, where ? is replaced by a single-character language identifier. For example, the English-language identifier is "a", and the corresponding filename would be `cki_a.bmp`.

Even if you choose a file or bitmap message type, you should include instructions in the built-in message field, which displays if errors arise when the file or bitmap is opened.

6.2.1   Message Format Codes

Message format codes (Format Code Help) control the text formatting displayed in the License Configuration dialog box at run time.

Table 4: Message Code Descriptions

Code	Description
\<regular>	Resets the font to the default (eight-point Arial)
\, \	Toggles bold on and off, respectively
\<I>, \</I>	Toggles italics on and off, respectively
\<u>, \</u>	Toggles underline on and off, respectively
\<font fontname>	Switches to the specified font
\<size fontsize>	Changes the font size
\<a webaddress>…\<?a>	Provides a link to a web page. The font is underlined and turns blue. When the text is clicked, the web browser opens to the specific web address

Following is an example of how source code appears, using the above format codes:

```
<font Times New Roman> <size 9> Regular text,
<b> bold text </b>, <I> italic text </I>,
<a http://www.CrypKey.com> link to CrypKey (Canada) Inc. web
page </a>
```

6.3   StealthPLUS^{TM}

An important complement to encrypted licensing is a methodology, embodied in StealthPLUS^{TM}, to protect your installations against hackers. If you have purchased the StealthPLUS^{TM} feature, you can activate it in the **Select Files** tab page of the CrypKey Instant main window (see Sec. 6.6.2).

Version 6.0 StealthPLUS^{TM} has evolved to the highest level of security yet. Although no one can guarantee that your program can't be hacked, we can guarantee that StealthPLUS^{TM} makes your program extremely tedious and painful to hack. Any version of your program that is hacked will not likely operate properly.

StealthPLUS^{TM} is a strong deterrent to reverse engineering and patching, helping to ensure that the security logic you put in your program stays in your program. In less than 60 seconds, StealthPLUS^{TM} automatically implements a battery of security measures into your program.

StealthPLUS^{TM} protects your application in two ways:

1. It compresses and encrypts the program. Your executable file is smaller after you have "stealthed" it. Since the code is encrypted, reverse engineering and debugging of the file becomes extremely difficult.

2. It guards against patching while your program is in memory. It is technically possible to debug or redirect program execution (patch) around the security code while it is in memory. StealthPLUS^{TM} detects debuggers and patches and immediately halts program execution.

StealthPLUS^{TM} also completely rewrites your program and runs it in memory in small pieces, minimizing the amount of code that must be exposed at any given time. This process provides an extremely strong level of protection.

Note: the Site Key Generator must be authorized for StealthPLUS^{TM} to run.

StealthPLUS^{TM} is also available as a standalone program to protect your CrypKey API-based programs.

Be aware of two potential constraints introduced by the use of StealthPLUS^{TM}:

- CrypKey uses StealthPLUS^{TM} on its DLLs that you include with your application. Since StealthPLUS^{TM} prevents debugging, you can not use a debugger on your application once CrypKey is applied to it, even if StealthPLUS^{TM} is not directly applied to it.

- Running your CrypKey Instant protected application inside an IDE (Integrated Development Environment), such as Visual Basic or Visual, may not work. There are two reasons for this:
    - StealthPLUS^{TM} may prevent it for security reasons.
    - The environment changes the operating directory and consequently CrypKey may not find the necessary CrypKey DLLs.

The workaround for these constraints is to compile and run the application directly.

6.3.1   StealthPLUS^{TM} File Auto-Distribution

StealthPLUS^{TM} has a very useful additional feature: it can pack all CrypKey distributable files, as well as all of your files, into your executable. StealthPLUS^{TM} can even install the CrypKey License Service upon first run for you!

See Sec. 6.6.3: Opening CrypKey Instant: Select Files tab page, for instructions on using StealthPLUS^{TM}.

The Auto Distribution feature can be used to ensure that:

- Your EXE has all of the files it needs to run – no matter where it is.
- Your EXE always uses the correct version of associated files.
- The NT Driver is guaranteed to be installed.
- Your EXE is self contained and easy to use.

6.4　　CrypWrap

The CrypKey Instant Encryption Wrapper, called **CrypWrap**, encrypts the file package that you send to your customer, and in addition simplifies the distribution of non-executable files. For example, you can encrypt databases or spreadsheets for mailing to your clients, who can, in turn, decrypt the wrapped file, using the encryption key that you provide. You can also encrypt an entire directory of files (not including subdirectories, which you would encrypt in separate CrypWrap operations).

When you select the Encryption Wrapper feature from the **Security Type** tab of the CrypKey Instant main window, you must enter an encryption key between 0 and 2^{32} (= 4294967296). This key is also the value that you enter into the **Level** field in the Site Key Generator **Configuration** tab page. This is a means of preventing hackers from decrypting the file — since the Site Key Generator processes the encryption key, the key is not stored in the encrypted file package, but rather is communicated to the customer's computer via the CrypKey license.

6.5　　Multilingual Support

Your CrypKey Instant protected product may be distributed in more than one language.

Your clients select the language in which they want your product displayed from those available in the drop down list. Language files are identified by a single letter code or language identifier; "a" is the language identifier for English. The default language is specified in the Interface tab of CrypKey Instant.

6.5.1　　User Language Selection

On start up, a CrypKey Instant protected product scans the current directory for language resource DLLs, compiling a list of those available and displaying the language names in the License Configuration dialog box. If English is the sole available language, the language menu is not displayed.

If your clients choose a language other than the default, the selection is stored in a file called cki.ini, located in the same directory as the protected product. This file is automatically created if it is required.

6.5.2   Selecting Languages at Run Time

Your protected product decides which language to use for interface components on start up.

1.   If a file called cki.ini resides in the current directory and contains a language identifier that has a valid resource DLL, that language is used.

2.   If a valid resource DLL exists for the default language (as listed in CrypKey Instant's Interface tab at the time of protection), that language is used.

If neither of the above is successful, English is used.

6.6   Protecting Your Application
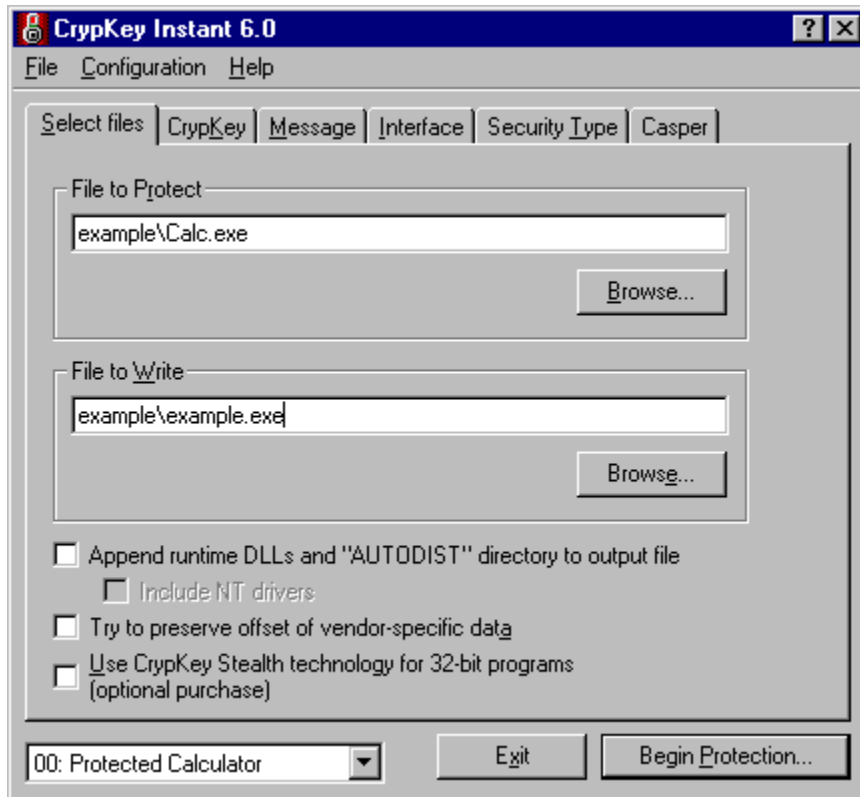
Figure 75: CrypKey Instant Main Window

The CrypKey Instant main window, shown above, contains a menu bar, six tab pages, a configuration description field, an **Exit** button, and a button labeled **Begin Protection**.

- The menu bar contains the general options **File**, **Configuration**, and **Help**, each of which has sub-options (for more details, see below — Sec. 6.6.1: CrypKey Instant – Main Menu Functions).

- The six CrypKey Instant tab pages are outlined in the following list:

  - **Select files** – identifies the application to be protected; applies StealthPLUS.
  - **CrypKey** – provides master and user keys; specifies level and options.
  - **Message** – creates the outgoing CrypKey protection message to your client.
  - **Interface** – enables certain commands; specifies language of communication.
  - **Security Type** – specifies the type of protection to be applied to the program.
  - **Casper** – manages the interface between CrypKey Instant and CASPER (an automated registration, authorization and payment system available from CrypKey (Canada) Inc.).

- At the bottom left of each tab page is a box containing a configuration description, i.e. the description of the particular arrangement of protection features that you are about to work with. For more information on this, see Sec. 6.6.2:Setting Up Multiple Configurations.

- Each tab page contains an **Exit** button and a **Begin Protection** button. The **Exit** button simply exits the program. The **Begin Protection** button applies to your application whatever protection features you have specified in the current session; you can click this button at any time. When the protection is applied, CrypKey Instant displays the following popup window:
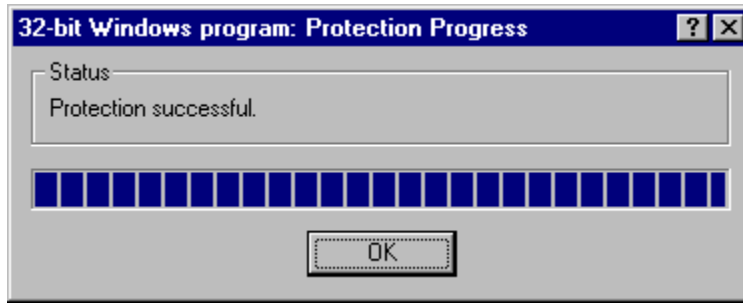
Figure 76: CrypKey Instant Protection Completed Popup

Normally, you use the **Begin Protection** button after you are satisfied with the entries made in all the tab pages that you have intended to use.

The sections that follow explain how the above capabilities are used to apply CrypKey Instant protection to your software products.

6.6.1   CrypKey Instant – Main Menu Functions

The menu bar at the top of the main window contains the following options, shown below with their sub-options.

- **File**

  - **Begin Protection** – same function as performed by the **Begin Protection** button at the lower right corner of the window

  - **Exit** – exit the CrypKey Instant program

- **Configuration** (for details, see Sec. 6.6.2, below)

  - **Reset Configuration** – return to the last configuration displayed

  - **Save Configuration** – save the current configuration

  - **Save Configuration As…** – save the current configuration as that of a new product

- **Help**

    - **Help Topics –** online help

    - **About CrypKey Instant… --** description of software release

6.6.2   Setting Up Multiple Configurations

In CrypKey Instant, you can set up numerous protection arrangements, with each arrangement combining various features in different ways. Each arrangement is called a *configuration*. You can set up a different configuration for each of your products and/or customer types. This can be particularly useful if you are managing a large number of products, and/or have several categories of customers.

The protection features that can vary from configuration to configuration include:

- the method by which options and levels are applied to your product

- the message that comes up when your application is accessed

- the ability to transfer product licenses between directories or between computers

- whether or not the product is encrypted

- whether or not CASPER is enabled

CrypKey Instant's configuration management functions allow you to store up to 100 configurations. If you have multiple products that you are protecting with CrypKey Instant, you can store each product's set of protection features as a different configuration. You can also set up more than one configuration per product in order to accommodate other requirements, such as customer categories. With this capability, when you update a given product and need to re-apply the protection features, you don't need to enter the features all over again.

Note: due to a limitation of Windows 9x/ME handling of INI files, CrypKey Instant's INI file where configurations are stored can not be larger than 64K. If you attempt to save additional configurations when the INI file is this large, the additions are lost. If you encounter this problem, save your options over an older configuration. Windows NT/2000/XP does not have this limitation.

Recording and Accessing Configurations

The configuration that you are currently working with is displayed in the listbox in the lower left-hand corner of each tab page. CrypKey pre-assigns the numbers from 00 to 99

to the full set of possible configurations, and reserves a place for each, although these placeholder configurations are initially blank. The text description (e.g., Protected Calculator as shown in Figure 75 above) references text entered into the **Title** field of the **Interface** tab page (see Sec. 6.6.6). By default, when you open CrypKey Instant, the configuration that you are working with is the first in the listbox, i.e. the one with the assigned number 00.

When you click the arrow in the configuration description listbox, the system displays a pop-down window showing the first seven entries in the list of current configurations, as illustrated below:
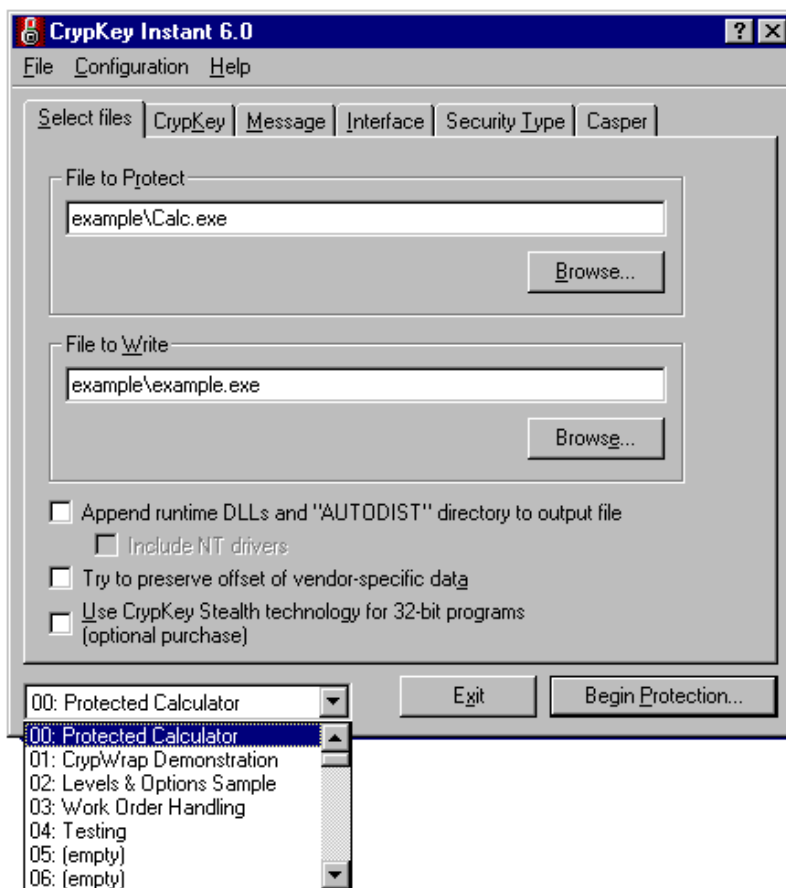
Figure 77: Configurations Listing

You can scroll through the complete listing of 100 configurations in the above listbox.

If you click to select an entry from the listbox, any updates that you make (using the **Save Configuration** button – see below) in the CrypKey Instant tab pages are applied to the selected configuration.

As shown in the listbox, blank configurations are identified by the title "{empty}". However, if you have previously selected an entry and saved settings for that configuration without specifying a title, the title shown here is "{untitled}".

Using the Configuration Buttons

As you work with the tab pages, you can at any time, from any tab page, save your updates or reset the values using the **Save Configuration**, **Save Configuration As…** , or **Reset Configuration** buttons.

- The **Save Configuration** button simply saves the settings from all tab pages, within the configuration currently selected. Once saved, there is no global "undo" command – to return the settings to their original values, you must edit them individually.

- The **Save Configuration As…** button saves the settings from all tab pages into whichever configuration you select. While using any of the tab pages, click an entry in the configurations listing (see Figure 77), then click the **Save Configuration As…** button. The system displays the Save Configuration popup, as shown below:
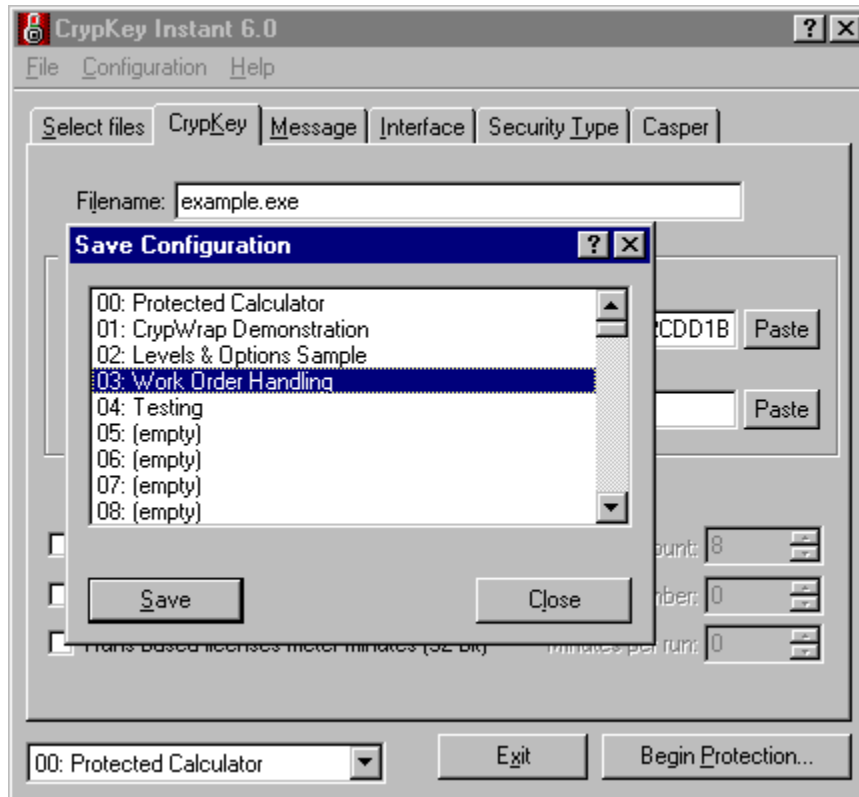
Figure 78: Save Configuration Popup Window

In the above window, click **Save** to save the configuration under the selected name, or click **Close** to exit the popup window.

- The **Reset Configuration** button resets any unsaved settings for the currently selected configuration, to the settings that were previously saved for that configuration.

General Note: if you make changes to settings for a given configuration, and then select another configuration without first saving or resetting, the system displays a popup message such as the following:
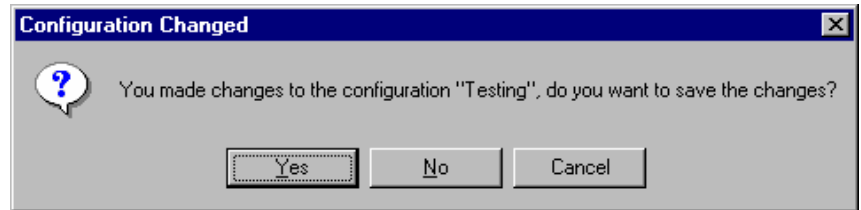
Figure 79: Configuration Change Confirmation Popup Window

In the above popup window, you can:

- click **Yes** to save the changes and continue to the next configuration selected

- click **No** to reject the changes and continue to the next configuration selected

- click **Cancel** to return to the configuration as it was before you selected another configuration

6.6.3   Opening CrypKey Instant: Select Files tab page

Procedures

1. Using the **Start** menu, display the CrypKey Instant program group, shown below:
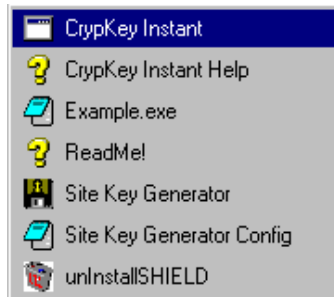
Figure 80: CrypKey Instant Program Group

2. In the above program group, click the **CrypKey Instant** icon. The system displays the following splash screen:

Figure 81: CrypKey Instant Splash Screen

3. In response to the splash screen, you can either do nothing, or click **Enter** within a few seconds of the appearance of the above popup. The results of both of these choices are described below:

- If you do nothing, the above popup disappears and is replaced as shown below by the main CrypKey Instant 6.0 window, ready for you to use:
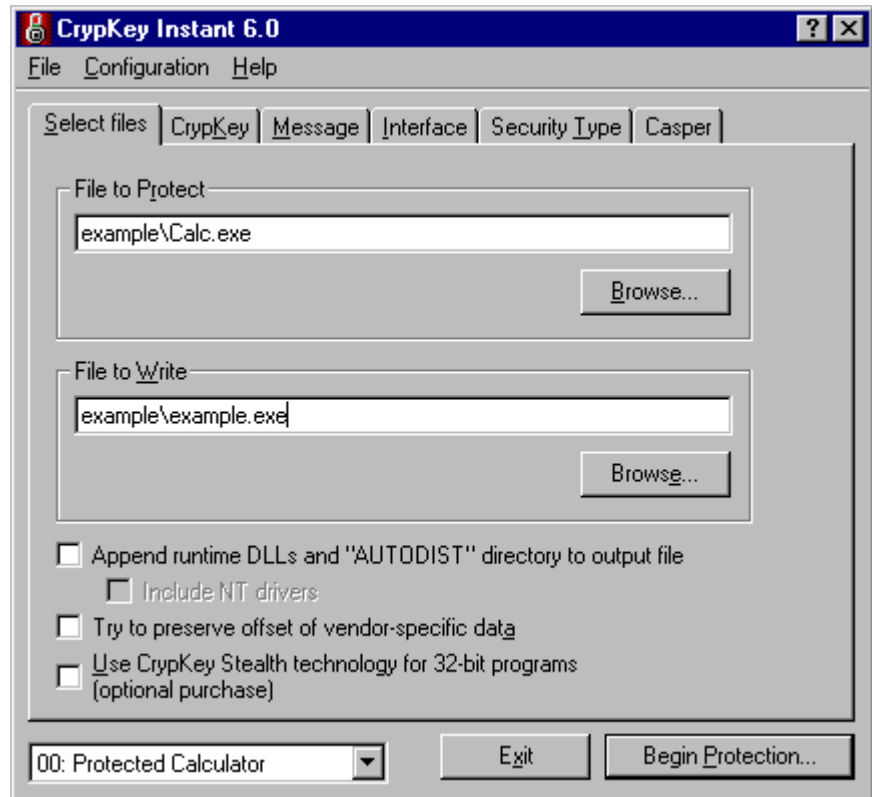
Figure 82: CrypKey Instant Main Window – Select Files Tab Page

To continue with the above window, proceed to **Step 4** below.

- If you click **Enter**, in response to the splash screen, the following window appears:
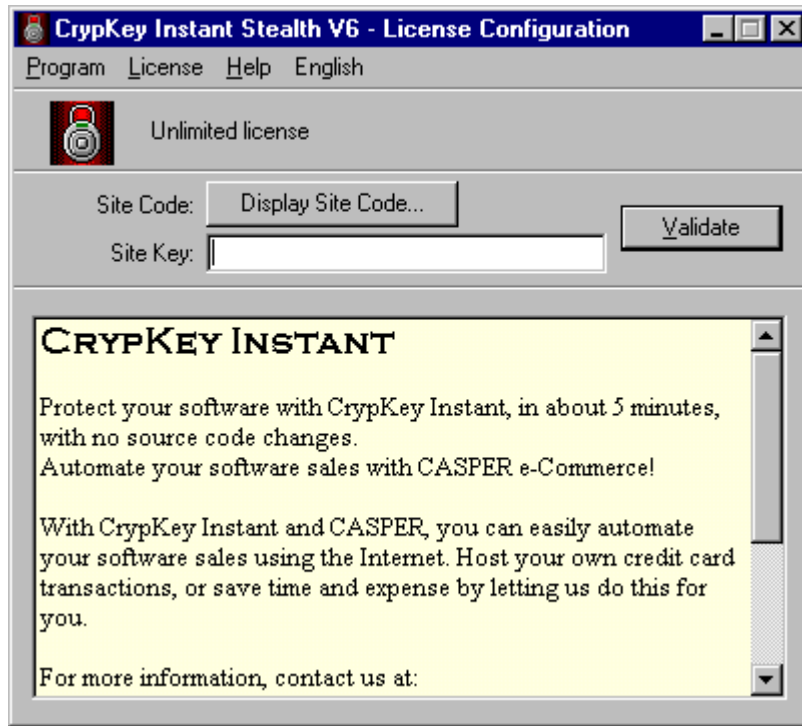
Figure 83: License Configuration Window (Authorized)

The above window gives you the ability to transfer your CrypKey Instant license between computers, or to "kill" the license. The window provides your with the following menu options:

- **Program**

    - **Close** — close the program

    - **Resume program execution** — return to the regular CrypKey Instant program operation, i.e. display the **Select Files** tab page

- **License**

    - **Transfer to directory** — see Chapter 8: Moving Protected Products.

    - **Transfer in from another computer** — see Chapter 8: Moving Protected Products.

    - **Transfer out to another computer** — see Chapter 8: Moving Protected Products.

    - **Kill license** — cancel the license. The **Kill license** function generates a "kill" code, which you can send to CrypKey (Canada) Inc. as verification after deleting a license.

- **Help** — online help

- **English** — selection of language (English or French) used for the application interface.

4. In the **Select Files** tab page (Figure 82), use the **Browse** button to enter file names into the **File to Protect** and **File to Write** fields. These fields are defined as follows:

- **File to Protect**: the file you want to protect (CrypKey Instant copies this file and wraps the encryption around it). If you are using the CrypWrap feature (see Sec. 6.6.7: Security Type tab page), you can type in a directory name (since the **Browse** button does not show directories).

    By default, CrypWrap encrypts all the included files, but not subdirectories; you must specify these individually. However, you can select the Recurse subdirectories checkbox in the Security Type tab page, in order to have CrypWrap include all directories and subdirectories.

    Note: if one of the files in the CrypWrap-processed directory is named setup.exe, it is automatically run when extraction is complete at the customer's computer.

- **File to Write**: the file that CrypKey Instant creates and around which it wraps its encryption.

The **File To Protect** file name should differ from the **File To Write** file name (you can rename the latter after protecting it with CrypKey Instant). If the file names are identical, you must point them to different directories.

5. If you want StealthPLUS™ (if you have purchased it) to cause runtime files to be added to your program at protection time, click the **Append runtime DLLs …** checkbox. This activates StealthPLUS™, causing required runtime DLLs and any additional files such as bitmaps, messages, and language modules to be compressed and added to the protected program.

The system also activates the **Include NT drivers** checkbox. If you are targeting your program to Windows NT, click this checkbox to cause the NT drivers to be included. You may prefer not to include NT drivers so that customers not using NT are not inconvenienced by the additional size of the program.

Notes:

- The **Append runtime DLLs …** option is available only if you have purchased StealthPLUS™.

- CrypWrap programs require all the CrypKey Instant runtime files to function. This may pose problems if you want customers to download a single CrypWrapped file. To deal with this issue, you can use the **Append runtime DLLs …** option to have CrypWrap include the runtime files, plus NT drivers if needed, in the archive and extract them as they are needed.

  Runtime DLLs are always extracted into the same directory as the CrypWrap archive. Therefore, if your application is running from a read-only media such as CD-ROM, you can't use the CrypWrap auto-extraction feature. Instead, you must include the runtime files separately on the CD-ROM. This limitation does not apply to Windows NT drivers, which are extracted into the system temporary directory.

6. Check the **Try To Preserve Offset Vendor-Specific Data** box to notify CrypKey Instant that you want to manage vendor-specific data in your program differently. Checking this box may fix errors that your program displays after it gains control from CrypKey. Some programs, especially multimedia presentation programs, append data to the end of the executable file. If your program displays a runtime error once it gains control from CrypKey, checking this box may solve the problem.

7. For 32-bit programs, check the **Use CrypKey Stealth…** checkbox. This ensures that CrypKey Instant uses its enhanced StealthPLUS^{TM} protection procedure, which is more difficult to hack than the standard protection.

> *Note:* StealthPLUS^{TM} may not work on all programs, and requires an additional license to activate. To utilize this feature on a trial basis, send us your site code from CrypKey Instant and we authorize the trial period. For information about the StealthPLUS^{TM} functionality, see Sec. 6.3.

6.6.4   CrypKey tab page

Procedures (continued)

8. Click the **CrypKey** tab to display the **CrypKey** tab page:
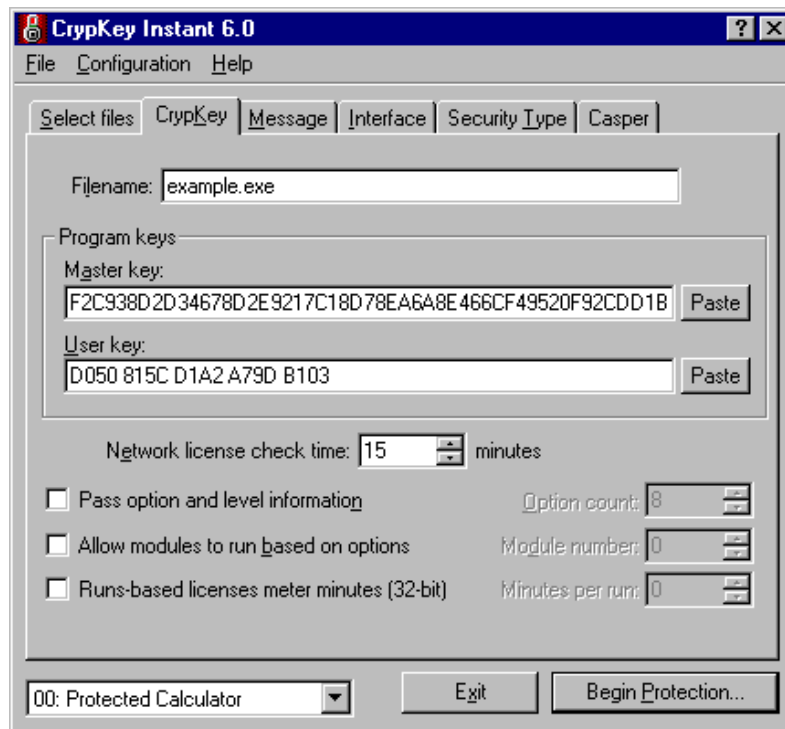
Figure 84: CrypKey Tab Page

9.   In the above window, enter the filename of your executable file (which, during your trial period, is always example.exe). This file is considered your license file and is the name you provide to CrypKey Instant when requesting your developer keys.

> *Note:* this filename must meet certain requirements if you are storing your license files in a different location than the protected program. For details, see Sec. 3.6.4: Storing License Files and the Protected Program in Separate Locations.

10. Enter your master key (using the **Paste** button described below) and user key into the **Master key** and **User key** fields. Both keys are provided by CrypKey (Canada) Inc. when you request your developer keys (during your trial period, use the example master and user keys — see Sec. 1.6.2: Trial Keys and License Keys).

The master key for Win32 applications is much longer than the user key, and it's impractical to enter it manually. That's why there is a **Paste** button beside the field in the above window. When you receive your master key (typically by email), do the following:

- within your email program, select the whole key (including any new lines, line wrapping or spaces)

- press the **Paste** button

  If there is problem with the paste operation or key length, the system displays a message to that effect.

You can use the same method for entering your user key.

> *Note:* the procedure for obtaining the Master Key is different from the standard if you are storing your license files in a different location than the protected program. For details, see Sec. 3.6.4: Storing License Files and the Protected Program in Separate Locations.

11. Click the **Pass Option and Level Information** checkbox and, if applicable, the **Allow modules to run based on options** checkbox, in order to use CrypKey Instant's options and levels features. These are the two mechanisms by which CrypKey Instant applies protection features to your application.

- Click the **Pass Option and Level Information** checkbox to activate the **Option Count** box, where you can use arrow buttons to enter the total combined number of desired options and one level. CrypKey Instant selects and applies the specified number of options, starting from the first value set up in the Site Key **Configure** tab page. The number specified for **Option Count** can be any value up to the full number of options specified in the Site Key **Configure** tab page.

   When your protected application initializes, it obtains the option and level information from the license and puts them into the CKLEVEL and CKOPTION environment variables. In C/C++ you can extract this information from the environment variables using the **getenv()** function. In Visual Basic, this requires that you code your application to use the Windows API function **ExpandEnviromentStrings()** to extract the option and level information from the environment variables. In C/C++, the options or levels can also be obtained using the Crypkey SDK **GetOption()** or **GetLevel()** functions.

   > *Note:* if you are using the CrypWrap feature (see Sec. 6.6.7: Security Type tab page), the **Option Count** value must be set to 0 (zero).

- If applicable, click the **Allow modules to run based on options** checkbox to activate the **Module Number** box, where you can use arrow buttons to enter the applicable module number. The module number must correspond to an option number specified in the Site Key Generator **Configure** tab page and activated in the Site Key Generator main window. You can view the names and numbers of currently identified modules in the listbox in the lower left corner of the window.

   This function allows you to to have multiple programs sharing the same license (i.e. for the same executable filename specified above) while maintaining the ability to control authorization for each one individually. On the other hand, when using the function you can assign only one option per module.

   With the **Allow modules to run based on options** function, you set up your modules (executables and DLLs) so that each runs only if a specified option is enabled. You must protect your executables and/or DLLs one by one, assigning each of them a unique module number. The module number corresponds to the option. For example, if you are protecting your module using module number 3, then you must previously have selected option 3 in the Site Key **Configure** tab page, and activated it in the main Site Key window, in order to successfully license the module. Otherwise, you receive an error message when trying to open your licensed application.

   Note that whenever you change the license, you are affecting all of the modules

sharing that license. Note also that you can later use the Site Key Generator's **Add to existing license** option to upgrade the license to include other modules.

12. Optionally, click the **Runs-based licenses meter minutes (32-bit)** checkbox. This activates the **Minutes per run** box, where you can use arrow buttons to specify in minutes the length of a run (note that this applies only to "runs" licenses, not "days" licenses). The allowable number of runs is decremented by one every time the specified number of minutes, or portion thereof, elapses during operation of the protected program. For example, if one run is defined as 60 minutes in length, running the application and exiting within 60 minutes uses up one run, whereas running the application for anywhere between 60 and 120 minutes uses up two runs.

6.6.5 Message tab page

Procedures (continued)

13. Click the **Message** tab to display the **Message** tab page:
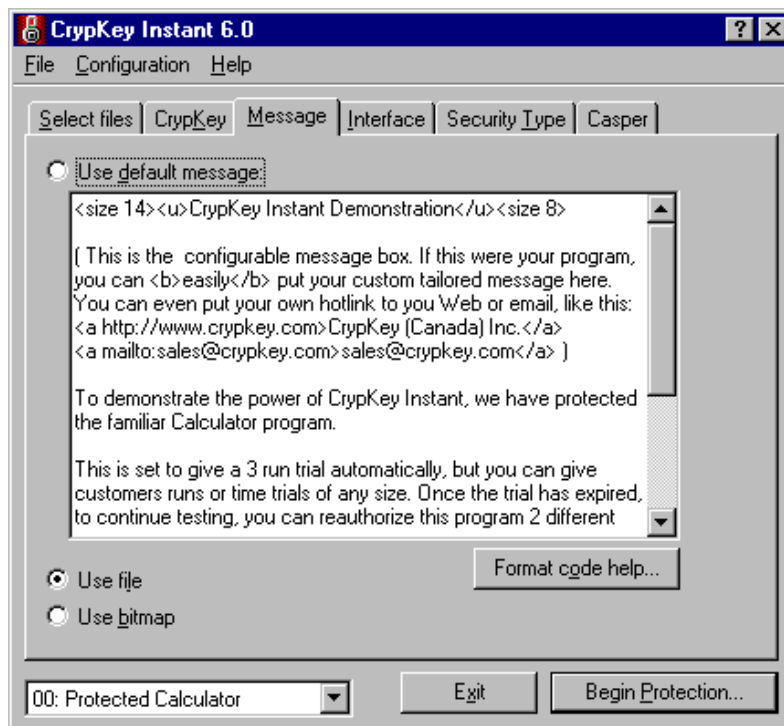
Figure 85: Message Tab Page

14. In the above window, select the type of message that you want your clients to see when the system displays the window telling them that they are unauthorized to use your application. The three available radio buttons produce the following results:

- **Use Default Message**: the protected program displays the text that you enter into the panel in the above window. This text is included in the protected program; no other files are needed. The displayed text is limited to 1024 characters — you are notified if the message is too long.

  Click the **Format Code Help** button for instructions on formatting your message (e.g. bolding, underlining, creating Web links). See Sec. 6.2.1: Message Format Codes, for more information on this.

- **Use File**: the protected program extracts the message from a text file at runtime, which you have placed in the same directory as the executable program. The file must be named `cki_?.msg`, where "?" is a single-letter identifier of the language used. The identifier for the English language is "a"; the filename for an English-language message would be `cki_a.msg`. The same format codes used in the default message can be used in the text file. The text file can exceed 1024 characters in length (although it should be kept brief for readability).

- **Use Bitmap**: the protected program displays a bitmap image in the License Configuration dialog box at runtime. The image is taken from a file that you have placed in the same directory as the executable program. The bitmap image must have the dimensions 374 x 190 pixels. The file must be named `cki_?.bmp`, where "?" is a single-letter identifier of the language used. The identifier for the English language is "a"; the filename for an English-language bitmap would be `cki_a.bmp`.

6.6.6 Interface tab page

Procedures (continued)

15. Click the **Interface** tab to display the **Interface** tab page:
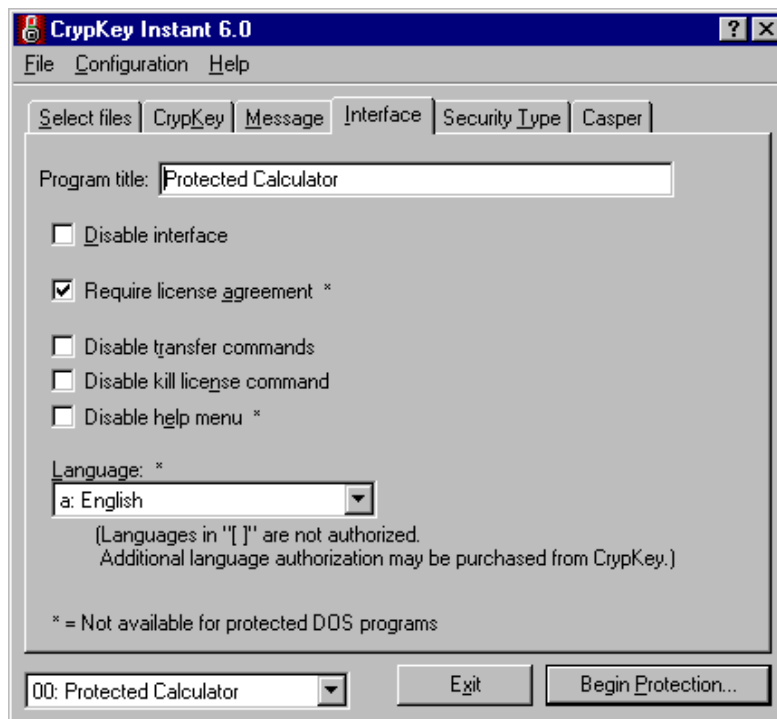
Figure 86: Interface Tab Page

16. In the above window, enter your program title, which is the name of the product you want to protect. When you click the **Save Configuration** or **Save As Configuration…** button, the specified title appears in the configuration description field at the lower left of the display. For more information on the Configuration buttons, see Sec. 6.6.2: Setting Up Multiple Configurations.

The optional toggle boxes beneath the **Program Title** field accomplish the following:

- **Disable Interface**: disable a clients' ability to view the CrypKey Instant interface (for example, if you only want to visibly protect one application, e.g. a main program with some utility programs) among several who are sharing a license. Protection for these applications is only apparent if no license exists, whereupon CrypKey Instant displays an error.

- **Require License Agreement**: require clients to read and accept your license agreement when they click **Display Site Code** (see Sec. 4.1: Producing a Site Code). At runtime, the protected program extracts and displays the agreement from a file named `cklicens.hlp`, which you have placed in the same directory as the executable program.

    Note: the recommended method of creating this file is as follows:

    - write the license agreement using Word, then save it as an RTF file

    - using a help-file compiler, compile the RTF file into the `cklicens.hlp` file

    You can download help compilers from the Internet, or if you have Visual Studio, you can find one called HCW.EXE in:

    ```
    C:\PROGRAM FILES\MISCROSOFTVISUALSTUDIO\COMMON\TOOLS
    ```

- **Disable Transfer Commands**: disable clients' ability to transfer your product license between PCs

- **Disable Kill License Command**: disable the **Kill License** command, which allows clients to kill their license. Disabling the command reduces the risk of accidental deletion of licenses.

- **Disable Help Menu**: disable clients' ability to access a help menu

- **Languages**: use the drop down list to indicate the languages supported by CrypKey Instant. These include English (the default), Dutch, French, German,

Hebrew, Italian, Japanese, Polish, Portuguese, Spanish, Swedish, and Turkish. You can select from the drop down list to enable the language in which you want your product distributed. Since the list is continually expanding, please contact us if your language of choice is not shown.

6.6.7   Security Type tab page

Procedures (continued)

17. Click the **Security Type** tab to display the **Security Type** tab page:
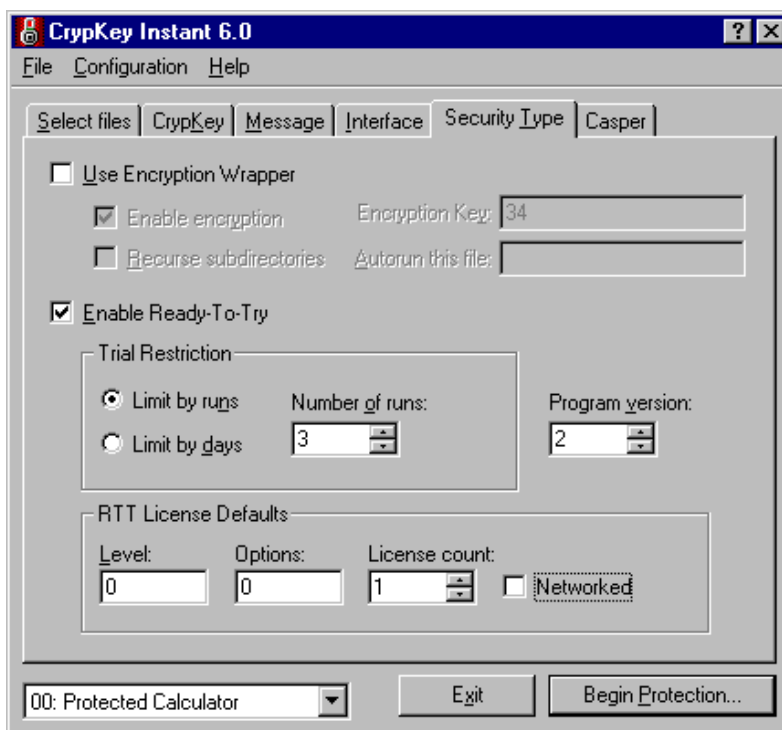

Figure 87: Security Type Tab Page

18. In the above window, click the **Use Encryption Wrapper** checkbox if you want to generate an encrypted, self-extracting file. Clicking this option enables the four sub-options **Enable Encryption**, **Encryption Key**, **Recurse subdirectories**, and **Autorun this file**.

This option is the CrypWrap feature of CrypKey Instant, used to wrap and encrypt both executable and data files. A valid license causes the original file to be extracted to the current directory on the user's hard drive.

> *Note:* when using the CrypWrap feature, you must set the number of options for the Site Key Generator to 0 (zero). This is done in the **Option count** box of the CrypKey tab page (see Sec. 6.6.4).

The CrypWrap sub-options are as follows:

- **Enable Encryption**: causes the wrapping process to include encryption. You may choose not to enable encryption — for example, you may need the license option and level specifications for another purpose. The wrapped files are still relatively well protected, i.e. not easily extracted individually by a hacker.

- **Encryption Key**: an integer greater than 0 and less than 2^{32} (i.e., less than 4294967296). If encryption is enabled, the transmitted encryption key must be correct in order for the wrapped files to be correctly extracted. If the key is incorrect, the extracted files are corrupted.

  To prevent hackers from unencrypting the file, the encryption key is not stored in the protected program; instead, it is communicated to the extractor via the CrypKey license. The same key must therefore also be entered into the **Level** field of the Site Key Generator (see Sec. 5.3.1: Generating Site Keys).

- **Recurse subdirectories**: the directory structure is recreated when unencryption occurs.

  By default, CrypWrap encrypts files specified in the Select Files tab page, but not subdirectories. You must specify these individually. However, if you select the **Recurse subdirectories** checkbox in the Security Type tab page, CrypWrap includes all directories and subdirectories in the encryption process.

- **Autorun this file**: causes the protected file, if it is an executable, to be automatically run when extraction is complete.

19. Check **Enable Ready-To-Try** to distribute your product with a built-in trial period. When clients initially execute your product, a trial license appears, identical to what you see in our trial version of CrypKey Instant. As part of its protective function, ready-to-try prevents your clients from receiving more than one trial period. They cannot create a second trial license, since CrypKey Instant places a non-removable signature on their hard drive.

- Limit your clients' trial period by runs or days, using the arrow keys to enter a number. The ready-to-try feature allows clients to use your product for a restricted time before deciding to purchase.

  Note: If you enable the ready-to-try feature for zero runs or days, you are in effect issuing the user an unlimited trial license. If you do not want the user to have a trial period, ensure that you do not have this feature enabled.

- Complete the **RTT License Defaults** fields, where you specify the license defaults that you want to use during your ready-to-try period. They include:

  - **Level** – the program level (defined in the Site Key Generator **Configure** tab page) assigned to the customer for the trial period.

  - **Options** – a decimal number representing the program option numbers (defined in the Site Key Generator **Configure** tab page) assigned to the customer for the trial period. For example, if Options 1, 2, and 5 are on, the specified number would be 19, which can be converted to the binary number 10011 representing an on/off sequence of options. For more details on this numbering system, see Sec. 5.1.4: Internal Handling of Levels and Options.

  - **License count** – In the case of a network license: the number of floating licenses. In the case of a non-network license: the number of fixed licenses. This parameter is used mainly for network licenses.

  - **Networked** – Used to create an RTT license that runs across a network.

20. Program Version: use the arrow keys to enter your product's number of versions (to a maximum of 32). This allows you to distribute new versions of your product with accompanying new trial periods, ensuring that clients who have already purchased your product can also experiment with newly released features. Because CrypKey Instant only allows one ready-to-try feature per computer , you must increase your product's version number to enable a second trial period.

6.6.8   CASPER Tab Page

CASPER (CrypKey Automated Software Purchase and Electronic Registration) enables you to automatically license your product over the Internet without the need for human involvement. Automatic electronic purchasing is cost-effective for you and convenient for your customers. CrypKey Instant provides the ability to interface your protected program with the CASPER electronic purchase wizard.

If CASPER is enabled in the **Casper** tab page, an **Electronic Purchase** button appears in the License Configuration dialog box of the protected program. Pressing this button enables the CASPER electronic purchase wizard, which steps users through the process of authorizing their program on the Internet. Note that to have your customers register your product using Casper, you must also ship the CASPER DLL with your protected program. This DLL works under 32-bit Windows only.

Procedures (continued)

21. Click the **Casper** tab to display the **Casper** tab page:
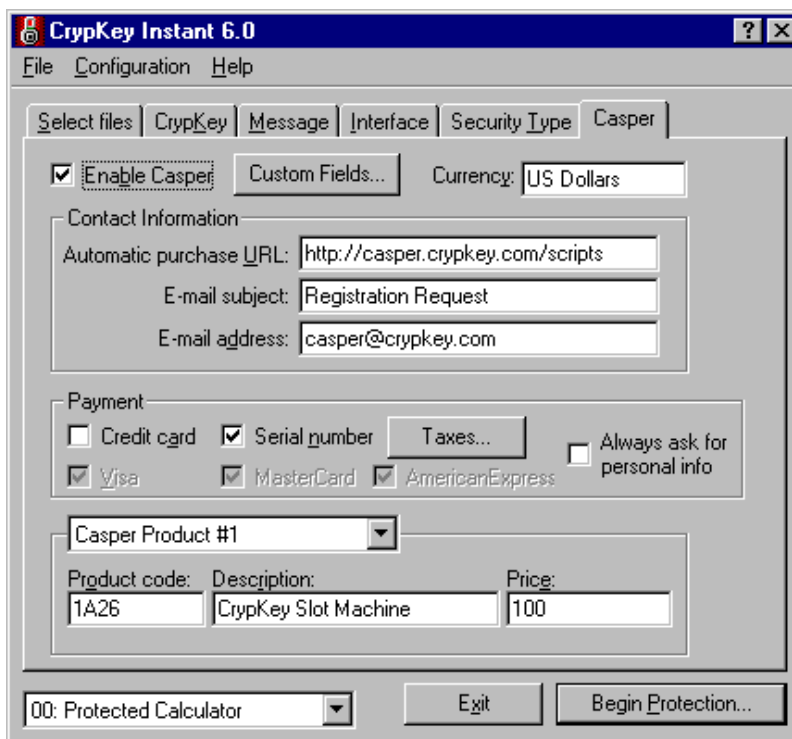
Figure 88: CASPER Tab Page

22. In the above window, click the **Enable CASPER** checkbox as shown if you are using CrypKey Instant and our CASPER software together. The CASPER software uses the information supplied in the **Casper** tab page.

> *Note:* this feature is applicable only if your system includes the CASPER functionality. For more information on the CASPER software, refer to the CASPER user manual.

23. If you are setting up custom input fields in the CASPER Wizard, click the **Custom Fields** button. CrypKey Instant displays the following window:
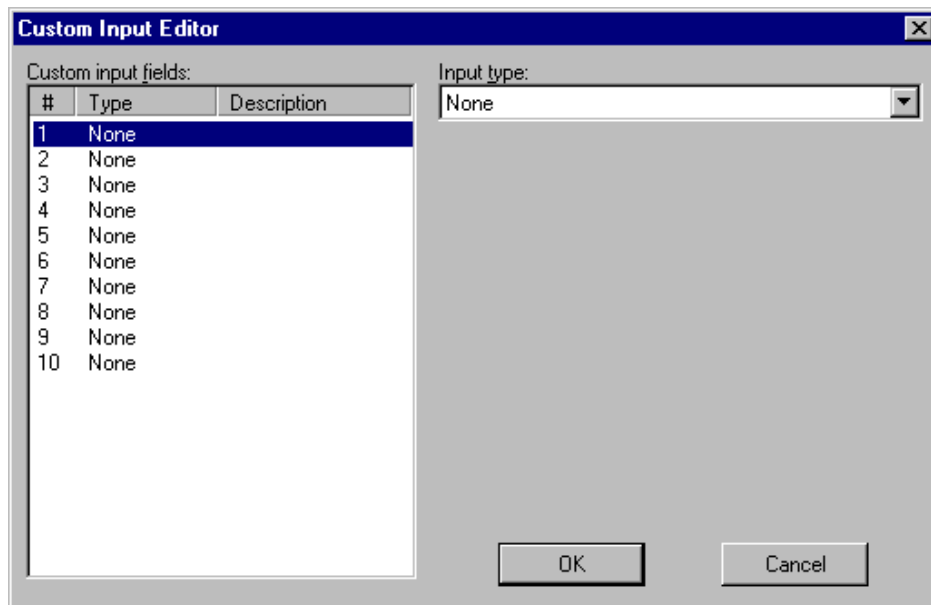
Figure 89: CASPER Custom Input Editor Window

In the above window, you can set up as many as 10 custom fields appear in the CASPER Wizard. Each field that you set up specifies a type of information that the CASPER Wizard requests from your customer, beyond the standard identity information (name, address, etc.) that CASPER prompts for when performing credit card purchases.

> *Note:* CASPER does not prompt for standard identity information if the customer is paying by serial number, unless the **Always ask for personal info** box (see below) is checked.

Configuring a CASPER custom input field

a) In the above **Custom Input Editor** dialog box, click a field number in the list.

b) Click the arrow beside the **Input type** box to display a drop down list containing the words **None** and **Custom**. **None** is the default value, meaning that no custom field is displayed.

c) Select **Custom**.

The Custom Input Editor window appears as follows:
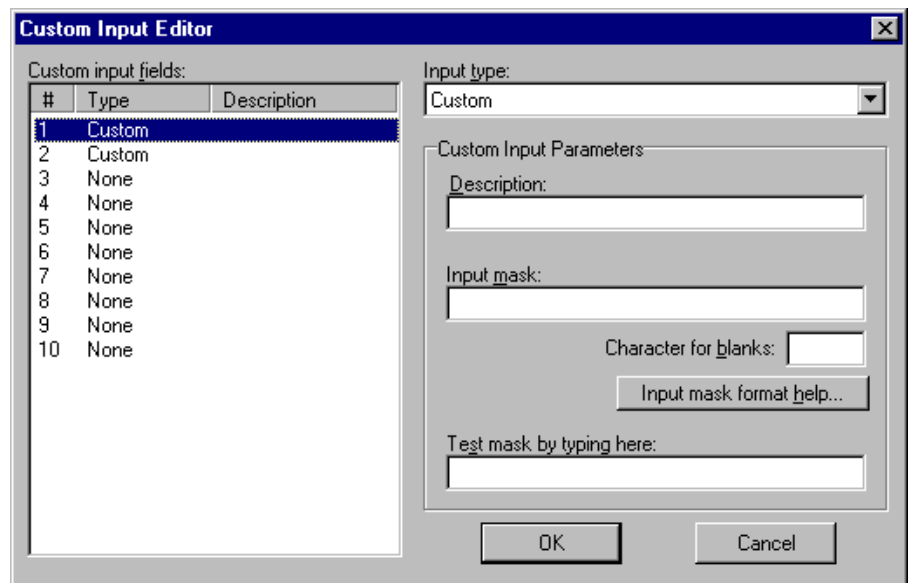
Figure 90: CASPER Custom Field Setup Window

d) Type a description into the **Description** field. What you type here appears as the name of the field in the CASPER Wizard, and should therefore clearly indicate the information that the customer is to provide.

e) Optionally, create an input mask using the **Input mask** field. An input mask consists of a string of characters that specify, character-by-character, the format of the data to be entered by the customer. If you don't specify an input mask, the customer can type anything into the custom field as it appears in the CASPER Wizard. Masks are useful for numbers or codes that have a specific format, such

as a phone number or a serial number. The table below describes the format codes for input masks.

Note: each input-mask code occupies a specific position in the field, and defines the type of character that must be entered at that position. The codes are case-sensitive.

Table 5: CASPER Input Mask Format Codes

Code	Meaning
L	requires an alphabetic character
l	(lower-case L) permits an alphabetic character but doesn't require it
A	requires an alphabetic or numeric character
a	permits an alphabetic or numeric character but doesn't require it
C	requires any character
c	permits any character but doesn't require it
0	requires a numeric character
9	permits a numeric character but doesn't require it
#	permits a number or a plus or minus sign but doesn't require it
/	displays a month, day, or year separator. The actual separator character displayed is taken from the user's control panel preferences.
- , ( ) *etc.*	All other characters, such as hyphens and parentheses, are displayed in the CASPER Wizard edit field as literal characters that the user can't change. For example, a telephone number mask could be "(000) 000-0000", and a serial number could be something like "LLLL-0000-00".

f)   In the **Character for blanks** field, enter the character, such as "_" or a space, that denotes a blank character position to be filled in by the customer. If you use "_", the mask created as

```
(000)000-0000
```

appears in the CASPER Wizard input field as

(____)____-_____

As the customer types values into the field, the blank characters are replaced with the input.

g)   In the **Test mask by typing here** field, enter some sample input to see how your mask performs. This field accepts input in the same way as your custom field when displayed by the CASPER Wizard. You should always test your masks to make sure they are appropriate for the information desired.

24. In the **Currency** box, specify the currency that you use for purchases (for example, "US Dollars"). What you enter here is displayed in the Casper wizard when money values are used.
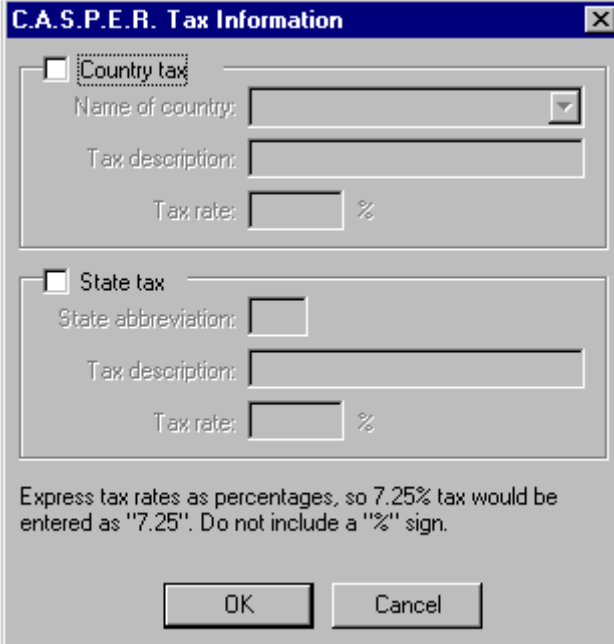
25. Fill in the **Contact Information** fields as needed:

- **Automatic purchase URL**: if you are using the fully automatic purchase method, enter the URL of your web server into this field. Otherwise, leave the field blank.

- **E-Mail subject**: if you are using the email purchase method, enter the subject that your Casper server is configured to handle. Otherwise, leave this field blank.

- **E-Mail address**: if you are using the email purchase method, enter the address that your Casper server is configured to handle. Otherwise, leave this field blank.

If both URL and email information are given, CASPER attempts to use automatic purchasing first. It switches to email purchasing if there is a communication problem.

26. Fill in the **Payment** fields as needed. You can select credit card purchasing and/or serial number purchasing, depending on how you have set up your CASPER communications and interface. If both are specified, customers are asked if they have a prepaid serial number; if they do not, the credit card purchase method is used.

- **Credit card** checkbox: if you click this box, the three credit-card company checkboxes (Visa, MasterCard, American Express) is activated. Click one or more of these to specify the credit card companies that are accessible to your CASPER server. When purchasing via CASPER, the customer is asked to indicate how payment is to be made. If the customer selects the credit card method, CASPER requests information concerning the customer's account with any of the credit card companies you have specified here.

- **Serial number** checkbox: enables the customer to indicate in CASPER that the customer has a prepaid serial number.

- **Taxes** button: when you click this button to configure CASPER to add tax automatically to the purchase amount, CrypKey Instant displays the following window:

Figure 91: CASPER Tax Information Popup Window

You can fill in the fields for both the Country and State types of tax; CASPER applies both taxes to the payment required from the customer. To ensure accurate tax processing, the country and/or state that you specify are usually the location

of your server. Tax is applied if the customer's state and/or country match the state and/or country that you configure in the above window.

a) Click the **Country Tax** checkbox. The system activates the associated fields.

b) In the **Name of country** box, click the arrow to obtain a drop down list of countries and then select a country.

c) In the **Tax description** box, type in (optionally) a description of the national tax.

d) In the **Tax rate** box, enter (required if you have selected the **Country Tax** checkbox) the tax rate as a percentage.

e) Click the **State Tax** checkbox. The system activates the associated fields.

f) In the **State abbreviation** box, enter the abbreviation of the state, province, canton, department, or other applicable regional entity.

g) In the **Tax description** box, type in (optionally) a description of the state tax.

h) In the **Tax rate** box, enter (required if you have selected the **State Tax** checkbox) the tax rate as a percentage.

- **Always ask for personal info** checkbox: Normally, CASPER asks for the customer's address/phone information only if the purchase is by credit card. If you click this checkbox, CASPER requests this information, even if the customer is using a prepaid serial number.

27. In the product field, click the drop down arrow to display a list of product numbers, as shown below:
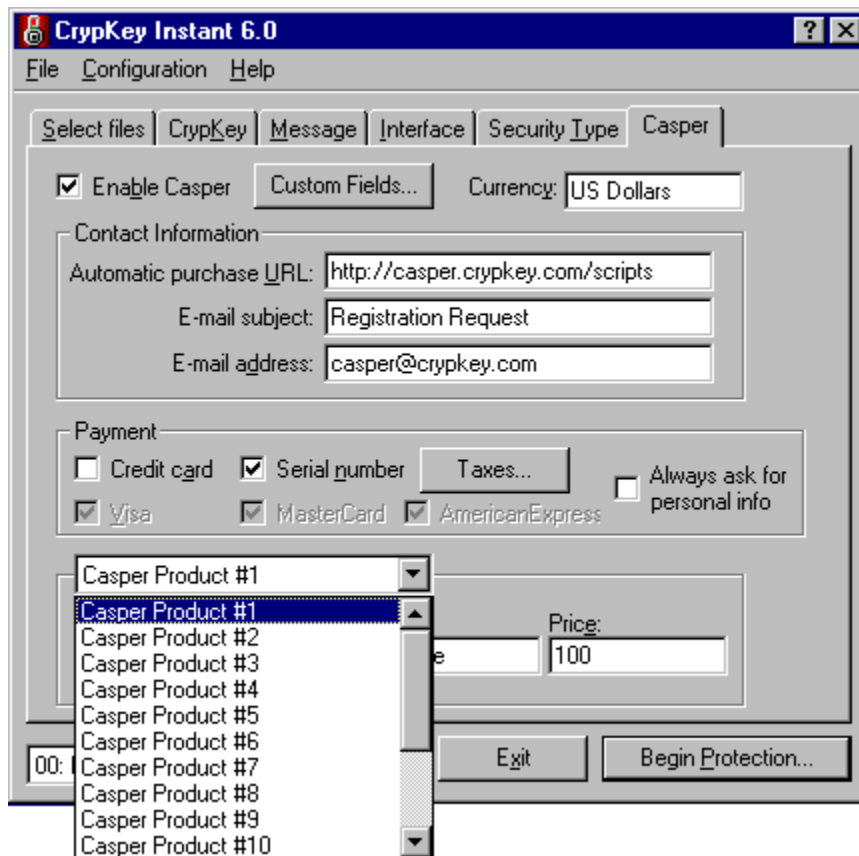
Figure 92: CASPER Product Numbers Drop Down List

As indicated by the list in the above window, you can configure up to 16 products to be displayed in the CASPER Wizard. If you configure more than one product, the wizard prompts the customer to specify which product he or she wants to purchase. One use for this capability is a case where you have different feature sets for your application available at different prices — for example, "Professional," "Standard," and "Light" versions. Each feature set can be set up as a product, with a specific license that includes option and level settings that enable or disable various features in your application.

a) Select a product number from the drop down list. You don't modify the list itself, but rather the supporting information in the fields below it.

b) Fill in the necessary product information in the fields given:

- **Product code**: an alphanumeric code that you define.

- **Description**: your own description of your application.

- **Price**: the application price (either a whole or decimal value), based on the currency you have specified in the **Currency** field.

Network Licensing

Because selling software often involves distributing information on networks, foolproof protection becomes even more important.

C rypKey Instant supports concurrent network users, meaning that you can issue licenses to your clients that allow them to run "x" number of users over a network at one time. Note that network drivers are required to run a CrypKey Instant protected product over a network.

Network drivers must be installed on the local drive of the server. Drivers need to be installed on a standalone machine only if it runs on runs on any NT-based platform (currently Windows NT/2000/XP).

To run your CrypKey Instant protected product on a network, perform one of the following actions:

- install your product on the server and access it from a client machine

  This is the simplest way to take advantage of this feature, and requires no extra steps other than installing your product and the driver on the server local drive.

- install your product on the client machine and access the license file that resides on the server

  This is a more advanced procedure, and offers the advantage of not having to load a large program from the server each time it is run. The procedure for this is described in CrypKey Instant Help: Contents\Feature reference\ License filename control.

For example diagrams of CrypKey network configurations, see Sec. 11: Appendix.

7.1 CrypKey Network Drivers

CrypKey uses an encrypted file request/response model to handle network authorizations. This innovative approach has major advantages:

- Your application uses the same CrypKey library for all network platforms. No changes to your application are required for different networks.

- Since your application uses only one library for all networks, there is a significant savings to you in code size and complexity.

- Your program can work on any network that does file transfers.

CrypKey Instant currently has drivers for the following platforms:

- Windows NT/2000/XP

- Windows 9x/ME

- Novell

For all networks, your clients require read, write, modify, and delete access to the shared server directory containing the CrypKey Instant protected product. For NetWare servers, your clients require read, write, and filescan permissions.

Each CrypKey Instant supported platform requires its own specific drivers. In your role as distributor, it is important to ensure that the appropriate drivers accompany your product to best facilitate clients using your product. The table below summarizes these drivers.

Table 6: Drivers and Platforms

Driver	Platform
wckserve.exe	Windows 95/98/ME
ckserver.nlm	Novell
CrypKey License Service	NT, Windows XP/2000

* **Note:** CrypKey Instant currently does not support the MS-DOS network. If your clients require such network support, CrypKey SDK may better suit your needs than CrypKey Instant.

7.1.1   Supported Platforms

Three network server operating systems are supported, and each requires a different driver. These drivers are listed below, in the order of likelihood that you use them:

- `setupex.exe` and `cks.exe`: These driver files are required to run an application on Windows NT (including Windows NT/2000/XP) standalone or server machines.

    Note: you must use this driver for standalone operation on NT platforms!

- `ckserver.nlm`: This is a Novell NetWare Loadable Module that works for NetWare 3.x, 4.x, and 5.x. Ckserver.nlm does not require any configuration. Novell supports only network usage.

- `wckserve.exe`: This is a Windows program that runs on any Windows 3.x or Windows 9X/ME server. It is unlikely that you need to support this platform as a server.

All server drivers require the client to have read and write access to the shared directory. For NetWare servers, the client must have read, write, file-scan, modify, and delete permissions.

7.1.2   Running Under Windows NT/2000/XP

When running a CrypKey Instant protected product on any NT PC (standalone or networked), you must install the appropriate NT drivers. Such drivers allow CrypKey Instant functions to directly access computer hardware, bypassing NT's built-in disabling of hardware access from normal user programs.

CrypKey Instant requires the CrypKey License Service, which is easy to use and can be called directly from your installation program. Driver installations are seamless to your clients.

The /NETDRIVE directory contains the NT CrypKey Driver, as well as Network drivers for other server platforms.

> *Note:* The NT CrypKey Driver is the most important driver of the CrypKey system. It is the Crypkey License Service required on NT/2000/XP systems, for *standalone and/or network licensing*. All other drivers in the /NETDRIVE directory are required only for network licensing.

You can easily add the drivers to your program's install process by including the CrypKey Network Driver Disk with your distribution. At the end of your installation process, prompt the user for the disk and call SETUP.EXE.

If the destination install directory is added to the command line for the Setup program, the drivers are automatically installed in the directory. No user interaction is required. Following is an example of such a command line:

```
SETUP.EXE C:\CRYPDEMO
```

See the readme.txt in ~\CKI.311\NETDRIVE\NTDRIVER for details that may have been documented after publication of this manual.

Legacy NT Support

CrypKey currently supports Windows NT 3.5, Windows NT 3.51, and Windows NT 4.0. Currently, only the Intel binaries are being shipped. Contact CrypKey for up-to-date platform support. Windows NT versions predating version 3.5 are not supported.

NT Driver Installation Procedure

1. Copy the files setupex.exe and cks.exe to the application directory.

    The file SetupEx.EXE is an NT install program. The file CKS.EXE is a self-extracting zip file of the 6 required setup files.

    Note: don't extract the CKS.EXE zip file — SetupEx.EXE expects to see this file as-is!

    Note: **You require administrator privileges to install the license service**.

    - Alternatively, simply include SetupEx.EXE and CKS.EXE in your Installation script (for example, InstallShield). The script would ensure that both SetupEx.EXE and CKS.EXE are copied into the Install directory, i.e. the directory where the user's program is being installed. After the files are copied, make InstallShield Script call SetupEx.EXE.

2. Run setupex.exe.

    SetupEx.EXE extracts and installs the following files from CKS.EXE:

    - WINNT/System 32 directory: ckldrv.sys, crypserv.exe
    - WINNT directory: ckrfresh.exe, ckconfig.exe, setup_ck.dll, setup_ck.exe

        Note: In Windows XP, these files go into the Windows and System directories.

Programmer's InstallShield Script

Programmers may prefer to use an InstallShield script such as the following to install the NT drivers. This script loads the necessary files, launches setupexe.exe, checks to see whether a reboot is required, and performs a reboot if needed.

```
// after these files have been installed
    LaunchAppAndWait ( TARGETDIR ^ "SETUPEX.EXE" , "" , WAIT );
    file://Find out if we need reboot, get setupex.exe return code
    from .xco file
        ret=OpenFileMode (FILE_MODE_NORMAL);
        ret=OpenFile (nFileHandle, TARGETDIR, "setupex.xco");
        ret=GetLine (nFileHandle, svLine);
        CloseFile (nFileHandle);

        if StrCompare(svLine, "-17")=0  then NTReboot=1;
        endif;


    file://at end of install...
        if NTReboot=1 then
        nDefOptions = SYS_BOOTMACHINE;
        szTitle      = "";
        szMsg1       = "";
        szMsg2       = "";
        nResult      = SdFinishReboot( szTitle, szMsg1,
        nDefOptions,szMsg2, 0 );
```

Testing the Installation

To measure the success of the installation, a file is created in the application directory called setupex.xco. It contains only the value 0 if the installation is successful. Any other number indicates an error, in which case you should contact CrypKey Support.

For a simple test of the installation, place both SetupEx.EXE and CKS.EXE in any directory, and then call SetupEx.EXE. You see your directory in Crypkey.ini. If the CrypKey NT service has never been on your system, you see that too.

Installation Error Codes

Setupex.exe returns an error code if it runs into a problem. This code is returned in one of two ways:

1. in the process termination code, which can be read by the process that launched setupex.exe, if this is supported

2. if (1) is not supported, the error code is written in ASCII to a file called setupex.xco, at termination

Some installation programs are able to receive such an error code. Processing codes of this type is optional.

The other reported errors that are likely to be caused by a bug in your installation are:

```
NTDRVR_INSTALL_ERR_NOT_NT                                          -1
NTDRVR_INSTALL_ERR_REMOTE_DRIVE                                    -2
NTDRVR_INSTALL_ERR_CANNOT_COPY_FILE                                -3
NTDRVR_INSTALL_ERR_CANNOT_RUN_CKSETUP                              -4
NTDRVR_INSTALL_ERR_CKS_EXE_MISSING                                 -5
NTDRVR_INSTALL_ERR_CANNOT_RUN_CKS_EXE                              -6
NTDRVR_INSTALL_ERR_MISSING_FILE                                    -7
//NOTE! You get this error when you do not have permission to load driver
files
//Likely fixed by logging in as a local administrator of the machine
NTDRVR_INSTALL_ERR_REG_COULD_NOT_OPEN_SERVICEMANAGER        -8
//These errors are unlikely and should be reported to us
NTDRVR_INSTALL_ERR_REG_COULD_NOT_OPEN_SERVICE              -9
NTDRVR_INSTALL_ERR_REG_COULD_NOT_REGISTER_DIRECTORY           -10
NTDRVR_INSTALL_ERR_STARTSERVICE_COULD_NOT_OPEN_SERVICEMANAGER   -11
NTDRVR_INSTALL_ERR_STARTSERVICE_COULD_NOT_OPEN_SERVICE          -12
NTDRVR_INSTALL_ERR_STARTSERVICE_COULD_NOT_START_SERVICE         -13
NTDRVR_INSTALL_ERR_STOPSERVICE_COULD_NOT_OPEN_SERVICEMANAGER    -14
NTDRVR_INSTALL_ERR_STOPSERVICE_COULD_NOT_OPEN_SERVICE           -15
NTDRVR_INSTALL_ERR_STOPSERVICE_COULD_NOT_STOP_SERVICE           -16
NTDRVR_INSTALL_ERR_REBOOT_NEEDED                               -17
```

Run Mode

CrypKey has two run modes — *silent* and *verbose*.

In *silent* mode (`SetupEx.EXE /S`), setupex.exe does not put any messages on the screen. It does complete checking and installs the Windows NT driver if it can. If it cannot install the driver, it returns an error code. Since silent mode does not report errors, it is up to the installation program to handle them. Note that the REBOOT_NEEDED message is not an error, but rather a warning.

In *verbose* mode (`SetupEx.EXE`), setupex.exe displays any errors it encounters. It does complete checking and installs the Windows NT driver if it can. If it cannot install the driver, it returns an error code. Note that verbose mode does not report errors on screen if it encounters Windows 95/98/ME, but instead does nothing and silently return.

7.1.3   Running on a NetWare Network

CrypKey Instant offers a Novell NetWare NLM that must be loaded on to your NetWare server machine. CKSERVER.NLM is used for NetWare 3.x and 4.x servers and must be granted read, write, and filescan permissions. This self-configuring NLM can service only the local file server on which it is installed, detecting CrypKey Instant protected products only on this server.

Note that you must manually modify the autoexec.ncf file to ensure CKSERVE.NLM automatically loads the next time you reboot your computer.

Procedure

1. Copy CKSERVER.NLM to the System directory.

2. In the Novell AUTOEXEC file, insert the statement

    ```
    LOAD CKSERVER
    ```

    This starts the driver upon reboot.

3. To start the driver manually, on the Novell server in monitor mode, type

```
LOAD CKSERVER
```

Note: Novell's Patch Level #5 for Novell 3.x. is the minimum patch level required to run CKSERVER.NLM on 3.x. This is available from us by request.

7.1.4   Running Under Windows 3.1/9x/ME/2000/XP

WCKSERVE.EXE is the Windows 3.1, 95, and 98 network driver. This MS-DOS program runs in any Windows environment, allowing the computer to act as a server for CrypKey Instant protected products. Its transparency ensures no loss of computer functionality.

Before running WCKSERVE.EXE, establish an environment variable to notify the program of the location of the CrypKey Instant protected product.

To establish an environment variable for WCKSERVE.EXE:

1. Insert the following command in the AUTOEXEC.BAT file:

```
SET CKSERVE=dir; [dir2;] [dir3;]
```

where dir is the path to the directory that holds the CrypKey Instant protected product

2. If more than one CrypKey Instant protected product resides on the PC, provide a path for each directory, separated by a semicolon. The commands take effect when the PC reboots.

Note that WCKSERVE.EXE also accepts the directory string normally contained in the WCKSERVE environment as a command line variable, as follows:

```
WCKSERVE.EXE C:\MYAPP1;C:\MYAPP2
```

where MYAPP1 and MYAPP2 are directories containing CrypKey Instant protected products.

7.2   Uninstalling the Windows NT Driver

The Windows NT driver has the ability to do partial and complete uninstalls. If other directories are using the driver, the uninstall removes only the directory setupex.exe from

the configuration. If no other directories are using the driver, the uninstall stops the service and removes all files used by the driver.

Procedure

1. Put setupex.exe in the directory you want to uninstall.

2. From the directory, run `SetupEx.EXE /D`.

This performs all the required actions. If no other directories are using the driver, all the driver files are deleted and a message notifies the user that the computer must be rebooted before another installation can be done. You can avoid this message by using the silent mode (`SetupEx.EXE /D /S`).

Note that if the user tries to do another installation before rebooting and the service was removed, the user sees the following "Error -9" message:

```
Register Directory: Unable to open CrypKey License Service.
Reason: The specified service does not exist as an installed
service.
```

The above error message disappears after the computer is rebooted.

If you wish to uninstall, even if there are other directories registered, you can use the `SetupEx.EXE /U` command.

WARNING: this command leaves the other registered directories without a driver to serve them. It is recommended that the command option /D be used in release versions and that option /U be used for test purposes only.

The driver can be reinstalled after the /U option is run, but you must first reboot. The other registered directories, if any were present, are still configured.

Moving Protected Products

Moving CrypKey Instant protected products is possible, given CrypKey Instant's ability to transfer licenses between computers.

A lthough as a distributor you are not typically using the license transfer feature, your customers may find it very useful. Consequently, the capability of CrypKey Instant contributes to the salability of your product. Reassuringly for you, if your clients start with one license, they end with one license; a license transfer is not a duplication of any type.

Licenses can be transferred using either of the following methods:

- direct: move a license from one local or networked directory to another

- floppy disk: move a license from one PC to another, via floppy disk, when the two PCs are not networked

8.1 Direct License Transfers

Direct license transfers move any type of license from one location on your PC to another.

The **Transfer To Directory** command requests a directory path to an existing, unlicensed copy of the same product on your client's hard drive, before transferring the license from the source directory to the target. This target directory must either be local to the source directory or connected by a network serviced by a CrypKey Instant network driver.

Example

You want to move a program with a valid fixed license from `C:\temp` to `C:\apps\bingo`.

Procedure

1. Copy the program to `C:\apps\bingo`.

2. Open the application in `C:\temp`. A splash screen similar to the following appears:
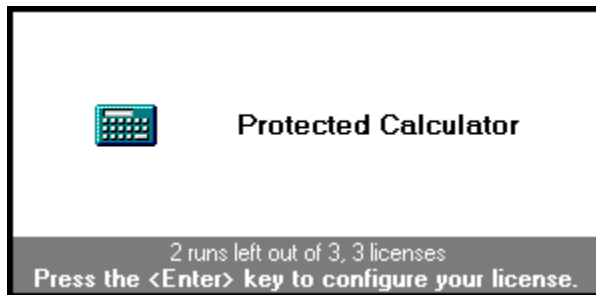

Figure 93: Protected Application Splash Screen

The splash screen remains displayed only briefly and then is replaced by the regular application-opening window.

3. While the splash screen is displayed, press **ENTER**, to configure the application license. CrypKey Instant displays the following window:
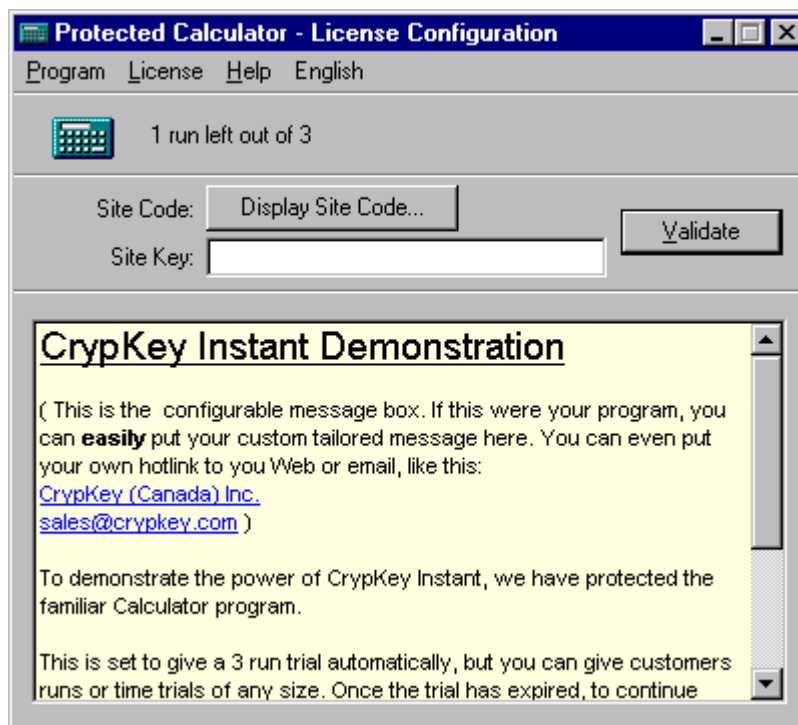
Figure 94: Application License Configuration Window

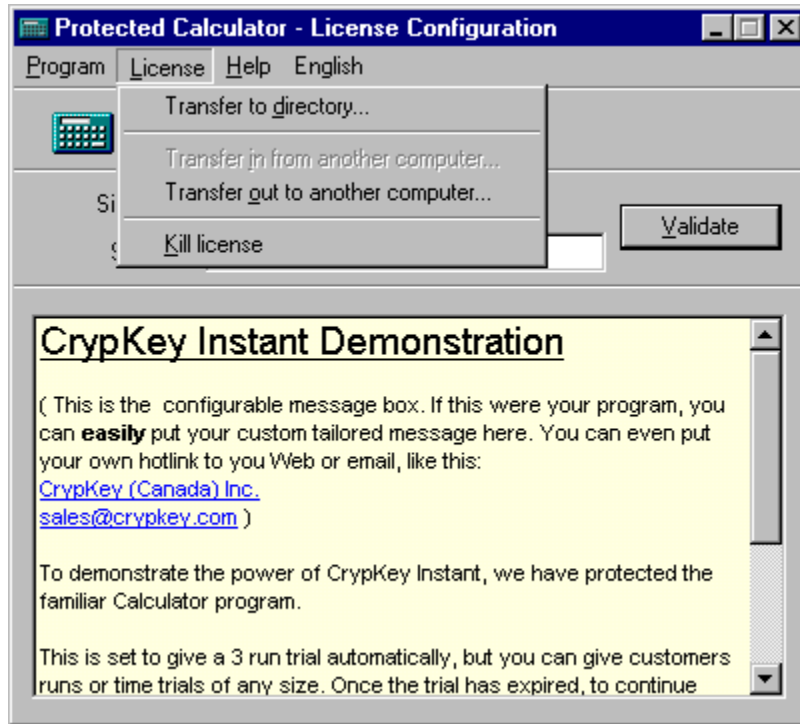**4.** In the above window, click the **License** menu option. The window now appears as follows:

Figure 95: License Commands Popup Window

5. In the above window, click the **Transfer To Directory** command.
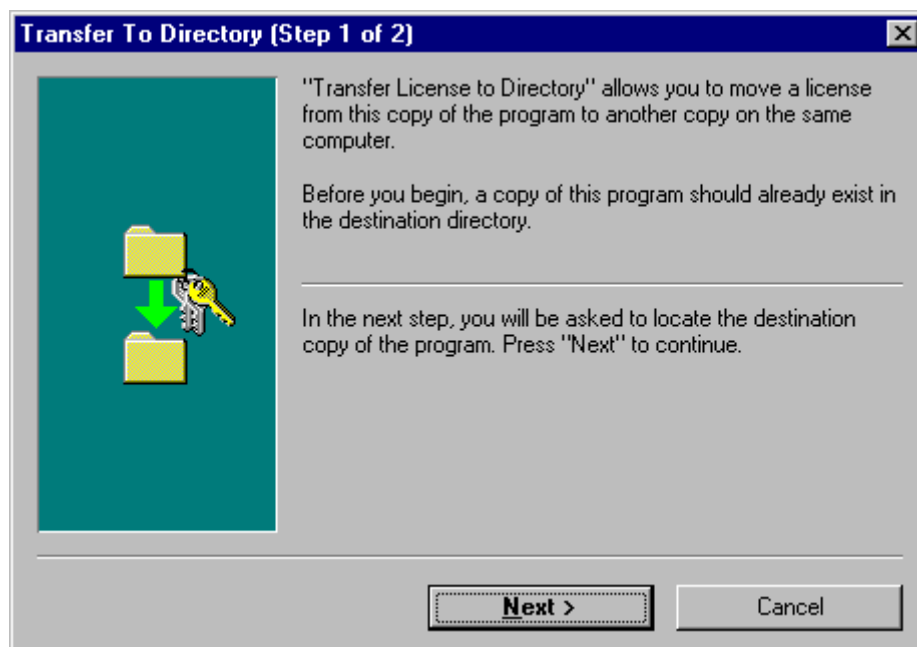
CrypKey Instant displays the following window:

Figure 96: Transfer to Directory Window

6. In the above window, click **Next**. CrypKey Instant displays the following window:
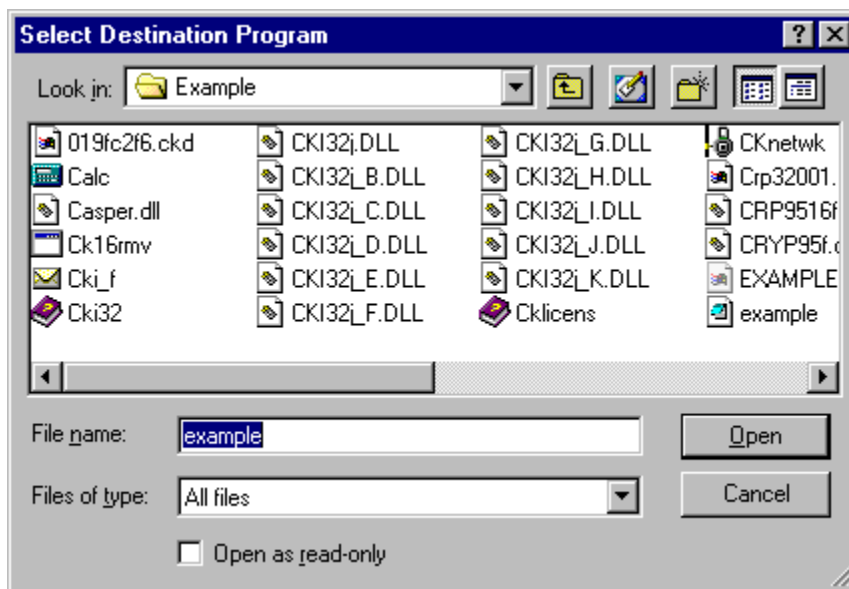

Figure 97: Select Destination Program Window

7. In the above window, navigate to the `C:\apps\bingo` directory, select the copied program filename, and press **ENTER**.

The program copy in `C:\apps\bingo` has the license that was previously assigned to the original program in `C:\temp`.

8.2 Floppy Disk License Transfers

This type of operation transfers a license from an existing authorized copy of an application on one computer to an unauthorized copy of the product on a second computer.

The transfer process does not jeopardize your license in any way and is completely secure because the floppy disk is registered to a specific PC in a specific location. This ensures the license can only be transferred to the target PC you specify.

Example

You want to transfer the license for the *Calculator* example program from PC-1 to PC-2.

Procedure

1. Ensure that you have an authorized copy of the application on PC-1, an unauthorized copy of the application on PC-2, and a floppy disk inserted into PC-2.

> *Note:* as indicated by Step 2, your first operation is on the *unauthorized* computer (i.e., PC-2).

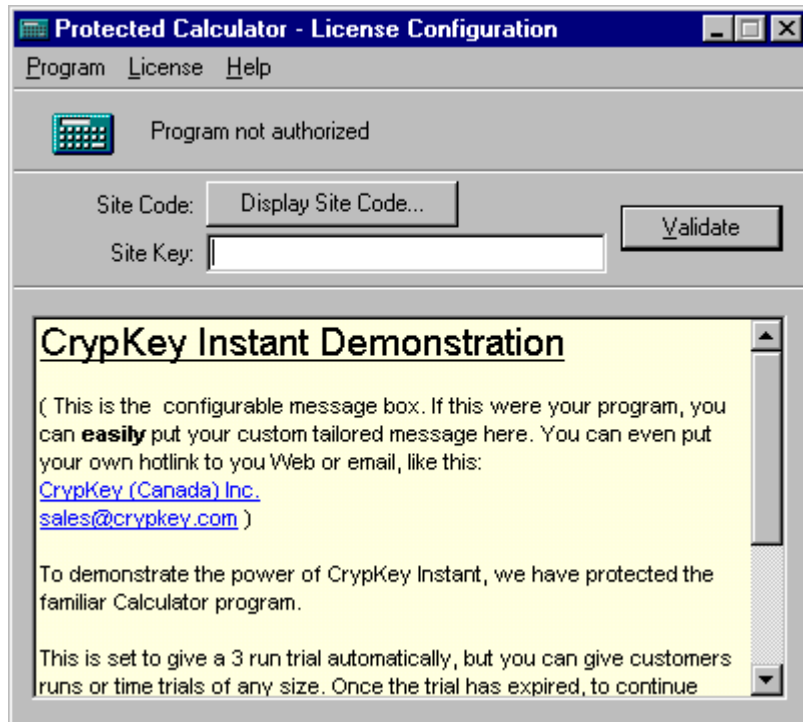**2.** Start the program on PC-2. The program's opening window is shown below:

Figure 98: Unauthorized Program running on PC-2

3. In the above window, click the **License** option to display the **Transfer in from another computer** command, as shown below:
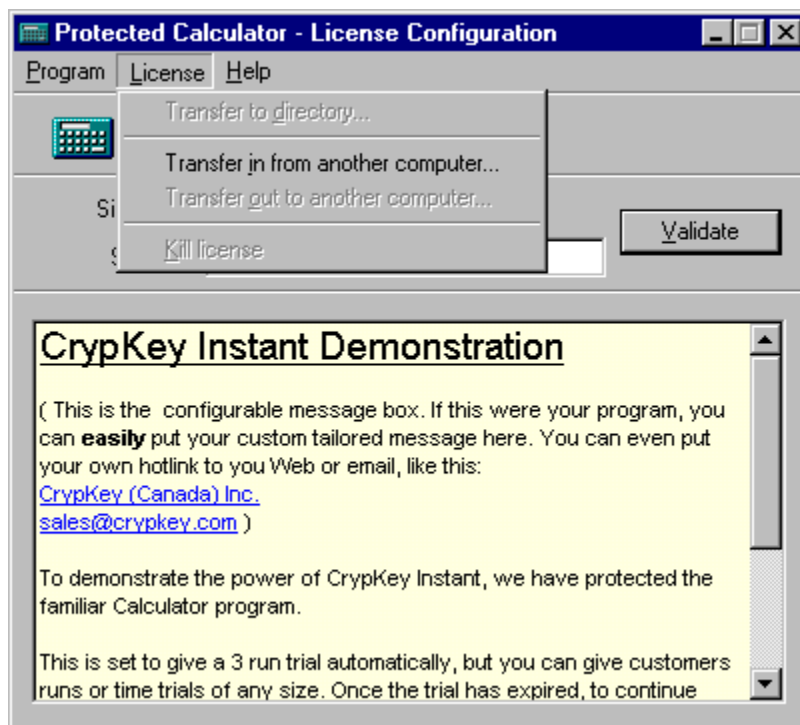

Figure 99: "Transfer in…" Command

4. In the above window, click the **Transfer in from another computer** option. The system displays the following window:
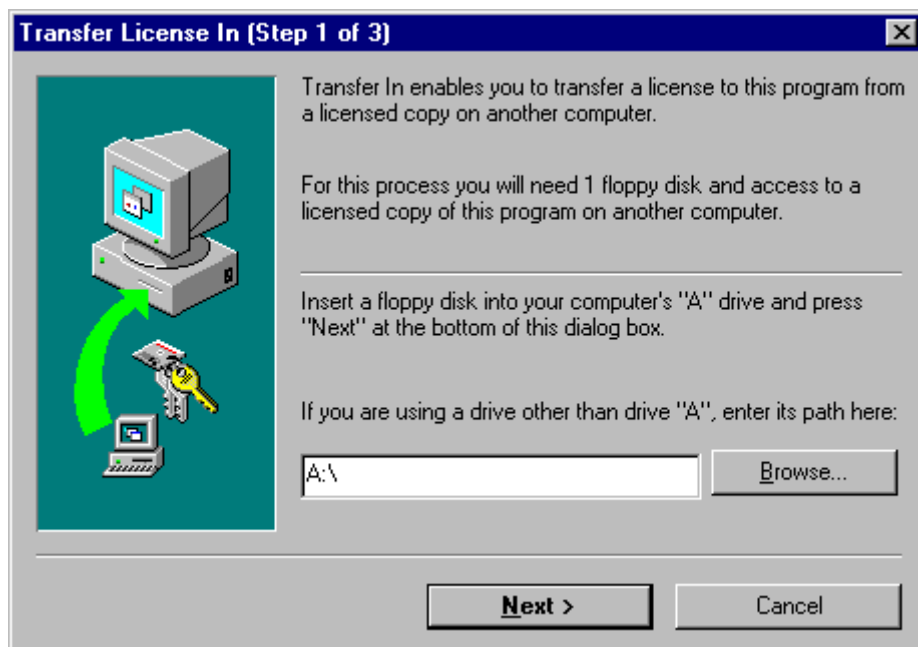

Figure 100: "Transfer License In" Window (Step 1)

5. In the above window, use the **Browse** button if necessary to supply the floppy disk path, then click **Next**. The program imprints its registration on the floppy disk and the system displays the following window:
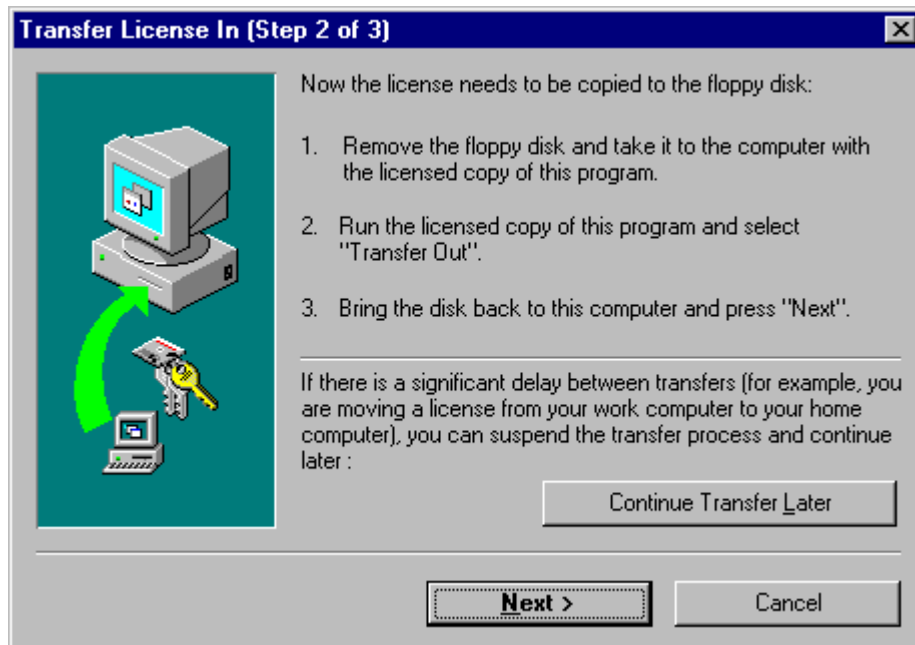

Figure 101: "Transfer License In" Window (Step 2)

6. If you need to close the PC-2 program while you work with the PC-1 program, click the **Continue Transfer Later** button in the above window. The system displays the following popup message:
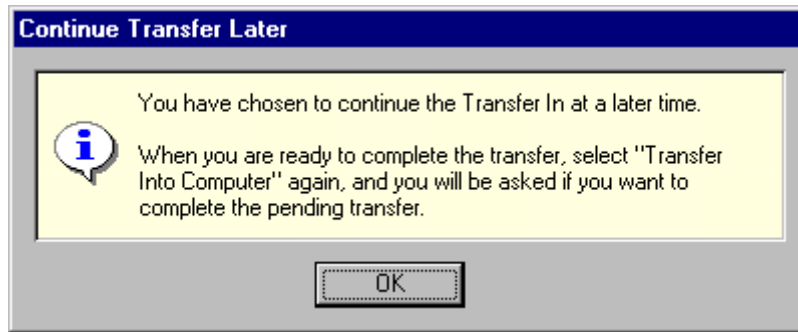

Figure 102: Continue Transfer Later Popup Window

7. Click **OK** to acknowledge the above popup.

8. Remove the floppy disk from PC 2, and insert it into PC 1.

9. Start the program on PC 1, and click the **License** button as shown below:
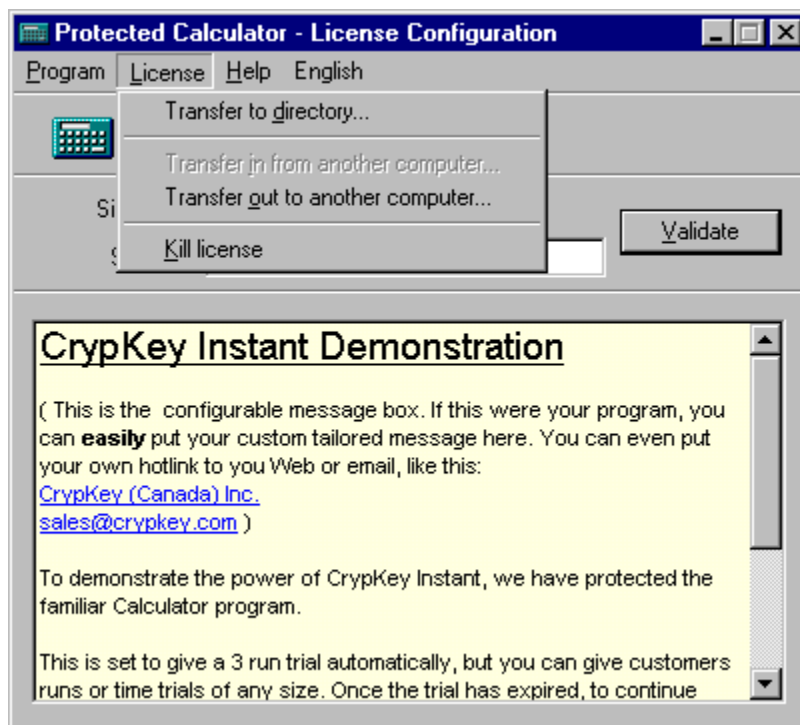

Figure 103: Program on PC-1: "Transfer Out" Command

10. In the above window, click the **Transfer out to another computer** option. The system displays the following window:
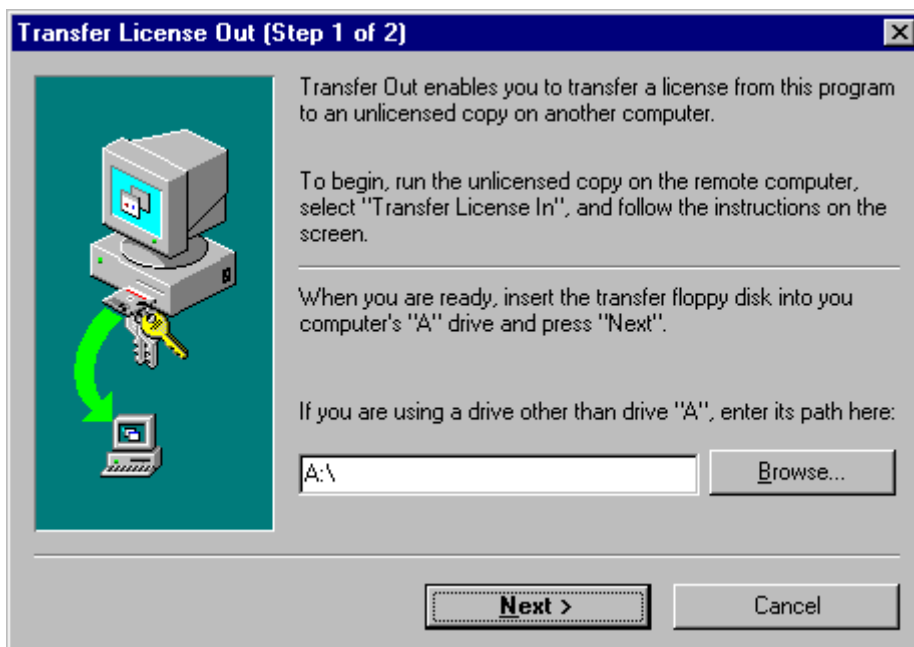

Figure 104: "Transfer License Out" Window (Step 1)

11. In the above window, use the **Browse** button if necessary to supply the floppy disk path, then click **Next**. The program reads the registration imprint file and then writes a matching file to the floppy disk, decrementing the license count at the source or discontinuing it (if it is a single user license).

12. Remove the floppy disk from PC-1, and return it to PC 2.

13. Resume the program on PC-2.

- If you did **not** exit from the program in Step 6, proceed to **Step 14**.

- If you exited the program in Step 6, the following window appears when you start the program again:
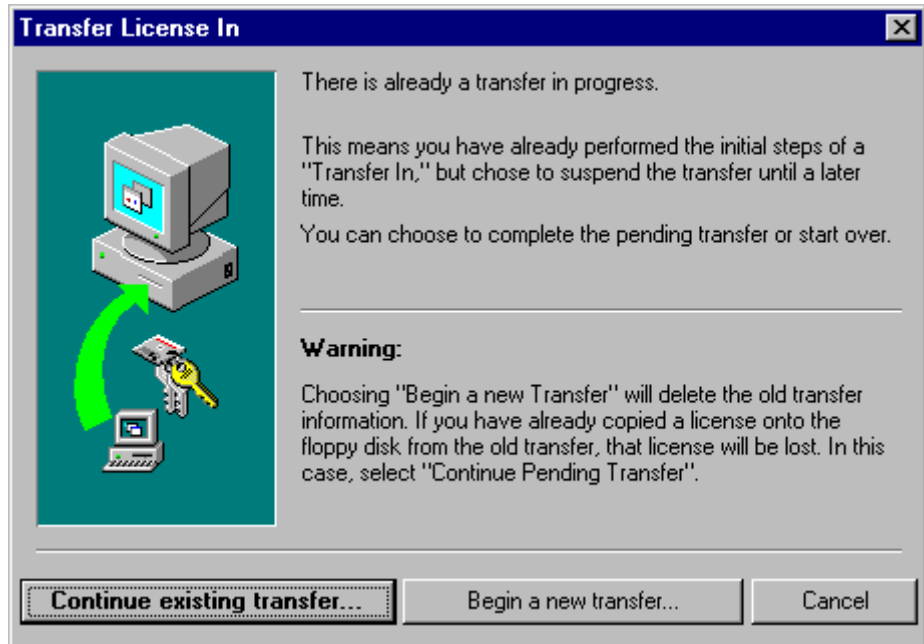
Figure 105: Transfer in Progress Window

The above window simply advises you that you have previously initiated a license transfer. To continue this operation, click **Continue existing transfer** in the above window. The following window is displayed:
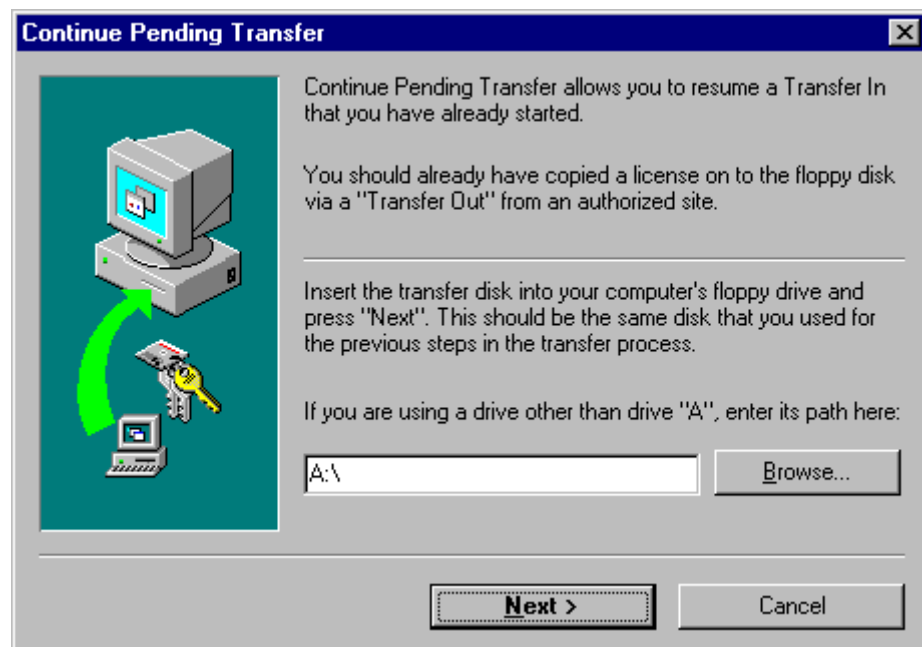

Figure 106: Continue Pending Transfer Window

14. If you did **not** exit the program on PC-2, the program window appears as follows:
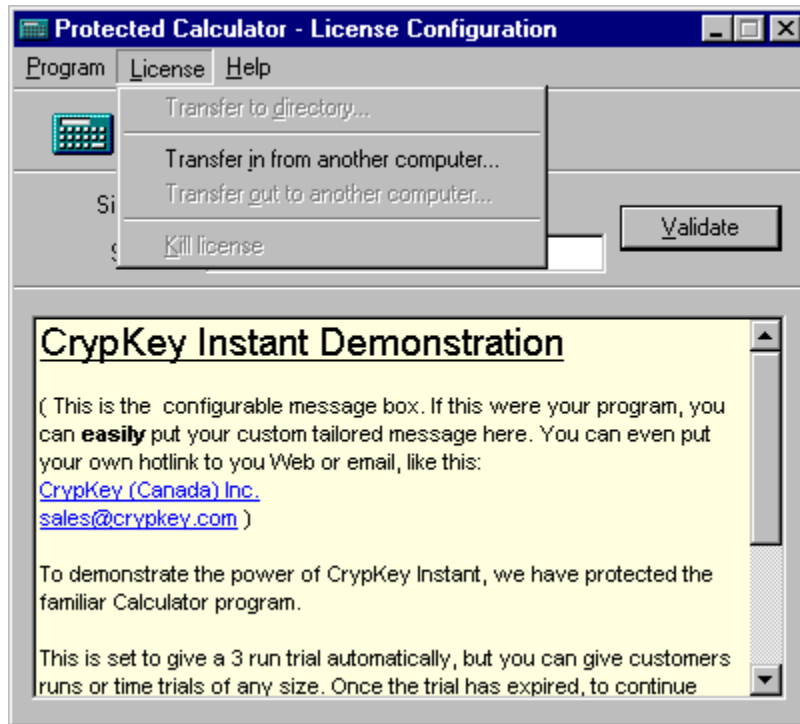
Figure 107: Window resuming operation of program on PC-2

In the above window, click **Transfer Into Computer** to complete the transfer. The system displays the Continue Pending Transfer window, shown in Figure 106.

15. Click **Next** in the Continue Pending Transfer window. The following window appears, indicating that the transfer is complete:

Figure 108: "Transfer License In" Window (Step 3)

16. Click **Finish**. The License Configuration window on PC-2 appears, showing that you are authorized to use it.

Frequently Asked Questions

The following questions are asked most frequently of our technical support representatives.

S uccessfully answering your questions is a priority of the CrypKey Instant technical support team. Since CrypKey's inception in 1994 and CrypKey Instant in 1998, we've strived to eliminate your guesswork. We encourage you to read through the following pages before calling us for support.

9.1   General

9.1.1   Software Protection

Q Is illegal copying of my product a real concern?

A Yes. In today's high-tech world, you need copy protection. A copyright sign on your product does not guarantee that users will not copy your product. Copyright laws, like all others, can be broken, despite enforcement efforts. If you're considering marketing overseas, the situation is even more serious. Many countries outside North America are without any form of copyright law, further increasing the possibility for unpaid copies of your product to enter the market.

Although software giants such as Microsoft can absorb sale losses related to illegal copying, smaller players, whose market is more defined and vertical, cannot. Software is no longer solely produced by large software houses and sold in mass quantities. Today's software developers include doctors, lawyers, engineers, and those in your profession: essentially, any individual with a knowledge that can be shared and

marketed through the medium of computers. Today's developers need CrypKey Instant.

9.1.2 CrypKey Instant Advantages

Q   Why is CrypKey Instant the protection package of choice?

A   The CrypKey Instant licensing system circumvents the problems prevalent in current software protection technology, as outlined below:

Table 7: Software Protection Technology—Problems and Solutions

Copy Protection Problem	Description	CrypKey Instant Solution
Key failure (hardware (dongle) or disk keys are subject to higher rate of failure than computers)	Keys transfer software from one computer to another. Hardware keys can suffer from fatal static shock, diskette keys can suffer from media failure or being misplaced. Because users frequently transfer software, this action, while protected, must remain as convenient as possible.	CrypKey Instant replaces hardware and disk keys with Telephone Authorization, where client computers become the "key" so that clients can easily transfer your protected product to other computers. With CrypKey Instant, an ordinary floppy can be used for license transfers..
Hardware incompatibilities	Hardware keys can be incompatible with some computers, printers, or other hardware keys. Disk keys can be incompatible with certain makes of computers and different sizes of disk drives.	No hardware key equals no hardware incompatibilities. CrypKey Instant has an outstanding record of running on any PC-compatible computer, including foreign machines (i.e., Japanese NEC PC) and diskless workstations.

Copy Protection Problem	Description	CrypKey Instant Solution
Induced downtime	When a copy protection key fails, time is required to obtain a new one, dependent on key inventory, protection company replacement procedures, and client location.	Your clients are up and running after one quick telephone call rather than waiting for a hardware or disk key in the mail.
Failure to protect	Bit copiers, sold as programs that can make "backup" copies of copy-protected software, can easily copy most disk keys.	With CrypKey Instant, your product cannot be copied by a bit copier. Your product is shipped on a CD and runs in demonstration mode until telephone authorization, whereby it becomes fully functional. Because your disk does not need to be copy protected, manufacture your disks yourself.
Costs	Key problems can eat up more than 50 percent of your technical support allowance.	Non-technical staff can issue telephone authorization with the CrypKey Instant Site Key Generator, freeing up your technical staff for technical support.
Client annoyance	Market acceptance of hardware keys (dongles) is declining.	Deliver product upgrades and renew licenses instantly. CrypKey Instant allows you to specify levels and/or options and the duration or number of times clients can use your product. You also have the option of selling your product on a time or per-use license basis.

9.1.3   Telephone Authorization

Q   How does CrypKey Instant protect products without using keys?

A   Telephone authorization replaces keys in the CrypKey Instant system. The process is as follows:

- once installed on your client's computer, your product generates a code specific to that computer, which your client telephones or faxes to you

- using CrypKey Instant, you generate an authorization code (for immediate or later distribution to your client) that only allows your product to run on your client's computer

9.1.4   Client Annoyance

Q   Won't clients be annoyed by needing to make a telephone call to use my product?

A   CrypKey Instant users have advised us that this drawback is typically perceived rather than actual, mitigated by client relief over the absence of hardware or disk keys. However, ways to capitalize on the CrypKey Instant telephone authorization system include:

- ship your product to potential clients in demonstration form. When your clients are ready to buy, use the authorization method to convert your demonstration program into a fully functional copy.

- send your clients a disk that demonstrates your product's options. Ask clients to call when they have determined which options they want. With CrypKey Instant, toggle on the desired options during the call, resulting in clients often purchasing more options than originally ordered.

- ensure your client is comfortable and satisfied with running your product. Clients appreciate support, and you may prevent problems and ill will from occurring.

9.1.5 24-hour Telephone Support

Q   Do I need 24-hour telephone support?

A   No. CrypKey Instant's trial licensing feature ensures clients can contact you for permanent authorization during regular business hours and can open and utilize your product any time they choose, including weekends and holidays. CrypKey Instant allows you to expedite repairing or changing licenses. Using CrypKey Instant can dramatically reduce your customer support hours. Trial license means that your product is available to your clients at any time, weekends and holidays included.

9.1.6 User Clock Manipulations

Q   Can clients tamper with CrypKey's time-dependent licenses by setting back their PC clocks?

A   No. CrypKey records each time clients check their license status from within your product. If clients set back their clocks more than 75 minutes, CrypKey generates an error code for your product.

Additional Clock Manipulation Checks

Programs are available on the market that automate the process of changing a computer's clock so that time-restricted protection can be bypassed.

These programs change the time that the protected program sees. For example, if the time never extends beyond your program's trial period, in theory, your program runs indefinitely.

CrypKey safeguards against clock manipulations by monitoring your customers' computers for the inconsistencies such an attack generates. CrypKey detects when time is falsely reported to your program and prevents your program from running. All times reported by CrypKey are the server's, adjusted to the local time zone of the computer.

CrypKey may also detect clock manipulation if users change the clock by more than several hours for benign purposes, such as testing. If your program is prevented from running in these kinds of cases, your customers can correct the situation by rebooting their computer.

9.1.7 Computer Signatures

Q   Is a computer's signature derived from the volume serial number? If so, hackers could alter this number with programs such as Norton Utilities or PC Tools or those that directly access hard disk sectors. If not, how difficult is cloning the machine authorized to run my product?

A   Computer signatures are derived from unchangeable parameters particular to the machine's software installation, which are nearly impossible to duplicate on another machine.

9.1.8 License Transfer to Floppy

Q   Transferring the license for my product to disk seems dangerous. A pirate could disk copy the floppy to generate an exact image of the first that could easily be used to authorize other machines. Is the onus on me to enable or disable the transfer to floppy?

A   Although the decision to allow floppy disk license transfers is yours alone, note that a transfer incorporates the following process:

1.   The signature of the target computer is written on the floppy (in highly encrypted files).

2.   The license is transferred from the source computer to the floppy.

3.   The license is transferred from the floppy to the target computer.

Even if the floppy is copied after Step 2, it only works in the specific target computer because of information encoded in Step 1.

9.2   Technical

9.2.1   Disk Compression Programs

Q   Is CrypKey affected by disk compression and defragmentation programs such as Norton Utilities Speed Disk or Nuts and Bolts?

A   CrypKey is generally immune to these programs. With Speed Disk, however, adhere to instructions in Norton Utilities Speed Disk, page 62, to ensure CrypKey licensing files remain undamaged (see Section 10.4: Norton Utilities Speed Disk for more information).

9.2.2   Library Impacts

Q   Does CrypKey Instant affect other third-party libraries?

A   No. CrypKey is highly non-intrusive, meaning that it works with virtually any software, and more importantly, any hardware.

9.2.3   Hard Disk Failure

Q   What happens if the hard disk fails, thus invalidating the CrypKey Instant license?

A   We provide a new license: no questions asked. Our clients always receive the benefit of the doubt.

In reality, hard disk failures among CrypKey clients are rare. CrypKey's three-year relationship with Flowel, a popular flow calculation program we market worldwide, has resulted in eight reported hard disk crashes, of which we feel only two are suspect.

9.2.4   Product Update Releases

Q   How does CrypKey Instant manage product update releases?

A   CrypKey Instant simplifies releasing your product updates. Copy the new version of the product over the old one, and it assumes the existing license.

9.2.5   Multiple Program Names

Q   Can a single product have multiple names using CrypKey Instant?

A   Yes. To successfully award a product multiple names, ensure all names key off one file guaranteed to occupy the same directory as your product. CrypKey Instant allows you to select the file on which you want the license based.

For example, all versions of Product1 key off a file named product1.dat, located in the same directory as the .exe for every installation of your product. This method makes it easy to consistently install CrypKey Instant in all your product versions.

9.2.6   Floating Licenses

Q   My clients sometimes ran three floating copies of my simple Windows product when they were only licensed for two. How did this happen?

A   CrypKey Instant's mechanism for counting license numbers is foolproof: if a particular application of your product fails to call Get Authorization () regularly, it loses its license. Parameters of the InitCrypkey () call control the time before the application fails. Change these parameters to suit your requirements to prevent unauthorized use of your product.

9.2.7   CD-ROM Distribution

Q   Does CrypKey Instant support distribution via CD-ROM?

A   Yes. CrypKey Instant can be utilized whether you install your executable from a CD-ROM to your hard drive or your executable remains resident on the CD-ROM.

In the latter case, the problem that arises concerns the inability of CrypKey Instant to write its license files, created dynamically, to the CD-ROM, which is read-only. Circumvent this issue by storing CrypKey Instant license files on your hard drive. CrypKey Instant stores license files where you specify (see Sections 1.7.6, 1.7.7, and 3.6.4).

Putting Your License on a Server and Your Program on the Client

In a network license situation, rather than downloading a large program across the network when it runs, install the program on the target machine, and ensure that only the license resides on the server.

9.2.8   Internet Distribution

Q Can files protected by CrypKey Instant be distributed over the Internet?

A Yes. Because CrypKey Instant eliminates hardware or disk key technology, it provides an ideal channel for Internet distribution.

9.2.9   File Set Protection

Q Can CrypKey Instant protect a set of files?

A Yes. Use CrypKey Instant to protect an unlimited number of programs related to your product. The options feature can individually enable or disable up to 32 programs per product at no additional cost.

Identify one module as main, whose license all other modules must check. Achieve this by passing the main module path to the InitCrypkey () call in ALL modules. All modules must also use the main module's master and user keys.

9.2.10   32-Bit File Access

Q Does CrypKey Instant support 32-bit file access?

A Yes, as of version 3.3.

9.2.11   Foreign System Compatibility

Q Is CrypKey Instant compatible with foreign PCs and operating systems?

A Yes. CrypKey is fully functional on the Japanese NEC PC and the Kanji version of Windows 95. Other Asian and European versions of Windows are also supported.

9.2.12 Removable Hard Drives

Q Does CrypKey Instant work with removable hard drives (i.e., Iomega Zip and Jaz drives)?

A Yes. CrypKey Instant fully supports Iomega Zip and Jaz drives. CrypKey Instant protected products can be normally installed and run from these drives. Other removable hard drives, however, are not supported, and CrypKey Instant protected software does not run from them.

9.2.13 Anti-virus Software

Q Will CrypKey Instant trigger anti-virus software that may be in use on a computer?

A No. CrypKey Instant does not trigger anti-virus software.

9.2.14 Installer Software

Q Is CrypKey Instant compatible with such installer software as InstallShield?

A Yes. CrypKey is fully compatible with all installer systems, especially InstallShield. We use InstallShield in our own software and have never experienced problems.

9.2.15 US Exports

Q Can I export my CrypKey Instant protected product from the US?

A Yes. In the past the US State Department has approved CrypKey Instant for export to all countries except Cuba and Syria. You can get your product officially approved by contacting the US government directly.

9.2.16 Windows 98

Q Does CrypKey Instant work on Windows 98?

A Yes. CrypKey Instant and CrypKey Instant protected products run under Windows 98. Note, however, that if converting from FAT 16 to FAT 32, you must first transfer your license to another PC to retain your authorization.

Troubleshooting

Having trouble? This section provides solutions to some common problems.

S ince implementing CrypKey Instant can create problems in some environments, you should check your environment type against the listed types to pinpoint problems and identify solutions.

This chapter includes the most common problems reported to CrypKey Technical support. For problems not listed here, please visit our website at www.crypkey.com and review our searchable support database. The database is accessible using a customer password, which you can obtain from us.

10.1   CrypKey License Service Problems

Most CrypKey Instant operational problems are manifested by error messages.

When there is a problem with the CrypKey License Service, the user reports one of the following:

- An error window such as the one shown below:
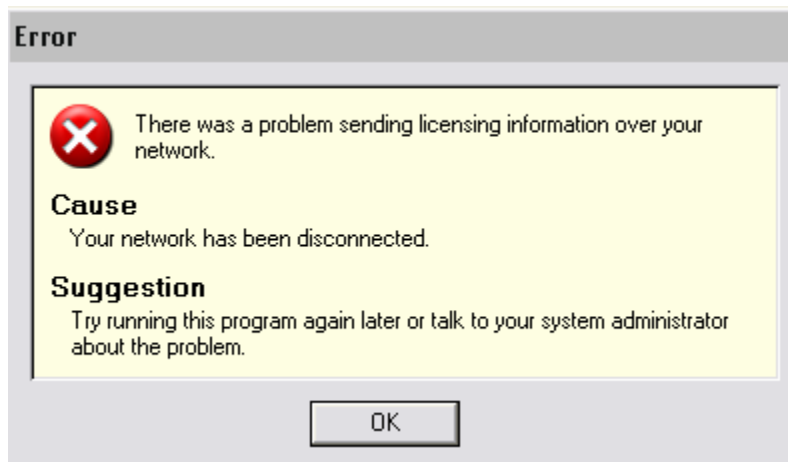
Figure 109: Network Disconnect Message Window

- A return code and error message, appearing only in the .ckn file (see Sec. 10.1.1: CrypKey Technical Support):

```
INITIALIZATION FAILURE

NETWORK: NETWORK DRIVER APPEARS NOT TO BE SERVING IN DIRECTORY / -102
```

This message means that the CrypKey driver you are using is not serving the directory in which your CrypKey-protected application is located. All CrypKey-protected applications must be served by the driver. This type of error usually occurs on Windows NT.

If you see this error, send an email message containing the date of setupex.exe to CrypKey Support at support@crypkey.com.

Problems of this type usually occur on NT or Novell Netware file systems where the directory security is modified. Refer to the following troubleshooting charts for assistance with this problem.
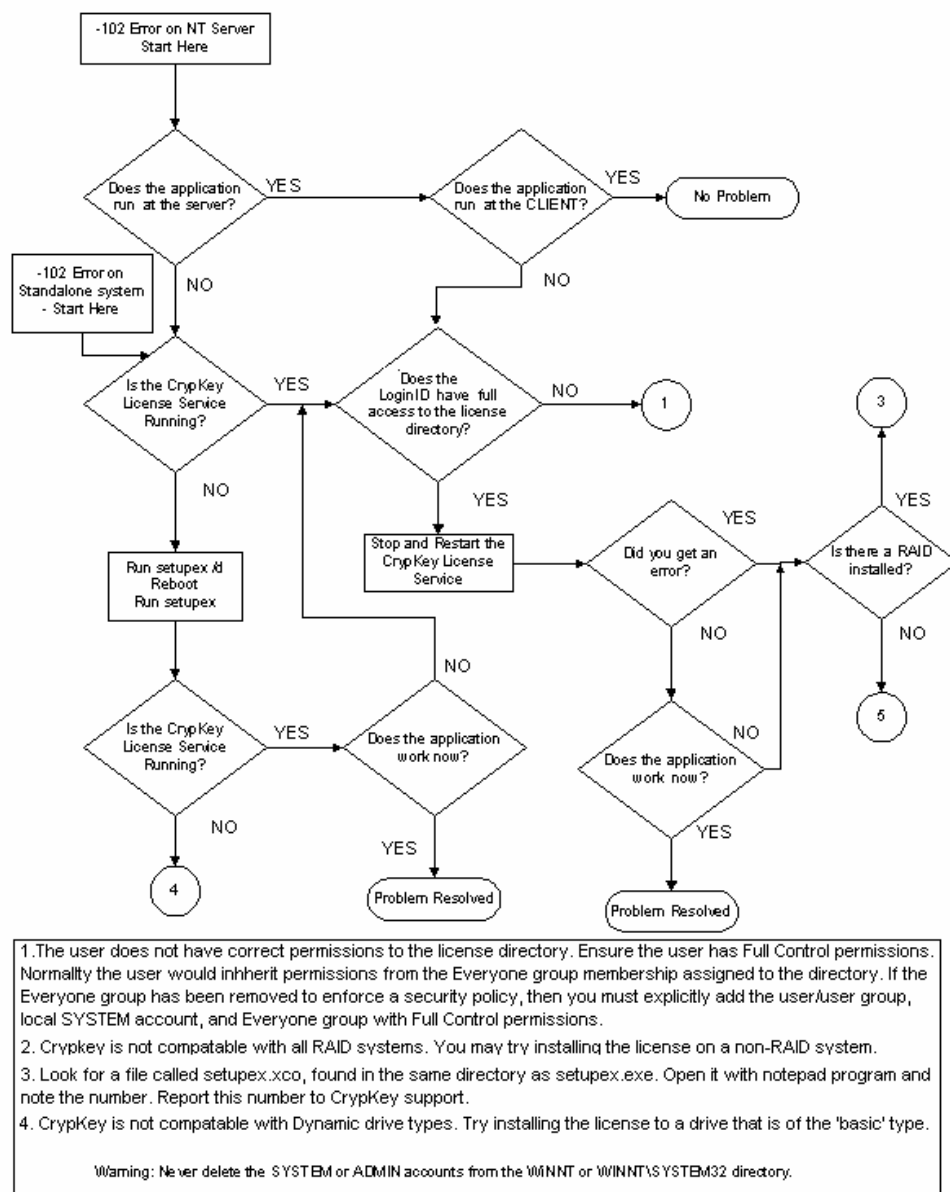
Figure 110: NT File System Troubleshooting Flowchart
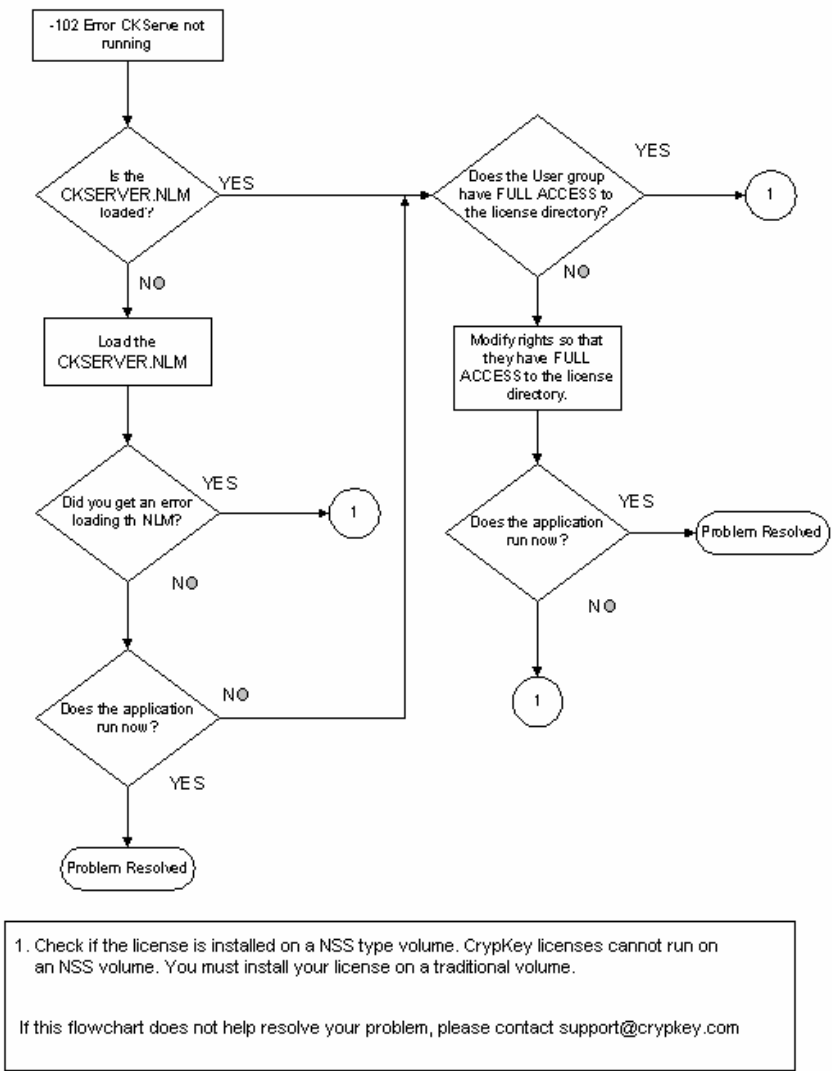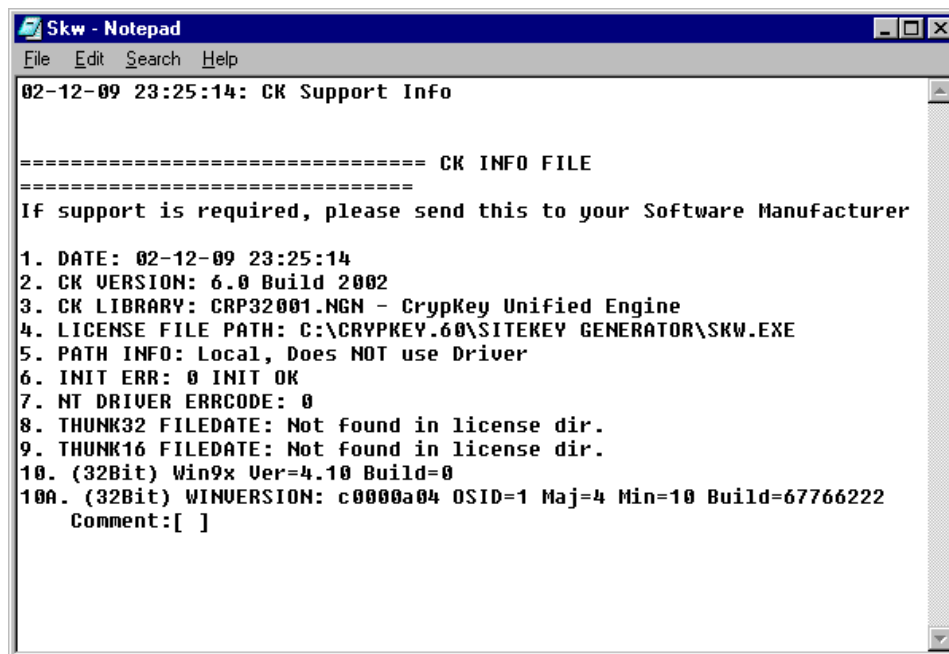
Figure 111: Novell File System Troubleshooting Flowchart

10.1.1   CrypKey Technical Support

When requesting technical support from support@crypkey.com, be sure to include the following information:

- Company name

- CrypKey account number

- A brief and concise explanation of the problem

- Error messages: your applications error messages may be ambiguous or not have significant meaning to CrypKey support. For this reason, develop your application to reference the associated CrypKey function and return code in your error messages.

- Sequence of events required to recreate the problem. Include information such as:

    - order of CrypKey functions called

    - return codes from those functions

    - operating system

    - license type and duration

- the CrypKey libraries used

- your compiler and version

- .ckn file – this is a file created by the CrypKey functions and contains useful information that may be valuable for resolving your problem. The file resides in your CrypKey directories. When opened, the .ckn information appears in a window similar to the following:

```
Skw - Notepad                                                     _ □ ×
File  Edit  Search  Help
02-12-09 23:25:14: CK Support Info


=============================== CK INFO FILE
==============================
If support is required, please send this to your Software Manufacturer

1. DATE: 02-12-09 23:25:14
2. CK VERSION: 6.0 Build 2002
3. CK LIBRARY: CRP32001.NGN - CrypKey Unified Engine
4. LICENSE FILE PATH: C:\CRYPKEY.60\SITEKEY GENERATOR\SKW.EXE
5. PATH INFO: Local, Does NOT use Driver
6. INIT ERR: 0 INIT OK
7. NT DRIVER ERRCODE: 0
8. THUNK32 FILEDATE: Not found in license dir.
9. THUNK16 FILEDATE: Not found in license dir.
10. (32Bit) Win9x Ver=4.10 Build=0
10A. (32Bit) WINVERSION: c0000a04 OSID=1 Maj=4 Min=10 Build=67766222
    Comment:[ ]
```

Figure 112: .ckn Diagnostic File

10.2   Windows NT Diagnostics

The Windows NT driver maintains two error log files. You can help us to rectify your Windows NT driver problems by sending (by email or fax) the error.log and the errord.log files, located in the C:\WinNT and the C:\WinNT\System directories.

10.3   NetWare-related Issues

The following errors can occur on Novell networks using CrypKey ckserver.nlm.

10.3.1   Sample Error 1

If your clients attempt to execute your CrypKey-protected product from a NetWare server, an error message resembling the following occurs:

```
CKSERVE is not serving this directory
```

To solve this error, ensure that:

- CKSERVER.NLM is running on the server

- the CKSERVER.NLM path statement within the autoexec.ncf is correct

- the directory name does not contain a period

- the maximum number of users for the CrypKey-protected product has not been exceeded

10.3.2   Sample Error 2

If your referenced library routine cannot be located within the current .nlm, the loaded Novell clib.nlm library may not be current, generating an error message resembling the following:

```
Undefined symbol:_chk
```

To solve this error:

1. Implement the Novell patch libup5.exe or a newer patch (available from CrypKey or Novell).

2. Ensure a copy of directfs.nlm is loaded.

3. Shut down the server and restart, which loads the new clib.nlms (clib.nlms cannot be manually unloaded and loaded).

10.3.3   Sample Error 3

If none of your clients is logged onto the network executing the CrypKey-protected program, but an error stating that there are users logged on appears:

1. Delete the <programname>.tb2 file from the network.

2. Shut down the server and restart it.

3. Restart the application.

10.4   Norton Utilities Speed Disk

Speed Disk is the defragmentation utility included in Symantec's Norton Utilities. Unfortunately, Speed Disk moves CrypKey licensing files, causing license loss. CrypKey uses four special licensing files (.ent, .rst, .key, and .41s) to control your product licensing. These files are hidden system files and reside in the same directory as the protected product.

To prevent license loss:

1. Open Speed Disk, and choose **File, Options, Customize,** and **Unmovable Files**.

2. Specify that the .ent, .rst, and .key, files cannot be moved (the .41s files do not need to be specified).

3. Choose **File, Options, Optimization,** and **Save** to save the new profile.

Section

11

Appendix

This section includes the following:

- CrypKey v6.x OS File Matrix

- CrypKey program flowchart

- peer-to-peer example network diagram

- example NT network configuration diagrams

Table 8: File Distribution Matrix

FILENAME	WIN9X	WIN ME	WIN NT	WIN 2000	WIN XP	NOVELL
cki32h.dll	✓	✓	✓	✓	✓	✓
cryp95e.dll[5]	✓	✓			▪	▪
crp9516e.dll[5]	✓	✓			▪	▪
ck16rmv.exe[5]	✓	✓			▪	▪
wckserve.exe[2]	✓	✓				
setupex.exe[1]			✓	✓	✓	
cks.exe[1]			✓	✓	✓	
ckserver.nlm						✓
cki32h_?.dll[4]	♦	♦	♦	♦	♦	♦
cki_?.msg	♦	♦	♦	♦	♦	♦
cki_?bmp	♦	♦	♦	♦	♦	♦
cklicens.hlp	♦	♦	♦	♦	♦	♦
splash.int[3]	♦	♦	♦	♦	♦	♦
ck16?.dll	❖	❖	❖	❖	❖	❖
ck16h_?.dll[4]	❖	❖	❖	❖	❖	❖
cknetwk.exe	❖	❖	❖	❖	❖	❖
hdsn1.dll	❖	❖	❖	❖	❖	❖
crp32001.ngn	✓	✓	✓	✓	✓	✓

Legend:
♦   Bullets indicate files that are optional. See product manuals for more information.
❖   Bullets indicate files required for 16Bit applications.
✓   Bullets indicate files required for 32Bit applications.
▪   Bullets indicate optional files depending on XP Home Edition/Pro compatibility mode settings.
Bullets with a light gray background indicate files that are common to 16 and 32Bit applications.
Files in **GRAY text** are required for a network.

For details, see Sec. 3.6: Distributing Your Protected Application.

Notes
1. setup.exe and cks.exe are files used to install the Crypkey License Service required on *all* NT systems whether networked or standalone.
2. wckserve.exe is required for Win9X/ME servers
3. splash.int is required for custom splash screen. See online database for more information.
4. See online database for more information regarding language support.
5. Thunk files for Win9X/ME go into the application or license directory only.

Figure 113: CrypKey Program Flowchart

Figure 114: Example Win9X/ME CrypKey Configuration

Figure 115: NT Network Configuration – Example #1

Figure 116: NT Network Configuration – Example #2

CrypKey Network Configurations

Configuration:
Application protected with CrypKey Instant.
Application uses an external license file(EXAMPLE.EXE).
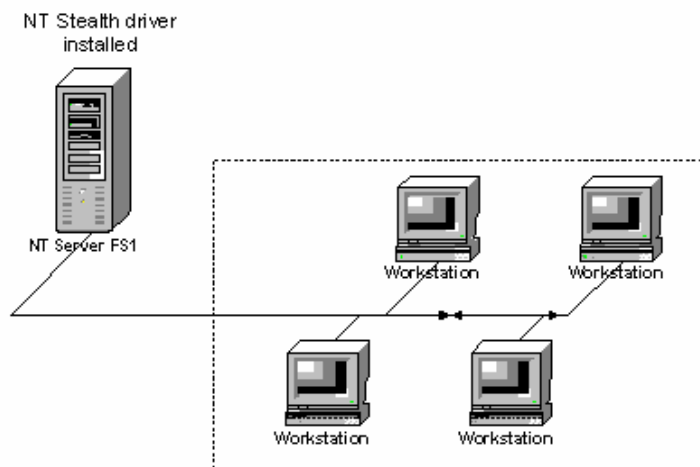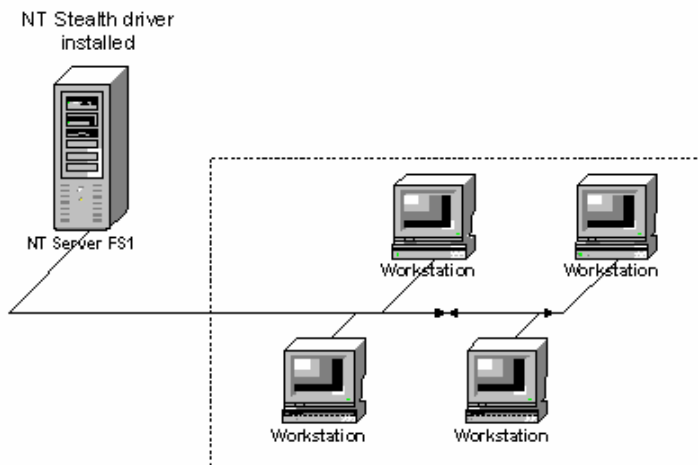Executable is installed on the CLIENT
Exe: C:\PROGRAM FILES\TEST\TEST.EXE
License installed on the server.
License: C:\PROGRAM FILES\TEST\EXAMPLE.EXE

NT Stealth driver installed

NT Server FS1

Workstation   Workstation

Workstation   Workstation
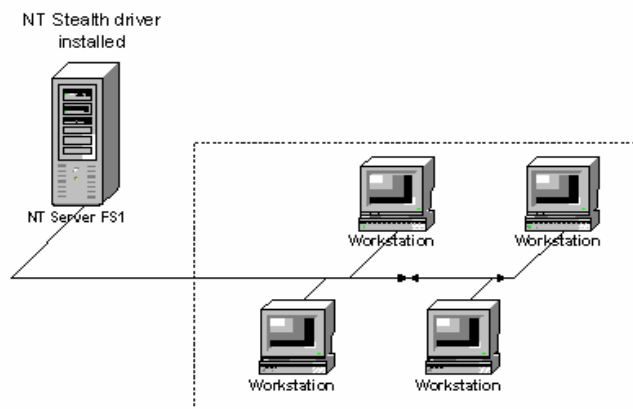
Client needs environment variable configured.
example:
LICPATH = \FS1\PROGRAM FILES\TEST\example.exe

Users have full security rights to the License directory on the server.

Executable installed on the clients.

Figure 117: NT Network Configuration – Example #3

Glossary

Learn CrypKey Instant's basic terminology.

T he following definitions for terms commonly used in this manual facilitates your understanding of the CrypKey Instant product and its protection strategies.

Automatic License

The license created automatically by CrypKey Instant when the ready-to-try feature is implemented (requires no site keys).

Developer Keys

The four keys that CrypKey issues you at purchase time, including:

1. company number
2. password number
3. master key
4. user key

When using CrypKey Instant, only Keys 3 and 4 are required.

Fixed License

A product license that is node-locked for use on the computer where it is installed. Copies of the license can be transferred to other computers, but only the computer that has the product installed can use the license.

Floating License

A product license that allows a pre-determined number of product copies to run concurrently on various client computers from a single, networked server source copy.

Level

A parameter defined for a product license. The Site Key Generator communicates the level to your product via the site key, enabling you to control how and what a particular instance of your product runs. CrypKey Instant only communicates the level to the protected product. You are responsible for implementing the actions(s) within the product based on the level.

License

Defines the authorization of a protected product. The license contains details of the authorization, including levels, options, license restriction, and license type. In physical terms, the license consists of four hidden system files that reside in the same directory location as the protected program.

Master Key

A hexadecimal number issued by CrypKey and based on your company number and product name. To use CrypKey Instant with your product, you need master and user keys (these key numbers must be typed into CrypKey Instant dialog box fields).

Option

An optional product module selection that can or cannot include a component as part of a product license. Together, the options and levels defined for your product comprise a 32-bit integer that is used as a part of the site key.

Site

In software licensing, the internal boot device (hard drive) of the computer where a protected product is installed. This is generally interchangeable with references to the computer itself.

Site Code

A site-specific hexadecimal number issued by a protected product when installed on a client's computer. The site code appears in the License Configuration dialog box of a protected product and is what your clients provide when requesting licensing changes for the product.

Site Key

A hexadecimal number based on a client site code, created by you via the Site Key Generator. The site key unlocks client software features and license restrictions.

User Key

A hexadecimal number based on your product password and issued by CrypKey. To use CrypKey Instant with your product, you need master and user keys (these key numbers must be typed into CrypKey Instant dialog box fields).