



User's Guide

By

New Technologies, Inc. (NTI)
2075 Northeast Division Street
Gresham, Oregon 97030
503-661-6912
<http://www.secure-data.com>

The NTI Secure ToolKit (ST) is a unique security tool that is used to encrypt files which contain sensitive information. It was designed primarily to help U. S. corporations comply with the security and information control requirements of the Financial Modernization Act of 1999 (Gramm-Leach-Bliley), the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act of 2002. Because its use is intended for non-technical computer users, it is very easy to use. Yet it provides a significant level of security because it relies upon the new, U. S. National Institute of Standards and Technology (NIST) tested Automated Encryption Standard (AES). It also provides corporations and government agencies with the comfort of having a secure backdoor which allows them to gain access to encrypted files when passwords are forgotten.

ST is an ideal security tool for use on portable notebook computers and it is also ideal for the secure transfer of files over the Internet. Recipients of files secured with ST also do not need a copy of the program to access the encrypted data. All they need know is the password or passphrase which was used to encrypt the file. ST provides corporate and government computer users with an alternative to programs like PGP and ST is very easy to use.

Table of Contents

I. INTRODUCTION	1
II. WHAT IS ENCRYPTION?	2
III. EVOLUTION OF PERSONAL COMPUTER SECURITY	4
IV. OVERVIEW OF NTI SECURE TOOLKIT	5
V. LICENSE STATEMENT	7
VI. DISCLAIMER OF WARRANTY	8
VII. CHOICE OF LAW	9
VIII. NTI SECURE TOOLKIT PROGRAM FEATURES	10
A. Provides Two Levels of File Access After Encryption	10
B. Handles Multiple Files	10
C. Checks for Errors	10
D. Requires Strong Passphrase (Password) Security	10
IX. DOS AND DON'TS	11
X. INSTRUCTIONS FOR USING NTI SECURE TOOLKIT	13
A. NTI SECURE TOOLKIT SETUP	13
1) Introduction	13
a) Updating Older Systems - Windows 95/98	13
2) Program Installation	14
3) Safekeeping	15
B. Using NTI Guard	16
1) Introduction	16
2) Selecting and Entering Filenames	16
3) Selecting and Entering A Passphrase	17
4) Encrypting Files	17
5) Decrypting Files	17
6) Verifying Encrypted Files	18
7) Sending Encrypted Files To A Person Who Is Not A Licensed User of ST ..	18
8) Sending Encrypted Files To A Person Who Is A Licensed User of ST	19
9) Information About NTI Guard and NTI	19

Table of Contents (Continued)

C. Using NTI Access	20
1) Introduction	20
2) Selecting Files To Decrypt	20
3) Verifying Files	21
4) Information About NTI Access and NTI	21
D. Using the Self Decrypting Archive (SDA)	22
1) Introduction	22
2) Accessing Files	22
3) Information About NTI Guard and NTI	23
E. Technical Support and Information	23

NTI Secure TookKit - User's Guide

New Technologies, Inc. (NTI)

I. Introduction

NTI Secure TookKit (ST) is a Microsoft Windows 95/98/NT/2000/XP-based security program. It quickly and easily secures the contents of files through the use of strong encryption. It does not secure Internet sessions or E-Mail message contents. ST supplements other computer and Internet security and its security focus is on computer files that contain sensitive information and data.

ST is ideal for use when the security of financial, health care, trade secret and corporate insider information is necessary and/or required by federal regulation. It is also ideal for use in government agencies to secure sensitive information. The Financial Modernization Act of 1999 (Gramm-Leach-Bliley) and the Health Insurance Portability and Accountability Act (HIPAA) require safeguards and controls over the security and privacy of consumer personal financial and health information. Additionally, the Sarbanes-Oxley Act of 2002 requires that management of public companies establish and maintain adequate internal controls concerning financial and other sensitive information. To comply with these regulations, corporations (and in some cases government agencies) must establish appropriate computer security and related controls over unauthorized access to sensitive information stored on computers. ST is an important software tool that does just that.

Today's personal computers and also the Internet were not designed to be secure. Microsoft and Intel Corporation intend to provide security in the design of future personal computer systems but such security will not be ready for years. In the meantime, corporate and government computer users are at risk when they use personal computers to store and share sensitive information.

ST was designed to **PREVENT UNAUTHORIZED ACCESS TO SENSITIVE INFORMATION STORED ON DESKTOP AND PORTABLE NOTEBOOK COMPUTERS AND TO SECURE FILE ATTACHMENTS TO E-MAIL**. ST was specifically created to fill the existing security gap until Microsoft provides secure notebook and desktop computing. ST provides an effective security control to assist corporations in securing consumer personal financial and health care data, insider information and other sensitive information at a minimal cost.

ST is not sold to the general public because it defeats computer forensics methods and tools. The sale of ST is also restricted to specific countries under U. S. export laws. Contact NTI for information about those countries that qualify for purchase of this powerful security tool.

II. What Is Encryption?

In its simplest form, encryption disguises data to make it unreadable to individuals that are not privy to the information. Encryption makes the data unreadable and decryption makes it readable. To decrypt data that has been encrypted, a password (or passphrase) or some other means of authenticating the recipient is typically required. When strong encryption is involved, as is the case with ST, the weak link is usually the password because easily guessed or simple passwords can be compromised. Therefore, simple words, names of family members, names of pets and common number patterns should not be used for passwords.

ST supports passphrases of up to 512 characters to aid the end user in the creation of a more secure passphrase. Lengthy and complex passwords, used in combination with strong encryption, provide the best possible security. Passwords/passphrases that exceed five characters in length and contain upper and lower case letters, numbers and also punctuation, provide good security for most situations. This is true when creating passwords for use with E-Mail accounts and network logons. However, you should be careful in using the same password for different accesses. For example, it is relatively easy to determine an E-Mail password or a password used within Microsoft Word or Microsoft Excel with the proper encryption breaking software, e.g., NTI's password recovery software (described at <http://www.forensics-intl.com/breakers.html>). Therefore, **if you used the same password with ST, your security could be easily compromised.**

ST provides a high level of security for sensitive information stored on notebook and desktop computers or for sensitive files transferred over the Internet as E-Mail file attachments. It provides this high level of security through the use of the NIST tested and endorsed AES (Advanced Encryption Standard) encryption algorithm with a key length of 256 bits. It is not designed to secure the contents of an E-Mail message, but protects its files that may be transferred as attachments to E-Mail messages. It can also protect files that are downloadable from Internet FTP sites. ST can provide a high level of security for Internet use by government agencies and corporations that choose to move sensitive portions of Internet communications as file attachments and file downloads.

As stated, ST relies on the AES encryption algorithm for its security. The DES (Data Encryption Standard) encryption algorithm is no longer approved by the U S Government and Triple DES is not approved beyond 2003. The U S Federal Information Processing Standard (FIPS) No. 197, dated November 26, 2001, promulgated and endorsed AES as the approved encryption algorithm for protecting sensitive (unclassified) electronic data in the United States.

Three AES encryption key lengths, i.e., 128, 192 and 256 bits, are approved by the U S Government under FIPS No. 197 and NTI has incorporated the highest 256 bit key length in the NTI Secure ToolKit. For this reason, the export of this software is restricted by the U S Department of Commerce to specific countries. Contact NTI for information about which countries are involved.

The U S National Security Agency (NSA) has conducted a review of the AES encryption algorithm and its applicability to the protection of national security information. The NSA review determined that the design and strength of all three AES key lengths are sufficient to

NTI Secure ToolKit - User's Guide

New Technologies, Inc. (NTI)

protect classified U S government information up to the 'SECRET' level. Their review concluded that only the AES 256 bit key length was strong enough to protect classified information at the 'TOP SECRET' level. This is the level of security provided by the NTI Secure ToolKit.

However, U S government agencies should seek approval from NSA before they use the NTI Secure ToolKit to protect national security information. Government agencies seeking to use the NTI Secure ToolKit for the protection of mission critical information, but non-classified, should request a review by NIST in accordance with the requirements of FIPS 140-2.

III. Evolution of Personal Computer Security

The worldwide acceptance of personal computers and the Internet has been a mixed blessing. IBM (and Microsoft, for that matter) did not anticipate the immediate popularity of the IBM PC, which was first introduced in 1981. The DOS operating system installed on the original personal computers was never intended for commercial and government use and was not designed with a data security foundation. To maintain compatibility with the early versions of DOS, upgrades to the original operating system could not adequately address security needs and issues. As a result, current desktop PCs and notebook computers lack adequate security. Many of these computers are used as tools to conduct financial transactions and to store trade secrets and sensitive medical, financial and employment information. Many of these computers are also connected to the Internet to send and receive E-Mail and to browse the wealth of information on the World Wide Web. Other personal computers are used by government agencies to conduct sensitive government and military business. Much of this sharing of data is done with little or no security involved. A key component in overcoming this lack of security is to prevent unauthorized access to files through the use of ST.

Microsoft intends to remedy the security weaknesses in its personal computer operating systems. Securing such operating systems will likely take years because there are millions of personal computers in use around the world that currently lack appropriate security. ST provides a high level of security for targeted computer files that contain sensitive data until such time as personal computers are made secure. The security afforded by ST is ideal for Internet transfers of sensitive files and for securing sensitive information on desktop and portable notebook computers. **THE POTENTIAL THEFT OF AN EXECUTIVE'S NOTEBOOK COMPUTER SHOULD BE THE CAUSE OF CONCERN FOR EVERY PUBLIC CORPORATION** because such computers typically contain all of the corporate "secrets". It is generally believed by security experts that having files unsecured on a notebook may endanger any claims of protecting corporate information, making compensation for theft of trade secrets all but impossible. File encryption security can help alleviate many of these concerns.

IV. Overview of NTI Secure ToolKit

ST is easy to use, very compact, and relies upon strong encryption to protect sensitive computer files. Selected files are encrypted and decrypted through the use of a user-defined password/passphrase. ST relies on the NIST tested AES encryption algorithm with a 256 bit key length that has been determined by the U.S. Government to be suitable for the security of sensitive information. AES encryption is much stronger than the Data Encryption Standard (DES) and Triple DES encryption algorithms that were previously authorized by the U.S. Government for use in commercial trade. The AES encryption algorithm has also been thoroughly tested and reviewed by universities and government agencies around the world. It is very powerful and should provide high levels of computer security for years to come.

ST encrypts sensitive files stored on desktop and portable notebook computers and secures files transferred over the Internet using a program referred to in this User's Guide as "NTI Guard". With ST, selected clients and employees can post secure files on Internet FTP sites for download. ST enables secure files to be transmitted through any E-Mail system that allows file attachments. The recipient only needs the password to gain access to the files; he/she does not need to have a copy of the ST software. Because of this feature, ST is easier to use than programs like PGP because it does not rely upon complex storage procedures, security procedures, and other mechanisms that inhibit use by non-technical computer users. As NTI's President and CEO, Michael R. Anderson says, "ST is so easy to use that even corporate CEOs can use it on their notebook computers without a training course."

ST is unique because it has a setup program that allows you (and only you) to access encrypted files when you or one of your computer users have forgotten or lost the password. **THIS ACCESS IS ESTABLISHED THROUGH A COMPANION PROGRAM TO NTI GUARD, CALLED "NTI ACCESS"**. NTI Access is especially helpful in the event of the death or termination of a key employee. The special recovery feature of NTI Access does not compromise the security or strength of the encryption. It is very important for you to know that this special access does not extend beyond the licensed user of ST. **You control this special backdoor program and even NTI can't help you break the encryption** without the custom program that you create during setup and that only you maintain.

NTI does not make ST available to the general public because its use could negatively affect our many law enforcement computer forensics specialist clients. If you need to break the security of other security products, NTI makes the best and most powerful password recovery software available for sale to its clients. Information about NTI's password recovery software can be found on the Internet at <http://www.forensics-intl.com/breakers.html>.

Licensed ST users can share encrypted files with others who do not have ST. This feature is referred to in this User's Guide as Self Decrypting Archive (SDA). With SDA, sensitive data can be distributed over the Internet to others who can easily gain access to the data through use of the passphrase/password which was used to encrypt the file. The passphrase can be distributed on a need-to-know basis by several means, e.g., separate E-Mail communications, fax distributions and/or through telephone transmissions. Be aware that these secure files become small security programs by themselves, and some E-mail systems will not accept program files as attachments. In these cases, you may want to zip the attachment or rename the file.

NTI Secure TookKit - User's Guide
New Technologies, Inc. (NTI)

ST is the strongest commercial encryption software available because it relies upon the U. S. Government tested and approved AES encryption. ST is also priced to compete with any similar product in the marketplace. Site licenses are also available for government agencies, financial institutions, medical facilities, law firms and any other legitimate business or government entity where security of private information is a priority. Because of the high security provided by ST, its export outside the United States is restricted to specific countries by law.

V. License Statement

The "NTI Guard" and the "NTI Access" programs contained within the NTI Security ToolKit are owned by New Technologies Armor, Inc. (NTI) and are licensed for use on a specific computer system. These programs are not licensed to be shared or copied for use by others. The NTI Guard and NTI Access programs are not shareware and, therefore, are not licensed for distribution other than by NTI or its authorized dealers and distributors. These programs can be licensed for use on more than one computer through a site license that can be obtained from NTI.

The Self Decrypting Archive (SDA) programs created by you when using ST are also owned by NTI, and they are licensed for use on multiple computer systems and multiple computer users of your choosing. The encrypted data stored within the SDA programs, is not owned by NTI and remains your exclusive property. For purposes of clarity, only the encryption/decryption software is the property of NTI and therefore it is covered by the license. When properly created by NTI Guard, the SDA programs are licensed to be shared or copied for use by others of your choosing. However, you are not authorized or licensed to share the NTI Guard and NTI Access programs.

Any alteration of this User's Guide or the referenced software nullifies any licensing agreements between the user and NTI. Violations of this licensing agreement constitute a violation of your license to use the software and may constitute a criminal and/or civil violation of United States and/or international copyright laws. NTI will pursue such violations to the fullest extent of the law.

VI. Disclaimer of Warranty

NTI has made every effort to verify the accuracy of this program. However, ST is sold and distributed "as is" without any warranty of any kind. In no event shall NTI, the authors, and/or authorized dealers and distributors be liable or responsible for any problems that could arise because of defects in the program or from the operation of the program. **TEST THIS PROGRAM THOROUGHLY BEFORE PUTTING IT INTO USE! MAKE BACKUP COPIES OF CRITICAL DATA IN A NON-ENCRYPTED FORM and make backups of the software after setup. Remember, NTI cannot help you break the security afforded by this software.**

VII. Choice of Law

This statement and the entire contents of this User's Guide shall be construed, interpreted, and governed by the laws of the state of Oregon and/or the courts of The United States of America, Judicial District of Oregon. The user of this program agrees that any legal actions brought will be filed in those respective jurisdictions.

VIII. NTI Secure ToolKit Program Features

ST is user friendly and very secure when dealing with sensitive data. You do not need to be a computer expert to use ST and the program has the following features:

A. Provides Two Levels of File Access After Encryption

- You can access encrypted files with the NTI Guard program using the assigned password or passphrase.
- The NTI Access program allows you to access encrypted files if you have forgotten or lost the assigned password or passphrase.

B. Handles Multiple Files

The program allows you to select one or more files to encrypt in a single session. Files can be easily located and tagged through a minimum of keystrokes. Further, all files in a given folder can be selected if you desire.

C. Checks for Errors

Every processing step involves complete error checking. When errors are discovered, you will receive a warning message describing the nature of the error and possible remedies.

D. Requires Strong Passphrase (Password) Security

Your password or passphrases used to encrypt files are not stored or maintained within the ST program modules. This makes the breaking of the encryption very difficult for a hacker or data thief. ST also requires a minimum length for your passphrase along with certain specified letters and characters or numbers. Such requirements help enforce the use of strong passwords and passphrases. As mentioned previously, passwords are usually the weakest link in computer security and ST helps strengthen this weak link in the security process.

IX. Dos and Don'ts

ST is an easy-to-use program. However, we have included some specific “dos” and “don'ts” in this section of the User's Guide that will help you maintain the strength of the security built into the design of ST.

- **DO NOT USE SIMPLE PASSWORDS OR PASSPHRASES BECAUSE THEY CAN BE EASILY GUESSED OR BROKEN.** The passphrase you choose greatly affects the security of the files you are encrypting. Your passphrase should not consist of your initials, first or last name, maiden name, children's names or any other personal information that someone can easily determine about you through social engineering. To increase the level of passphrase security, ST requires that the passphrase be a minimum of five characters in length and can be up to a maximum of 512 characters in length. ST also requires the passphrase to have at least one upper and one lower case character, and at least one number or symbolic/punctuation character, e.g. a comma, asterisk, quotation mark, etc.
- **DO NOT LEAVE WRITTEN PASSWORDS OR PASSPHRASES NEAR YOUR COMPUTER OR IN A PLACE WHERE THE PASSPHRASES CAN BE EASILY FOUND.** If you need to write down a passphrase, you should place the written copy in a secure place.
- **STORE THE “NTI ACCESS” PROGRAM IN A SECURE LOCATION SEPARATELY FROM THE “NTI GUARD” PROGRAM.** We recommend you save the NTI Access program to a floppy disk and store the disk in a locked cabinet or safe. Your security for all NTI Guard encrypted files will be compromised if there is unauthorized access to the NTI Access program because it can be used to access all of your files which were encrypted with the NTI Guard program.
- **DO NOT DELETE OR LOSE THE “NTI ACCESS” PROGRAM.** If you do, you will not be able to decrypt the files without knowing the password or passphrase that was used to encrypt the files.
- **ALWAYS SAVE A BACKUP COPY OF THE ORIGINAL DATA FILE(S).** There is always a possibility that encrypted files may be corrupted, altered or damaged due to power surges, machine failure, etc. Encrypted files may also be corrupted during long-term storage or transfer over the Internet. When encrypted files have been damaged, they cannot be decrypted and you must refer back to a backup copy of the important data.
- **ADD VERSION NUMBERS OR IDENTIFIERS TO THE NTI ACCESS AND NTI GUARD PROGRAM NAMES IF YOU CHOOSE TO CONFIGURE MULTIPLE COPIES OF THE PROGRAMS.** Only the NTI Access program created at the same time as the NTI Guard Program(s) will decrypt files created by the companion program. This means that you will not be able to decrypt files using NTI Access unless you use the NTI Access program that was created at the exact same time as the NTI Guard program(s). The creation process takes place when you first initialize the ST program. To rename the files, right click on the icon, select “Rename” on the menu and then

NTI Secure TookKit - User's Guide

New Technologies, Inc. (NTI)

modify the name, such as “NTI Guard V1” and NTI Access V1” for example.

- **DO NOT ATTEMPT TO ALTER THE PROGRAM.** Such attempts could result in the program becoming inoperable. Further, modifications to this program in any way nullify your license to use this program.

X. Instructions for Using NTI Secure ToolKit

A. NTI Secure ToolKit Setup



1) Introduction - NTI Secure ToolKit is easily installed on Microsoft Windows NT4, Windows 2000 and Windows XP. It can also be installed on Windows 98 and 95. The setup program is identified by the icon in the left margin. When the setup program is executed it will create other programs that are unique to your license and those other programs are described below.

a. Updating Older Systems (Windows 95/98) - For older versions of Windows 98 and Windows 95, an updated Microsoft system file, **advapi32.dll**, may be required. If you are unable to install NTI Secure Toolkit using the instructions under **Program Installation** in section 2 below, please follow the instructions immediately below to install the updated Microsoft dll file.

- ◆ Create a bootable floppy diskette by doing the following:
- ◆ Insert an unused floppy diskette into drive A of the computer (If you do not have an unused floppy diskette, **MAKE SURE THAT THE FLOPPY YOU USE DOES NOT HAVE IMPORTANT DATA OR INFORMATION STORED ON IT** because the information will be erased by following the procedures below.).
- ◆ Double click on the “My Computer” icon on your computer screen.
- ◆ Right click on “3 ½ Floppy (A:)”.
- ◆ Click on “Format”.
- ◆ Place a check on “Quick (Erase)” (This will erase the contents of the floppy to allow for enough room to copy **advapi32.dll** on the floppy.).
- ◆ Place a check on “Copy System Files”.
- ◆ Click on “Start”.
- ◆ The operating system will now create a bootable floppy diskette.
- ◆ Click on “OK” to close the “Format” window.
- ◆ Go to www.dll-files.com, enter **advapi32.dll** in the “search” box, and click “go”. Follow the instructions to download **advapi32.dll** to the bootable floppy diskette in drive A.
- ◆ Click on the “Start” box in the lower left-hand corner of the computer screen.
- ◆ Click on “Programs” and then click on “Accessories”.
- ◆ Click on “Notepad”.
- ◆ Type the following: **copy advapi32.dll c:\windows\system** in Notepad. Remember to put a space between “copy” and “advapi32.dll” and “advapi32.dll” and “c:\windows\system”.
- ◆ Click on “File” in the upper left-hand corner of Notepad and then click on “Save As”.

NTI Secure ToolKit - User's Guide

New Technologies, Inc. (NTI)

- ◆ Save the file with the name **A:\autoexec.bat** in Notepad.
- ◆ Exit Notepad.
- ◆ Click on the “Start” box in the lower left hand corner of the computer screen.
- ◆ Select “Shutdown”, then select “Restart” and then click “OK”.
- ◆ The computer should restart in a DOS mode and automatically copy the **autoexec.bat** file. If your computer does not restart in a DOS mode, but restarts in a Windows mode, it means that the computer's CMOS settings will need to be modified to allow the computer to copy the floppy disk in Drive A. Contact IT Support within your organization to modify your computer's CMOS settings or to help you complete the installation.
- ◆ When the computer has finished copying the **autoexec.bat** file, the computer screen will indicate, “1 file(s) copied”.
- ◆ Remove the floppy from Drive A.
- ◆ Restart the computer by simultaneously pressing the keys: Ctrl, Alt, and Delete.
- ◆ The computer will then restart in a Windows mode.
- ◆ The computer is now updated for **advapi32.dll** and you can follow the instructions for installing NTI Secure ToolKit under **Program Installation** in section 2) below.

2) Program Installation - Once you have received your licensed copy of ST, you should save it to a new folder before running the program. **DON'T RUN IT IN YOUR DOWNLOAD E-MAIL FOLDER!**

- The setup program will be easy to identify because the file name will include a number. It will be named with a name that includes your registration number, e.g. the setup program file will be named ST00587.EXE, if your registration number is 00587 then. The setup program can also be identified by the program icon shown in the upper left hand corner of this section. As stated above, **DON'T RUN THE SETUP PROGRAM FROM YOUR E-MAIL FOLDER. COPY IT TO ITS OWN DIRECTORY.**
- To run ST Setup, simply double click on the setup icon (A picture of the icon is shown in the upper left hand corner of this section.). The program will make a quick check for the existence of the NTI Guard and NTI Access programs in the folder that you are in. If these files do not exist in the folder, a new (matched) pair of NTI Guard and NTI Access files will be created.
- If you purchased more than one license of NTI Secure ToolKit, the setup program will create multiple NTI Guard program files, depending on the number of licenses you have purchased, along with one (1) NTI Access program file. As an example, if your registration number is 00587 and you had purchased a license for five (5) copies, the setup program would name the five (5) NTI Guard program files “NG00587A, NG00587B, NG00587C, NG00587D, NG00587E”, and the matched NTI Access program file would be named “NA00587”.

NTI Secure ToolKit - User's Guide

New Technologies, Inc. (NTI)

- After successful completion, a notice message will appear on the screen, which says: *“The NTI Secure ToolKit applications have been created. Keep NTI Access.exe in a safe place and use NTI Guard.exe.”*
- See the “Dos and Don'ts” (Section IX) of this User's Guide for recommendations if you wish to use multiple versions of NTI Guard and NTI Access.
- Do not attempt to alter the program(s) in any way.

3) Safekeeping

- We **STRONGLY RECOMMEND YOU STORE THE NTI ACCESS PROGRAM IN A SAFE PLACE** after it has been created through the setup process. NTI Access contains key information to unlock any file encrypted with the companion NTI Guard program(s). Remember that the simultaneously created NTI Guard program(s) and NTI Access program are uniquely matched programs that were created at the time you first ran the ST setup program.
- Should NTI Guard or NTI Access already exist in the same folder, Setup will not install the programs and will display the message *“NTI Access and/or NTI Guard have been installed in this folder already. Please remove them if you want to make a new pair of applications.”*
- **If you already have an existing NTI Access program file set up on your computer, DO NOT DELETE THE PROGRAM FILE** because it has the key archive for files encrypted by its companion NTI Guard program(s). You will be unable to access the previously encrypted files if you have forgotten or lost the passphrase without the matched NTI Access program file.

B. Using NTI Guard

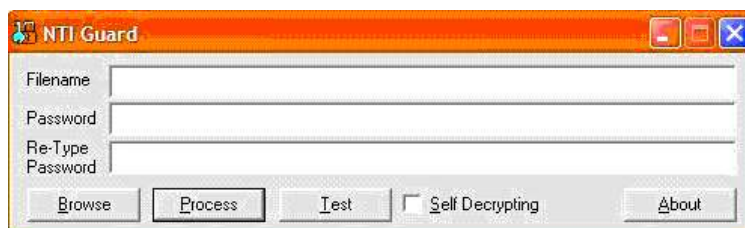
1) Introduction - NTI Guard can be used to encrypt, decrypt, and test an encrypted file, as explained below. You can also create a Self Decrypting Archive (also discussed below) that allows you to send the encrypted file(s) to another party who may not have ST.



- By double clicking the NTI Guard icon (A picture of the icon is identified on the immediate left of this paragraph), the program displays a temporary screen announcing the name of the program and the appropriate copyright information. The NTI Guard window is then displayed as shown below.

2) Selecting and Entering Filenames

- To choose the files to be encrypted/decrypted, select the “Browse” button to display the standard Windows interface. This interface displays a listing of the available files in the folder along with the path information of the current folder. When using this Windows interface, use the mouse to click on the file. If you want to select multiple files, hold the Control (Ctrl) key down at the same time you select the files with the mouse. Click on the “Open” button in the Windows interface and the selected file(s) are automatically placed in the “Filename” box in the NTI Guard window.
- If you wish, you can manually enter the name of the file to be encrypted in the “Filename” box. You must enter the complete name of the file that has been saved on your computer, including any extension to the file, such as: “.doc”, “.txt”, and “.xls”. The filename must also include quotation marks (“) before and after each filename. For example, if you saved a Microsoft Word document under the filename, “XYZ Company”, Word would have saved the file as “XYZ Company.doc”. In this example, “XYZ Company.doc” must be entered in the “Filename” box.
- If you have multiple files to be encrypted, add a space between each of the filenames in the “Filename” box. If the filenames have multiple words with spaces between them, you must include quotation marks before and after each filename when entering the filenames in the “Password” box.



3) Selecting and Entering A Passphrase

- Once a filename is selected, you must enter a passphrase in the "Password" box.
- **The passphrase is required to be at least five characters, with at least one lower case, one upper case, and one number or special character.** Special characters can be entered from the keyboard and they would include the following: !@#\$%^&*()_+|=|~\[]\{|};:'",./<>?). An example of an acceptable password would be, "CatEye\$" because it contains both upper case, lower case and one special character. It is also more than five characters in length. If your password does not meet these requirements, after you have clicked on the "Process" button, a dialogue box will state: *"The password is not valid. It must be at least five characters, contain at least one upper and lower case character and at least one numerical or symbolic character."* Select a new passphrase that includes the required parameters in the "Password" and "Re-Type Password" boxes. To some individuals this might seem overly restrictive but weak passwords are always the weakest link to any element of computer security.
- You must enter the same passphrase in the "Password" and "Re-Type Password" box or you will not be allowed to proceed, and an "Error" dialogue box will appear which says: *"Passwords do not match."*
- When typing and re-typing the passphrase, the program will enter asterisks (*) for the passphrase so you will be unable to see the typed passphrase. Since the passphrase can be up to 512 characters long, you may wish to use the "cut and paste" method by cutting the passphrase from a different document and then placing it into the "Password" box and the "Re-Type Password" box. Caution: anyone who can see your screen can see your passphrase if you use the cut and paste method.

4) Encrypting Files

- When you click on the "Process" button, NTI Guard will attempt to encrypt the file(s). If the passphrase is determined to be acceptable and the process was completed successfully, a dialog box will appear on the screen which states: *"Filename: The file has been successfully encrypted."* Select "OK" to close the dialog box.

5) Decrypting Files

- You can decrypt the file(s) at any time by entering the filename(s) in the "Filename" box and typing the passphrase in the "Password" box. You do not need to re-type the passphrase in the "Re-Type Password" box to decrypt the selected file(s).
- Click on the "Process" button and the selected file(s) will be decrypted and a

NTI Secure ToolKit - User's Guide

New Technologies, Inc. (NTI)

dialogue box will appear which states: "*Filename: The file has been successfully decrypted.*"

- You will not be able to decrypt an encrypted file if it has been modified or it has been damaged. If the file has changed, a dialogue box will appear after clicking on the "Process" button which states: "*Filename: The hash of the file is not correct. The file was modified.*"
- If you have forgotten or lost the passphrase, use NTI Access (discussed below) to gain access to the encrypted file(s).
- If you are having trouble when typing in the passphrase in the "Password" box, please review the procedures above under the section "Selecting and Entering A Passphrase".

6) Verifying Encrypted Files

- The "Test" button in the NTI Guard window above should be used before you attempt to decrypt the file to determine whether the encrypted file has been modified or damaged. This can happen when files are transferred over the Internet. If a file has been unknowingly changed, altered, or damaged you will not be unable to access the encrypted file.
- To verify that an encrypted file has not been changed; enter the filename in the "File Name" box, type the passphrase in the "Password" and "Re-Type Password" boxes and then click on the "Test" button.
- If the file has not changed, a dialogue box will appear on the screen which states: "*Filename: The file is intact and has not been altered.*"
- If the file has been changed, a dialogue box will appear on the screen which states: "*Filename: The hash of the file is not correct. The file was modified.*"

7) Sending Encrypted Files To A Person Who Is Not A Licensed User of ST

- Check the "Self Decrypting" box when you want to send encrypted files to another party who is not a licensed user of ST. **THIS BOX MUST BE CHECKED BEFORE** you select the "Process" button.
- Enter the filename in the "Filename" box.
- Place a check in the "Self Decrypting" box.
- Enter the passphrase in the "Password" and "Re-Type Password" boxes.

NTI Secure ToolKit - User's Guide

New Technologies, Inc. (NTI)

- Select the “Process” button.
- You will notice that the file now has the “Self Decrypting Archive” (SDA) icon attached to it (See “Using the SDA” below for identification of the icon). If you do not see the SDA icon attached to the file, the person receiving the file will not be able to decrypt the file(s) if he/she does not have a licensed copy of ST. Repeat the steps above if the icon is not attached to the file.
- Attach the selected file(s) to an E-Mail and send it to the user, give it to the user via some computer storage media, or move it to a shared folder.
- Do not place the passphrase in the same location as the encrypted file. Send the passphrase separately to the user using a different method if possible.
- Please refer to “Using the SDA” section below for an explanation of how the user receiving the encrypted file gains access to it.

8) Sending Encrypted Files To A Person Who Is A Licensed User of ST

- You do not need to check the “Self Decrypting” box if you are sending an encrypted file to a person who has a licensed copy of ST.
- Follow the procedures for encrypting a file under “Using NTI Guard” above, except that you do not need to check the “Self Decrypting” box.
- Attach the selected file(s) to an E-Mail and send it to the user, give it to the user via some computer storage media, or make it available on the LAN (Local Area Network) or Internet.
- Notify or send separately to the user the passphrase that the user will need to decrypt the file.
- The party receiving the encrypted file simply saves the file to a folder, opens NTI Guard program, enters the full filename in the “Filename” box, types the passphrase in the “Password” and “Re-Type Password” boxes and then clicks on the “Process” button. The file should now be decrypted. A dialogue box will appear which states: *“Filename: The file has been successfully decrypted.”*

9) Information About NTI Guard and NTI - Click on the “About” button to display licensing information about NTI Guard and NTI. Information about NTI and the program can also be found on the Internet at <http://www.secure-data.com>.

C. Using NTI Access



1) Introduction - NTI Access is the archive key version of ST that allows you to access files encrypted by NTI Guard. We know of no other encryption tool that provides the benefits of such a companion program for gaining access to encrypted files.

- To run NTI Access, double click on the icon (See display in the upper left-hand corner of this paragraph.). After briefly displaying the splash screen, the main window will appear as in the figure below.



2) Selecting Files To Decrypt

- Enter the filename of the encrypted file(s) that you want to access in the "Filename" box.
- For multiple files, add a space between each of the filenames. If the filenames have more than one word with spaces between them, you must include quotation marks before and after each filename.
- You can also select the "Browse" button to display the standard Windows interface. This interface displays a listing of available files in the folder along with the path information of the current folder. When using this Windows interface, hold the Control (Ctrl) key down at the same time to select multiple files. Click on the "Open" button in the Windows interface and the selected file(s) are automatically placed in the "Filename" box in the NTI Access window.
- You will notice that there is no place for a password in this program. That is because the encryption keys to the file(s) are already embedded in the program.
- Once you select a file(s), click on the "Process" button and a status window will appear. If the file is encrypted with the matching NTI Guard program and the encrypted file has not been changed, the file will be decrypted. The filename will not change; however the file size and date information will be updated to reflect the new file. The dialogue box appearing on the screen will state: *"Filename: The file has been successfully decrypted."*
- If the file has been changed, damaged or altered, or you have attempted to access a file using an NTI Access program that was not paired to the NTI Guard program(s) used to encrypt the file, you will not be able to gain access to the file. In such a case and after clicking the "Process" button, a dialogue box will appear

NTI Secure TookKit - User's Guide

New Technologies, Inc. (NTI)

which states: *“Filename: Either the file has been changed or an incorrect version of the NTI Access program is being used. Please see the Manual for instruction on use of the NTI Access program.”* Please refer to the “Dos and Don’ts” (Section IX) of this User’s Guide for using multiple versions of NTI Guard and NTI Access. Always use the correct companion version of NTI Access program when decrypting a file using the NTI Access program.

3) Verifying Files

- The “Test” button is used to determine if the encrypted file has been modified or damaged after it was encrypted. You cannot access the encrypted file with NTI Access if the file has been changed, damaged, altered or if you are using a NTI Access program which is not paired with the NTI Guard program used to encrypt the file.
- To verify that the file has not been changed, enter the filename.
- Click on the “Test” button and a dialog box will open which will provide you with the status of the file. If the file has not changed, the dialog box will state: *“Filename: The file is intact and has not been altered.”*
- If the file has been changed, damaged or altered, or you have attempted to access a file using an NTI Access program that is not paired with the NTI Guard program that encrypted the file, the following dialogue box will appear after clicking the “Test” button: *“Filename: Either the file has been changed or an incorrect version of the NTI Access program is being used. Please see the Manual for instruction on use of the NTI Access.”* Please refer to the “Dos and Don’ts” (Section IX) of this User’s Guide for using multiple versions of NTI Guard and NTI Access.
- Click the “OK” button on the dialog box and you will return to the NTI Access window.

4) Information About NTI Access and NTI

- Click on the “About” button to display information about NTI Access and NTI. Information can also be found about the program and NTI on the Internet at <http://www.secure-data.com>.

D. Using the Self Decrypting Archive (SDA)



1) Introduction - The Self Decrypting Archive (SDA) allows you to share NTI Guard encrypted files with others who do not have a licensed copy of ST. An SDA is created when using NTI Guard by clicking on the “Self Decrypting” box and following the instructions under “Using NTI Guard” program above. The SDA will have the same filename as the encrypted file with “.exe” appended to the filename.

2) Accessing Files

- If you send the encrypted file as an E-Mail attachment, the user should save the file attachment, noting the location where the file is saved.
- The user should then open the Windows Explorer and move to the saved location. At this location, the icon appearing in the upper left-hand corner of the introductory paragraph of this section will appear. By double clicking on the icon, a message box is displayed which reads *“Extracted the file (Name and location of the file) from the self decrypting archive (Name and location) successfully. Enter the password and click ‘Decrypt’ to get the original file back. Simply click ‘Cancel’ if all you want is the extracted encrypted file.”*
- The “NTI Guard Self Decrypting Archive” window will now appear (See below).
- The user should enter the passphrase in the “Password” box.
- If the file is E-Mailed to the user, the passphrase should be delivered to the user in a separate E-Mail or ideally using another form of communication.
- The user should double click the “Decrypt” button. The file is then decrypted and the file is saved in the original format in which it was created, such as Word, Excel, Corel, etc. A dialogue box will appear which states: *“Filename: The file has been successfully decrypted.”*
- The user should now simply double click on the unencrypted file to open the file.



- There may be a possibility that the same filename exists on the user's computer as the encrypted filename. In this situation, when the user double clicks on the SDA icon, a dialog box will appear indicating with a “yes” or “no” whether the user

NTI Secure ToolKit - User's Guide

New Technologies, Inc. (NTI)

wants the existing file to be overwritten or not.

- If the user selects “No”, a “Save As” dialog box will appear and the user should enter a new filename or different location for the encrypted file. If a new filename is chosen, make sure the file extension “.exe” is added to the new file name.
- If the user clicks “yes”, the existing file on the computer is overwritten with the encrypted file. The “NTI Guard Self Decrypting Archive” window will then appear as previously explained.
- If you click on the “Cancel” button before successfully decrypting the file, the program saves the encrypted file to the folder. The encrypted file also remains attached to the SDA icon. Simply delete the encrypted file so that only the executable file (with the icon at the top of this section) remains. Then double click on the SDA icon. The “NTI Guard Self Decrypting Archive” window will again appear. Follow the previous steps for decrypting other files as explained in this section.
- Once the user has successfully decrypted the file, the user may wish to delete the SDA. This can be done by right clicking the mouse on the SDA icon and then selecting “Delete”.

3) Information About NTI Guard and NTI

- Click the “About” button to display information about NTI Guard and NTI. You can also find information about this program and NTI on the Internet at <http://www.secure-data.com>.

E. Technical Support and Information

The NTI team sincerely hopes that you will enjoy using this security tool kit. If you have questions, comments or problems, **contact NTI after reading this User's Guide**. For that purpose you can contact NTI via e-mail at support@forensics-intl.com or by phone at 503-661-6912. Information and articles about security and computer forensics related information can also be found on the Internet at <http://www.forensics-intl.com/info.html>. Current happenings at NTI be found at <http://www.forensics-intl.com/whatsnew.html>.