

TREK CRYPT USER GUIDE



August 2025

Approved for Public Release; Distribution is Unlimited.

TABLE OF CONTENTS

<u>PARAGRAPH</u>	<u>PAGE</u>
1 Welcome.....	1
1.1 Getting Started	1
2 Technical Support.....	1
3 Introduction.....	1
4 Overview of the User Interface	1
4.1 Main Window	1
4.2 Menus.....	2
5 Quick Start Guides	3
5.1 How to Generate a Public and Private Key	3
5.2 How to Generate an Unwrapped and Wrapped Key	3
6 Details.....	4
6.1 Main Window Key Information Area	4
6.2 Application Messages	6
6.3 Application Settings	8
7 FAQ and Troubleshooting	9

FIGURES

<u>FIGURE</u>	<u>PAGE</u>
Figure 1 Main Window	2
Figure 2 Main Window Key Information Area	4
Figure 3 Messages Dialog	7
Figure 4 Configure Messages Dialog	7
Figure 5 Clear Messages Dialog.....	8

1 Welcome

The Telescience Resource Kit (TReK) is a suite of software applications and libraries that can be used to monitor and control assets in space or on the ground.

The TReK Crypt application provides the capability to create cryptography keys that can be used with TReK applications that provide cryptography services.

1.1 Getting Started

Start with the Introduction which provides an application overview. Next, try the Quick Start Guides for “How Tos” for common functions. For help with details, reference the Details section. See the FAQ and Troubleshooting section for helpful hints and solutions to the common “gotchas”.

2 Technical Support

If you are having trouble installing the TReK software or using any of the TReK software, please contact us for technical assistance:

E-Mail: trek.help@nasa.gov

Messages sent to this address are automatically forwarded to the TReK team.

The HOSC Help Desk (256-544-5066) can provide assistance as needed and is available 24x7.

3 Introduction

The TReK Crypt application provides the capability to generate cryptography keys that can be used with TReK applications that provide cryptography services. For more information about TReK cryptography services please see the TReK Concepts document.

4 Overview of the User Interface

4.1 Main Window

The main window contains several areas as shown in Figure 1. The Message area is a dock window that you can float or dock. To float a dock window, use your left mouse button to click and hold the title area while dragging the window to another area of the screen. To dock, use the title bar to drag the dock window over the main window and drop.

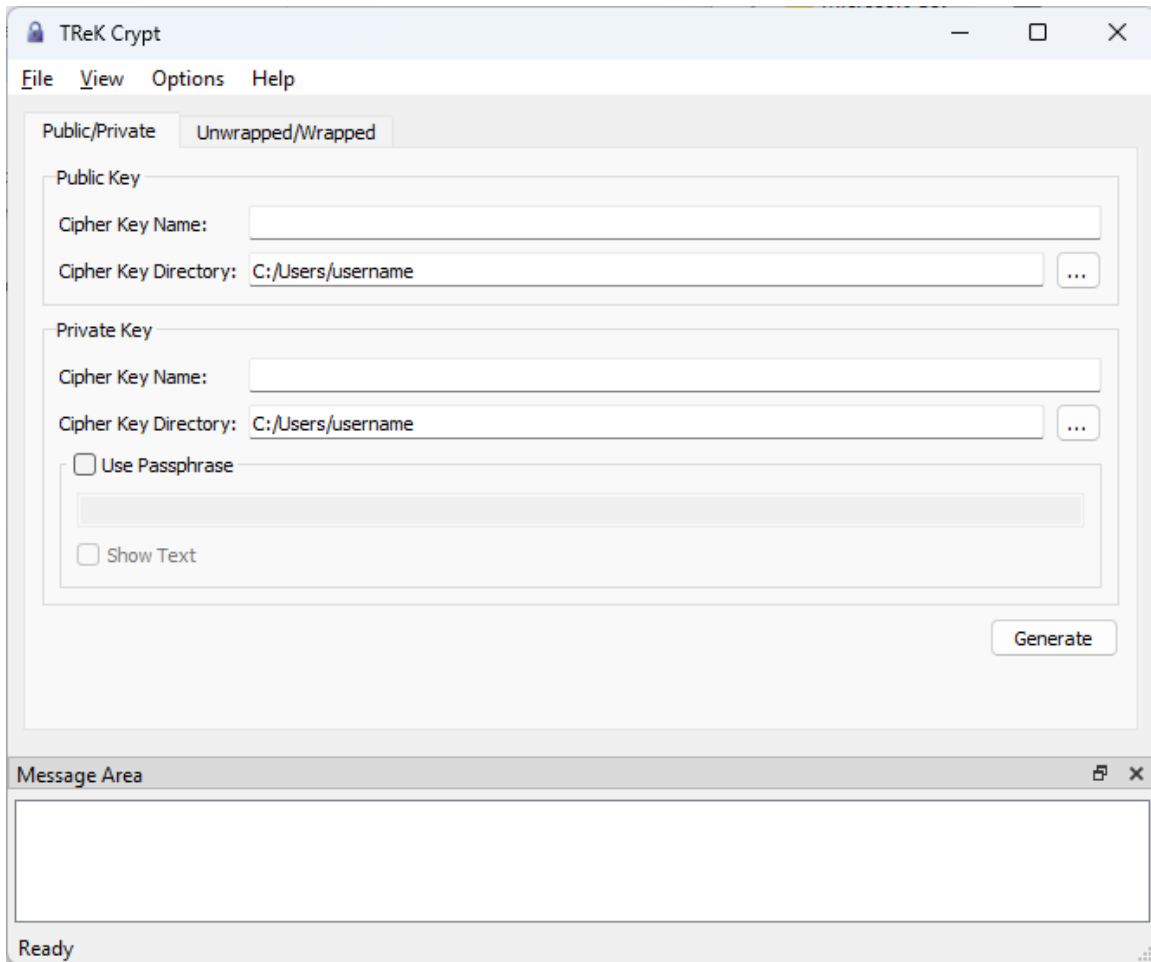


Figure 1 Main Window

Key Information Area

The Key Information area is used to enter information about cryptography keys and to generate the keys.

Message Area

The Message Area displays important status and error messages. The message area can be cleared using the View menu.

4.2 Menus

The application menus are File, View, Options, and Help. Each of these menus is described in more detail below.

File Menu

The File menu provides the capability to exit the application.

View Menu

The View menu provides the capability to clear the main window message area and show and hide different areas in the main window.

Options Menu

The Options menu provides access to the Messages dialog. The Messages dialog displays application messages.

Help Menu

The Help menu provides access to on-line help and application version information.

5 Quick Start Guides

This section provides “How Tos” for common functions.

5.1 How to Generate a Public and Private Key

The following steps describe the minimum necessary to generate a public and private key.

1. Select “Public/Private” tab to choose this encryption scheme.
2. In the main window Public Key box fill out the Cipher Key Name and Cipher Key Directory fields. The Cipher Key Directory will default to your home directory.
3. In the main window Private Key box, fill out the Cipher Key Name and Cipher Key Directory fields. The Cipher Key Directory will default to your home directory. If you wish to use a Passphrase, check the “Use Passphrase” checkbox, and enter the passphrase in the field provided. The passphrase will not be displayed in the clear. If you wish to display it in the clear, you can check the “Show Text” checkbox.
4. Push the Generate button to generate the keys.

Note: If you need to generate peer keys just repeat this process.

5.2 How to Generate an Unwrapped and Wrapped Key

The following steps describe the minimum necessary to generate an unwrapped and wrapped encryption key.

1. Select “Unwrapped/Wrapped” tab to choose this encryption Scheme.
2. In the main window Unwrapped Key box fill out the Cipher Key Name and Cipher Key Directory fields. The Cipher Key Directory will default to your home directory.
3. In the main window Wrapped Key box, fill out the Cipher Key Name and Cipher Key Directory fields. The Cipher Key Directory will default to your home directory. If you wish to use a Passphrase, check the “Use Passphrase” checkbox, and enter the passphrase in the field provided. The passphrase will not be displayed in the clear. If you wish to display it in the clear, you can you check the “Show Text” checkbox. Choose the Cipher Class.
4. Push the Generate button to generate the keys.

6 Details

This section covers various application details.

6.1 Main Window Key Information Area

The Main Window Key Information Area is shown in Figure 2. Each field is described below.

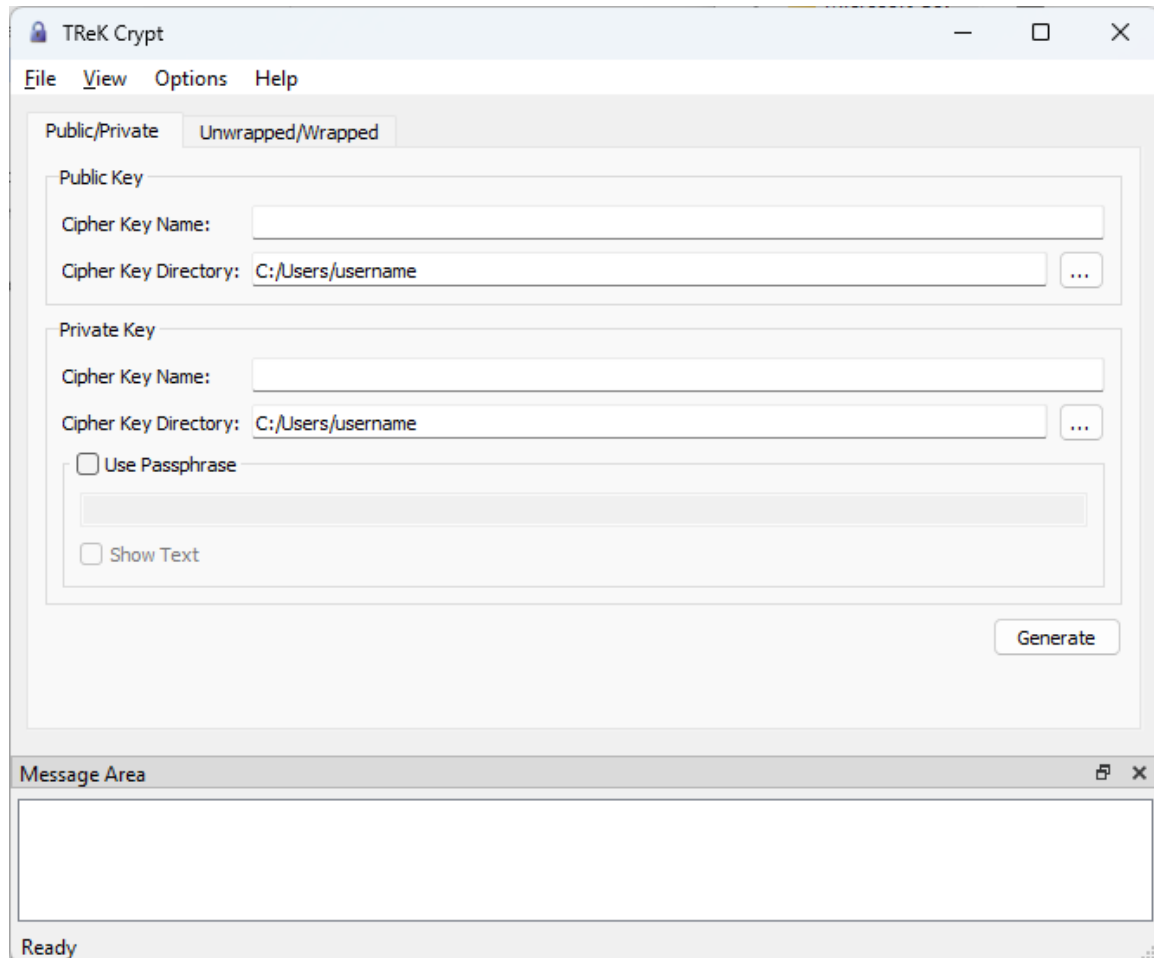


Figure 2 Main Window Key Information Area

Scheme

The tabs provide two different encryption scheme options. You can choose between Public/Private Key encryption or Unwrapped/Wrapped encryption.

Depending on which scheme you choose, you have slightly different input requirements.

For Scheme “Public/Private”:

Public Key Cipher Key Name

The Cipher Key Name field in the Public Key group box is used to enter a name for the file that will be created to hold the public cipher key.

Public Key Cipher Key Directory

The Cipher Key Directory field in the Public Key group box is used to enter a directory for the file that will be created to hold the public cipher key. The ... button can be used to browse the local disk for a directory. This field will default to your home directory.

Private Key Cipher Key Name

The Cipher Key Name field in the Private Key group box is used to enter a name for the file that will be created to hold the private cipher key.

Private Key Cipher Key Directory

The Cipher Key Directory field in the Private Key group box is used to enter a directory for the file that will be created to hold the private cipher key. The ... button can be used to browse the local disk for a directory. This field will default to your home directory.

For Scheme “Unwrapped/Wrapped”:

Create Unwrapped File/Use Existing File

This option allows you to choose whether to create a new unwrapped file or, if you already have one, use an existing file.

Unwrapped Key Cipher Key Name

The Cipher Key Name field in the Unwrapped Key group box is used to enter a name for the file that will be created to hold the unwrapped cipher key.

Unwrapped Key Cipher Key Directory

The Cipher Key Directory field in the Unwrapped Key group box is used to enter a directory for the file that will be created to hold the unwrapped cipher key. The ... button can be used to browse the local disk for a directory. This field will default to your home directory.

Cipher Key File (If Use Existing)

The existing unwrapped cipher key file to use. File must already exist. The ... button can be used to browse for the existing file.

Wrapped Key Cipher Key Name

The Cipher Key Name field in the Wrapped Key group box is used to enter a name for the file that will be created to hold the wrapped cipher key.

Wrapped Key Cipher Key Directory

The Cipher Key Directory field in the Wrapped Key group box is used to enter a directory for the file that will be created to hold the wrapped cipher key. The ... button can be used to browse the local disk for a directory. This field will default to your home directory.

Cipher Class

The Cipher Class is used to choose the number of bits (128/256) and encryption mode (GCM/CCM):

- AES GCM – Galois/Counter Mode – Single-pass encryption, authentication based on entire message, wide adoption.
- AES CCM – Counter with CBC-MAC – Two-pass encryption, plain text with MAC to calculate, limited adoption.

Use Passphrase

The Use Passphrase checkbox is used to specify that the private key generated should require a passphrase. If this box is checked, the passphrase must be entered into the text field. The passphrase text will not be displayed in the clear. If you want to see the text entered in the clear, check the Show Text checkbox.

Show Text

The Show Text checkbox is used to display the passphrase text in the clear.

Generate

The Generate button is used to generate the keys.

6.2 Application Messages

Various types of application messages are generated including information, progress, warning, error, and debug messages. Application messages are stored in memory and written to a temporary log file. The temporary log file is created on application initialization and exists if the application is running. It is deleted when you exit the application. The log file is in the temporary directory provided by the operating system. Only a subset of messages is stored in memory while all messages are written to the temporary log file. The maximum number of application messages stored in memory is controlled by the message storage setting in the Configure Messages dialog. Once the maximum is reached, older messages are deleted to make room for new messages. Setting the maximum value to a large number can impact application performance since it will increase the amount of memory used by the application. Setting this number too low can cause you to miss important messages. The application default was selected to protect against both scenarios. Messages stored in memory are displayed in the Main Window Message Area and the Messages dialog. The Messages dialog is shown in Figure 3. The Main Window message area only displays Info, Warning, and Error messages. The Messages dialog displays messages based on the display preferences defined in the Configure Messages dialog. By default, the Messages dialog will display information, progress, warning, and error messages. Columns in the Messages dialog can be sorted by clicking on the column header. The Messages dialog is available from the Options menu.

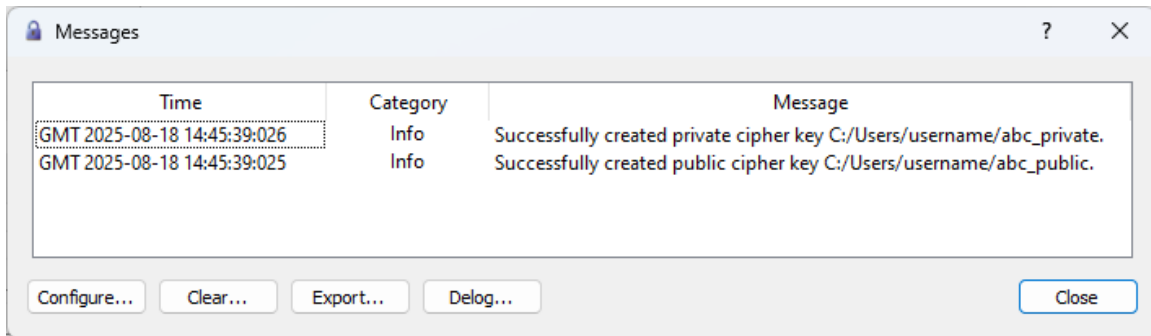


Figure 3 Messages Dialog

Configure

The Configure button provides access to the Configure Messages dialog shown in Figure 4. This dialog provides access to preferences associated with messages. Display preferences can be set to filter the types of messages (category) displayed in the Messages dialog. Export Preferences control how the time tag is added to the filename that is created when messages are exported. See the Export section for details. Message storage defines the maximum number of messages that will be stored in memory while the application is running. Once the maximum is reached, older messages are deleted to make room for new messages. The Set to Defaults button can be used to reset these properties to application defaults.

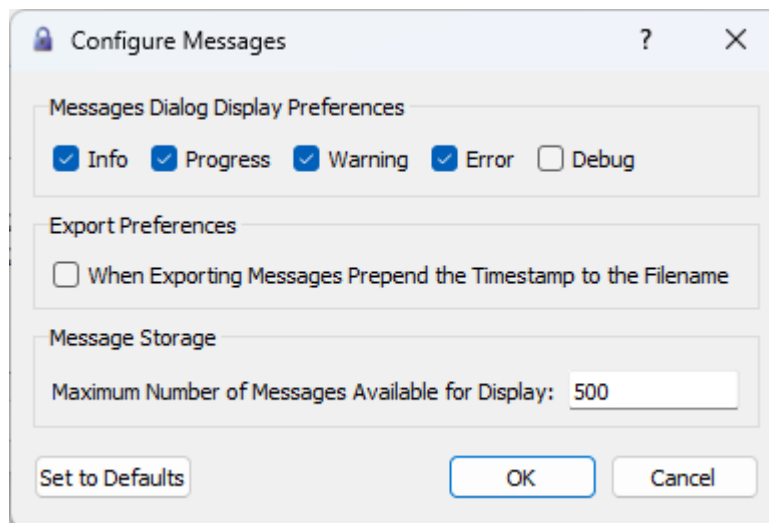


Figure 4 Configure Messages Dialog

Clear

The Clear button provides access to the Clear Messages dialog shown in Figure 5. This dialog provides two ways to clear application messages stored in memory. You can clear all the messages or clear selected messages. Once you clear messages, the messages are permanently deleted in all views (Main Window Message Area and the Messages dialog).

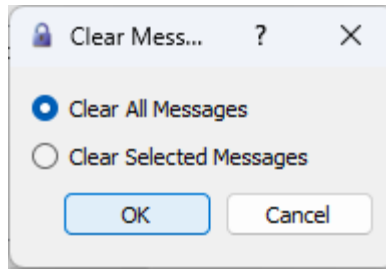


Figure 5 Clear Messages Dialog

Export

The Export button provides the capability to save all the application messages currently in memory to a file. When you push the Export button you will be prompted for a directory and filename. Export will save all messages in memory, not just the messages currently displayed in the Messages dialog (i.e., the Display Preferences are not applied). The name you provide for the file will be modified with a time tag that is added to the filename. The time tag indicates the time the file was closed. The default is to append the time tag to the filename. For example:

Filename Input: messages.txt
 Filename Output: messages_2017-05-07_13~03~28.txt

If you would like to prepend the time tag to the filename you can set this preference in the Configure Messages dialog. This would result in the following:

Filename Input: messages.txt
 Filename Output: 2017-05-07_13~03~28_messages.txt

Delog

The Delog button provides the capability to save all application messages generated since the application was started. Delog will retrieve the messages from the temporary log file. When you push the Delog button you will be prompted for a directory and filename. A timetag is not applied to the filename.

Filename Input: messages.txt
 Filename Output: messages.txt

6.3 Application Settings

The Crypt application saves some settings as application settings each time you exit the application. The next time you run the application, the application will initialize with the previous application settings. The following application settings are saved:

- Application Window Size
- Configure Messages Selections

- Encryption Scheme

7 FAQ and Troubleshooting

This section addresses Frequently Asked Questions and provides tips for troubleshooting common gotchas.

No FAQs yet.