SafeNet Authentication Client

Integration Guide

Using SAC CBA for SecureZIP

THE
DATA
PROTECTION
COMPANY

Document Information

Document Part Number	007-012820-001, Rev. A
Release Date	April 2015

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as SecureZIP.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Client (SAC) is a Public Key Infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SafeNet's certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system. SAM enables management of the complete user authentication life cycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet's hardware or software tokens devices. SAM is designed and developed based on the best practices of managing PKI devices in common PKI implementations. It offers robust yet easy to customize frameworks that meets different organizations' PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

For more information, refer to the *SafeNet Authentication Manager Administrator Guide*.

SecureZIP combines ZIP compression and strong crypto to deliver a Smart Encryption security solution. It allows IT administrators to enforce security policies and ensure data availability to your organization. It helps address your daily data security challenges, including protecting sensitive data, meeting compliance requirements and reducing overall costs and operational overhead.

This document provides guidelines for deploying certificate-based Encryption/Decryption in SecureZIP using SafeNet tokens.

SecureZIP can be configured to support multi-factor authentication in several modes. Certificate-based Encryption/Decryption will be used for the purpose of working with SafeNet products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC)** — SafeNet Authentication Client is the middleware that manages SafeNet's tokens.
- **SecureZIP for Windows Desktop**

Environment

The integration environment that was used in this document is based on the following software versions:

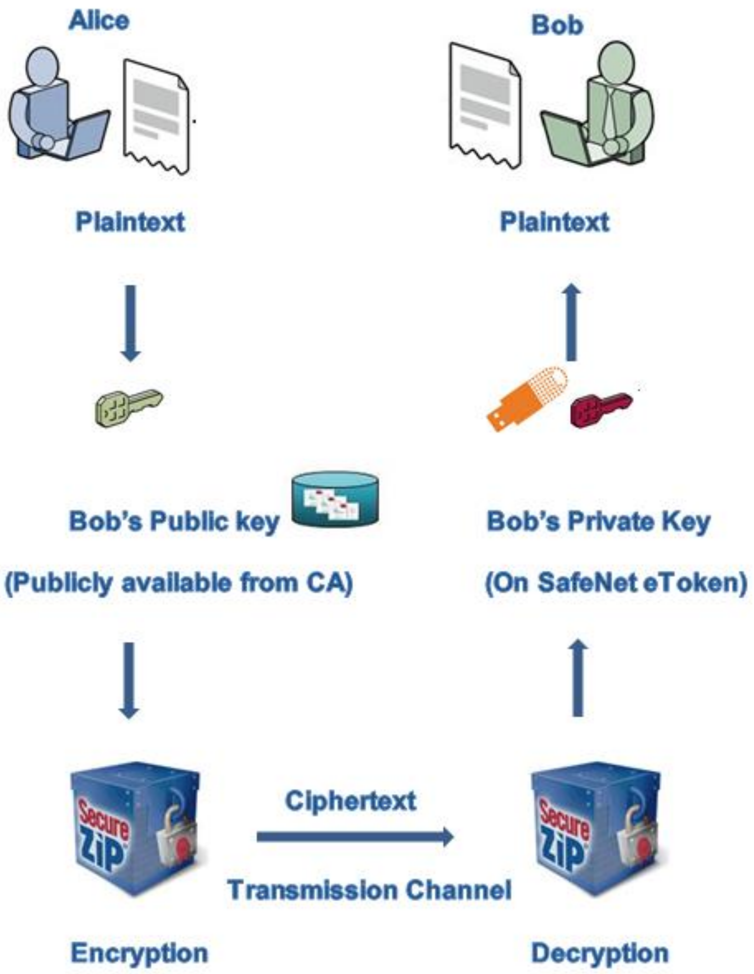
- **SafeNet Authentication Client (SAC)**—Version 9.0
- **SecureZIP for Windows Desktop—**Version 14.20.0027

Audience

This document is targeted to system administrators who are familiar with SecureZIP, and are interested in adding certificate-based encryption/decryption capabilities using SafeNet tokens.

Encryption and Decryption Flow

The diagram below illustrates the flow of certificate-based encryption and decryption:



Encryption Flow:

1. Alice opens SecureZIP for Window Desktop and adds a file to encrypt for Bob (recipient).
2. Alice selects the public certificate of Bob to encrypt.

Decryption Flow:

1. Bob connects the SafeNet eToken that contains his certificate private key.
2. Bob provides the eToken PIN.
3. The system validates the certificate on the SafeNet token. On successful validation, the file is decrypted and opened.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for SecureZIP using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, TPO should be configured with MS CA Connector. For further details, refer to the section “Connector for Microsoft CA” in the *SafeNet Authentication Manager Administrator’s Guide*.
- SafeNet Authentication Client 9.0 should be installed on all client machines.
- A user is created in Active Directory and an appropriate certificate is enrolled for the user on the smart card. The certificate is located on the **Published Certificates** tab within the user's properties in Active Directory.
- Active Directory, LDAP server, and client (where SecureZIP is installed) are up and running and can communicate with each other.

Supported Tokens in SAC

SAC supports a number of tokens that can be used as second authentication factor for users who authenticate to SecureZIP.

SafeNet Authentication Client 9.0 (GA) supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID and VSR

Smart Cards

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software Tokens

- SafeNet eToken Virtual
- SafeNet eToken Rescue

Configuring SecureZIP

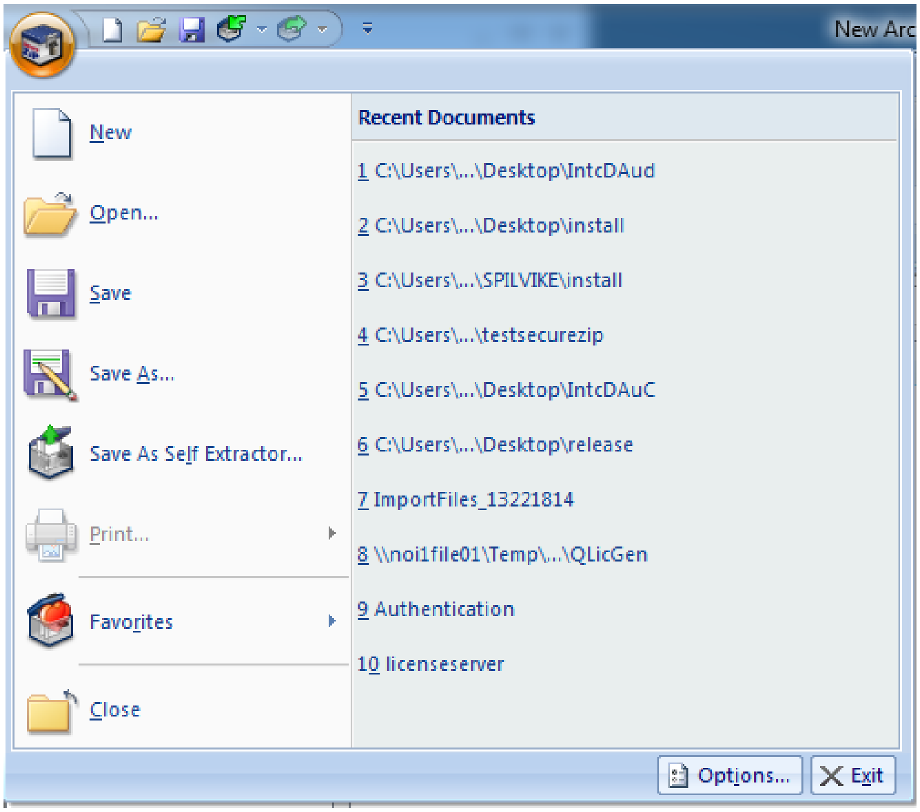
To use certificates for encryption and decryption, SecureZIP needs to access the certificates.

In this guide, integration is demonstrated using the LDAP server for accessing public key certificates for encryption.

Configuring SecureZIP to Point to Certificate Stores

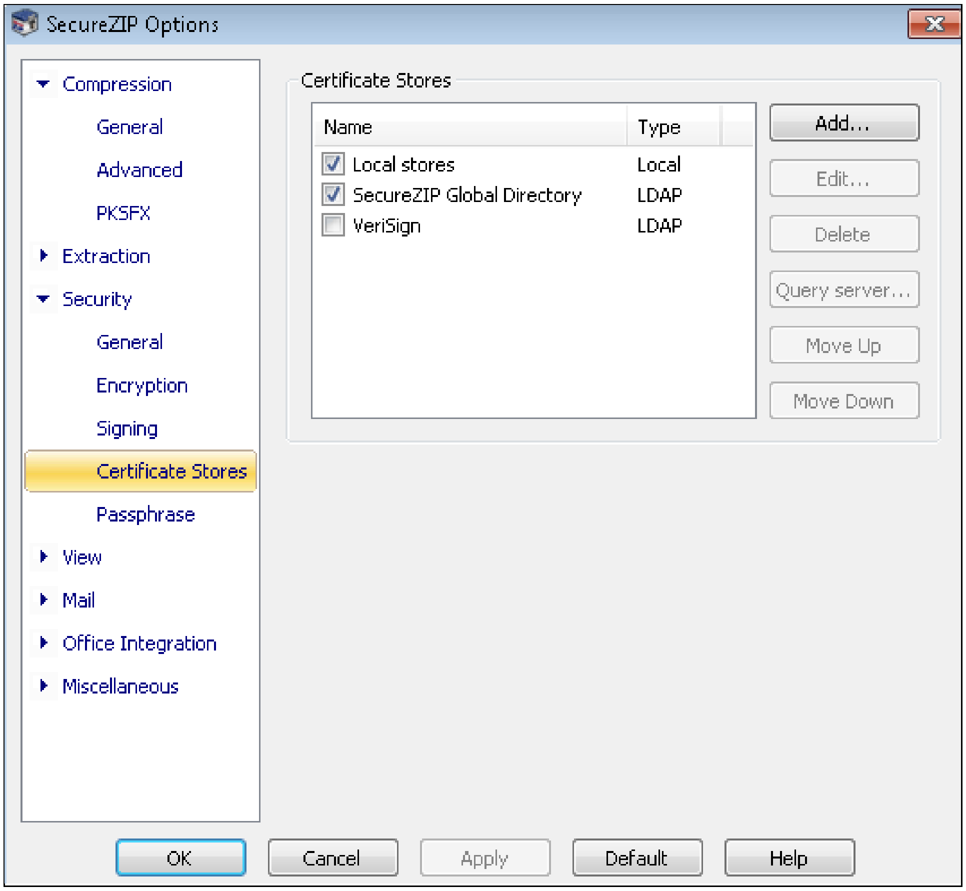
To encrypt user certificates, SecureZIP for Windows Desktop needs to access public certificates. You need to configure SecureZIP as to where the certificates are located.

1. To start the SecureZIP application, click **Start > Programs > SecureZIP > SecureZIP for Windows**.
2. Click the SecureZIP icon in the upper left corner, and then click **Options.**


New Arc
New
Open...
Save
Save As...
Save As Self Extractor...
Print...
Favorites
Close
Recent Documents
1 C:\Users\...\Desktop\IntcDAud
2 C:\Users\...\Desktop\install
3 C:\Users\...\SPILVIKE\install
4 C:\Users\...\testsecurezip
5 C:\Users\...\Desktop\IntcDAuC
6 C:\Users\...\Desktop\release
7 ImportFiles_13221814
8 \\noi1file01\Temp\...\QLicGen
9 Authentication
10 licenseserver
Options...
Exit

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

3. On the **SecureZIP Options** window, click **Security > Certificate Stores**. To add a new certificate store, click **Add**.

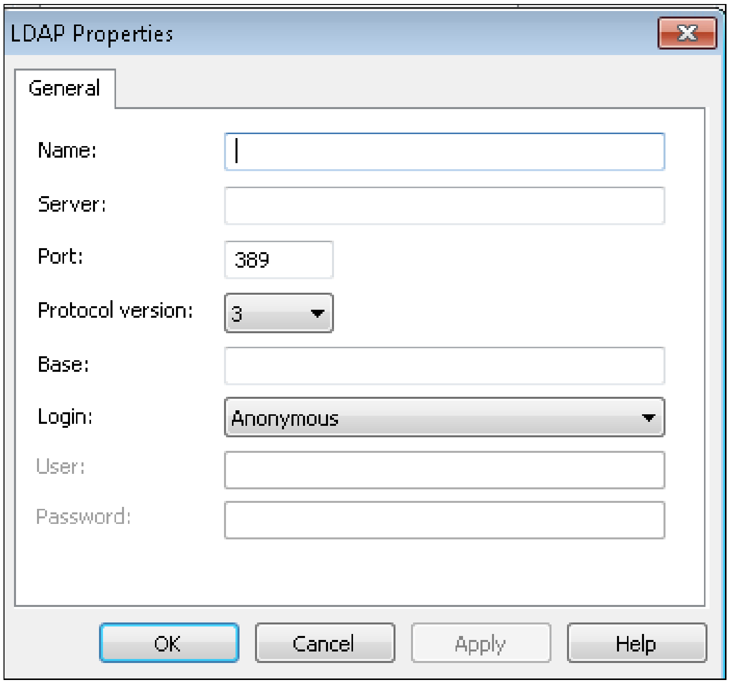


Name	Type
☑ Local stores	Local
☑ SecureZIP Global Directory	LDAP
□ VeriSign	LDAP

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

4. On the **LDAP Properties** window, complete the following fields, and then click **OK**:

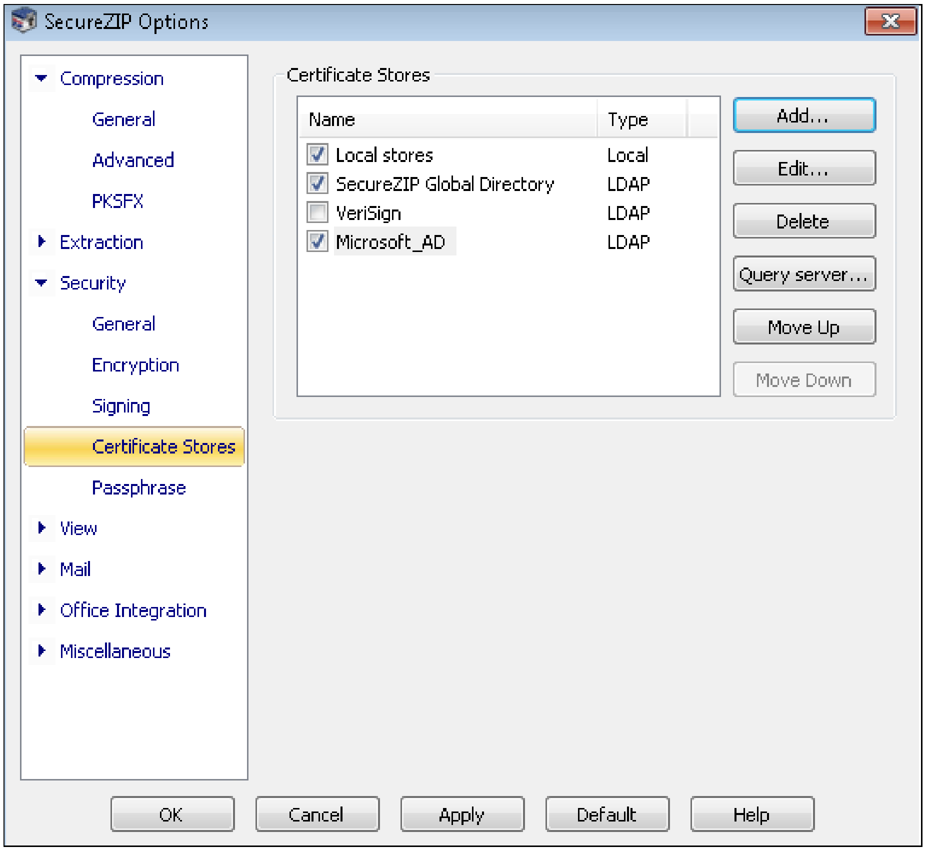
Name	Enter a name to identify the server in the **Certificate Stores** list.
Server	Enter IP address of the LDAP server or a name that resolves to such an address.
Port	Enter the IP port to use. Port 389 is customary and is entered as the default.
Protocol Version	Enter the version of LDAP that you are using. Most likely this is the newer version 3.
Base	Enter the query string that SecureZIP should use as the base or root of the LDAP search for certificates, analogous to a root folder or directory in a file system; for example, **cn=users,dc=xyz,dc=com**.
Login	Select an appropriate value.
User	Enter the user account with which to log in if the LDAP server requires a login.
Password	Enter the password associated with the user account.



Name:
Server:
Port: 389
Protocol version: 3
Base:
Login: Anonymous
User:
Password:

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

5. On the **SecureZIP Options** window, in the **Certificate Stores** list, select only the certificate store you just created, and clear all other certificate stores. Click **OK**.



Certificate Stores

Name	Type
☑ Local stores	Local
☑ SecureZIP Global Directory	LDAP
□ VeriSign	LDAP
☑ Microsoft_AD	LDAP

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

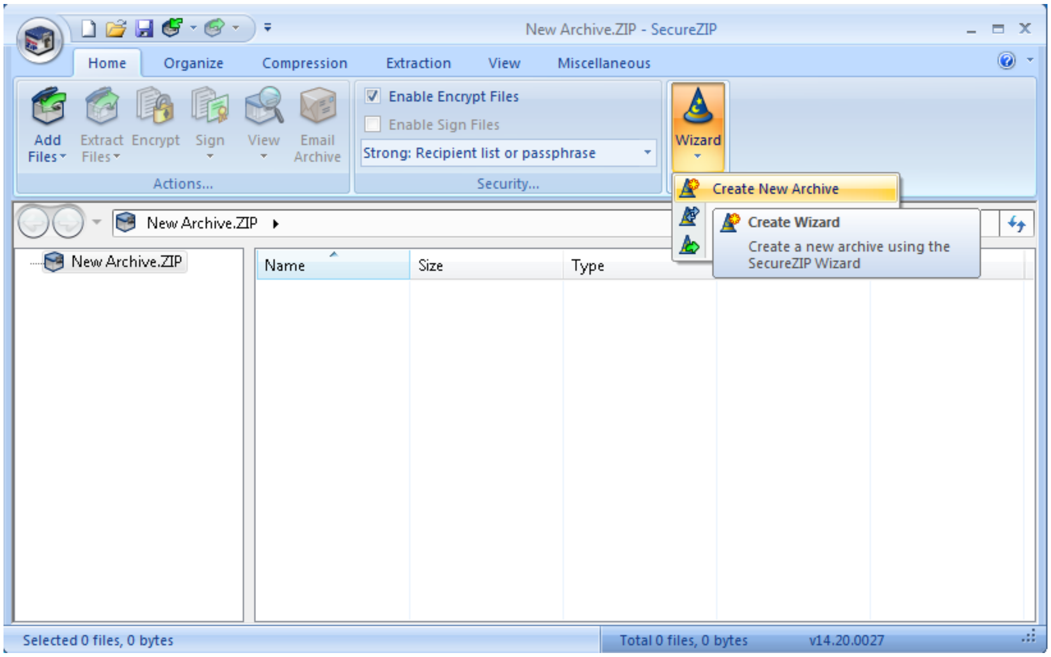
Running the Solution

To verify this integration solution:

1. Encrypt a file with proper public certificate of the user.
2. Decrypt the same file using user certificate's private key that is present in the token.

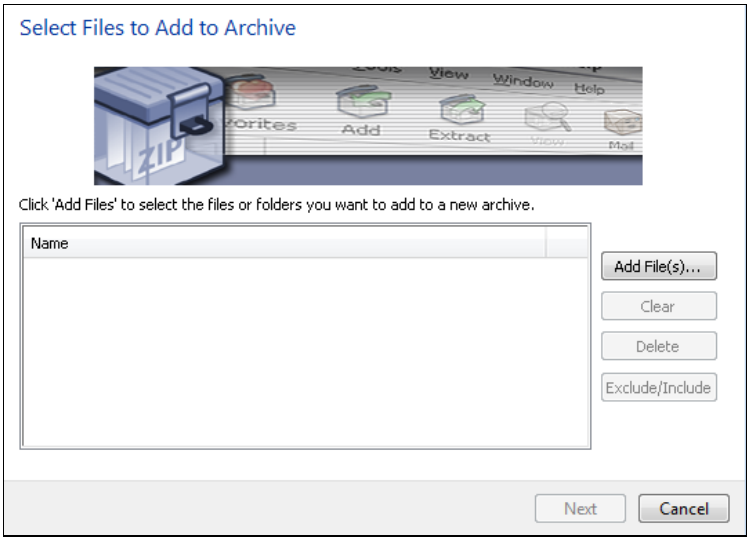
Encrypting a File

1. To start the SecureZIP application, click **Start > Programs > SecureZIP > SecureZIP for Windows**.
2. On the SecureZIP main window, click **Wizard > Create New Archive**.



(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

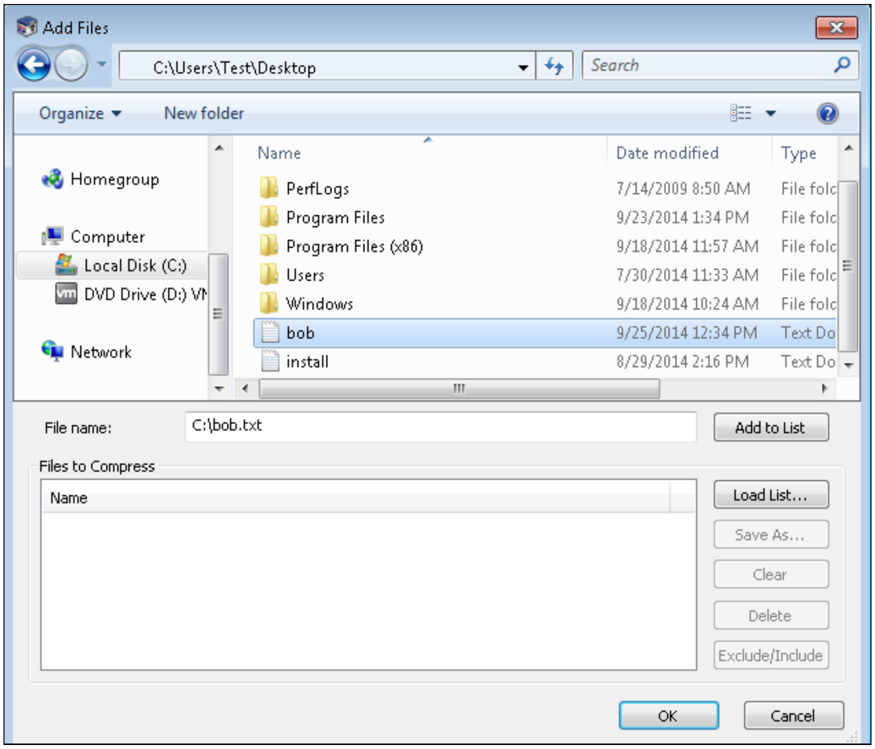
3. On the **Select Files to Add to Archive** window, click **Add file(s)**.


Select Files to Add to Archive

Click 'Add Files' to select the files or folders you want to add to a new archive.

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

4. On the **Add Files** window, perform the following steps:
   a. Select the file you want to encrypt (for example, **bob.txt**).
   b. Click **Add to List**. The file is added under **Files to compress**.
   c. Click **OK**.



C:\Users\Test\Desktop

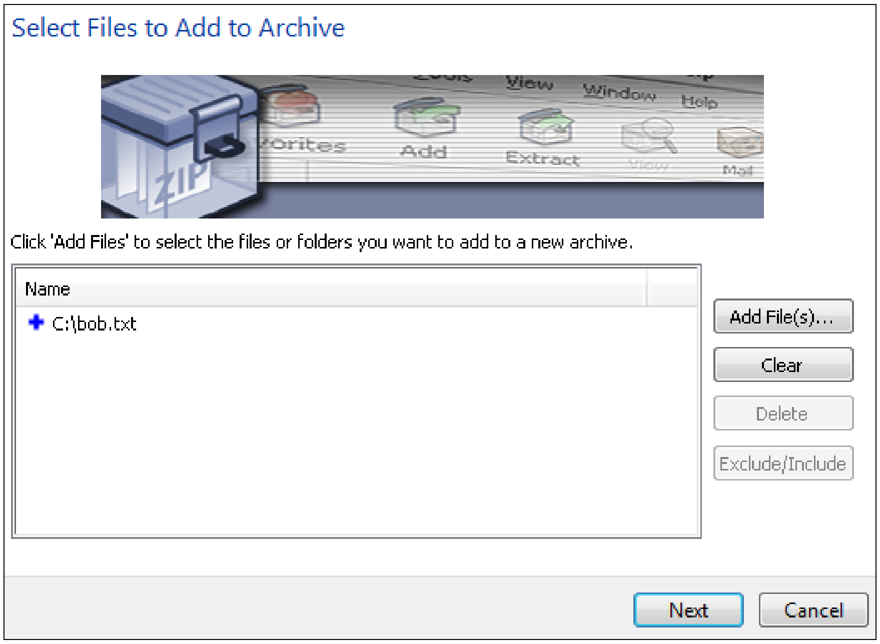
Name	Date modified	Type
PerfLogs	7/14/2009 8:50 AM	File folc
Program Files	9/23/2014 1:34 PM	File folc
Program Files (x86)	9/18/2014 11:57 AM	File folc
Users	7/30/2014 11:33 AM	File folc
Windows	9/18/2014 10:24 AM	File folc
bob	9/25/2014 12:34 PM	Text Do
install	8/29/2014 2:16 PM	Text Do

File name: C:\bob.txt

Name

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

5. On the **Select Files to Add to Archive** window, the file is added in the list. Click **Next**.



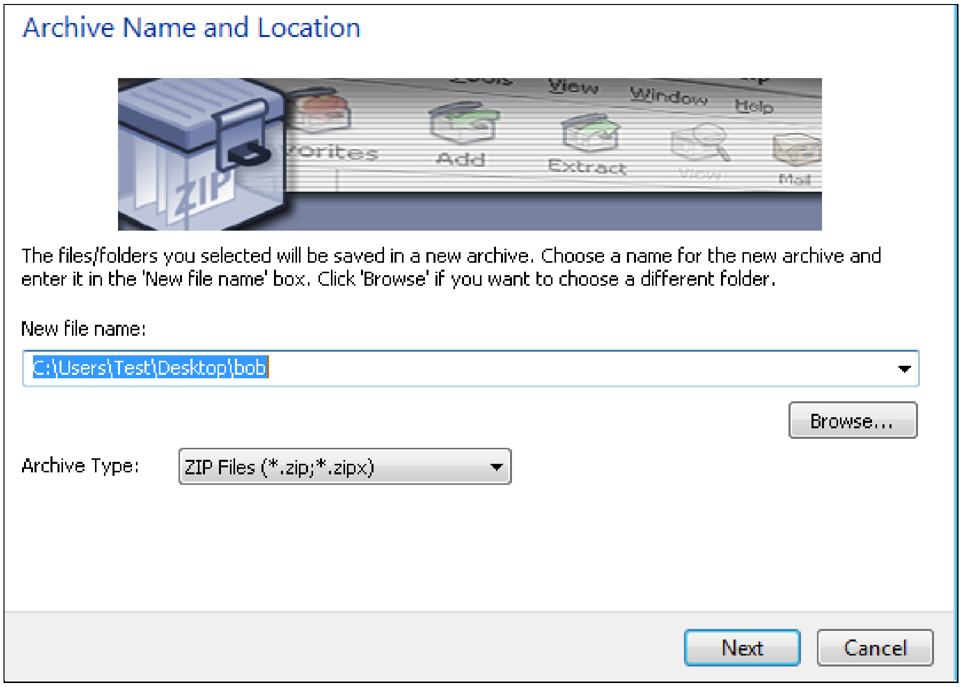
Select Files to Add to Archive

Click 'Add Files' to select the files or folders you want to add to a new archive.

Name
✚ C:\bob.txt

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

6. On the **Archive Name and Location** window, in the **New file name** field, enter a name and path for the encrypted file, and then click **Next**.



Archive Name and Location

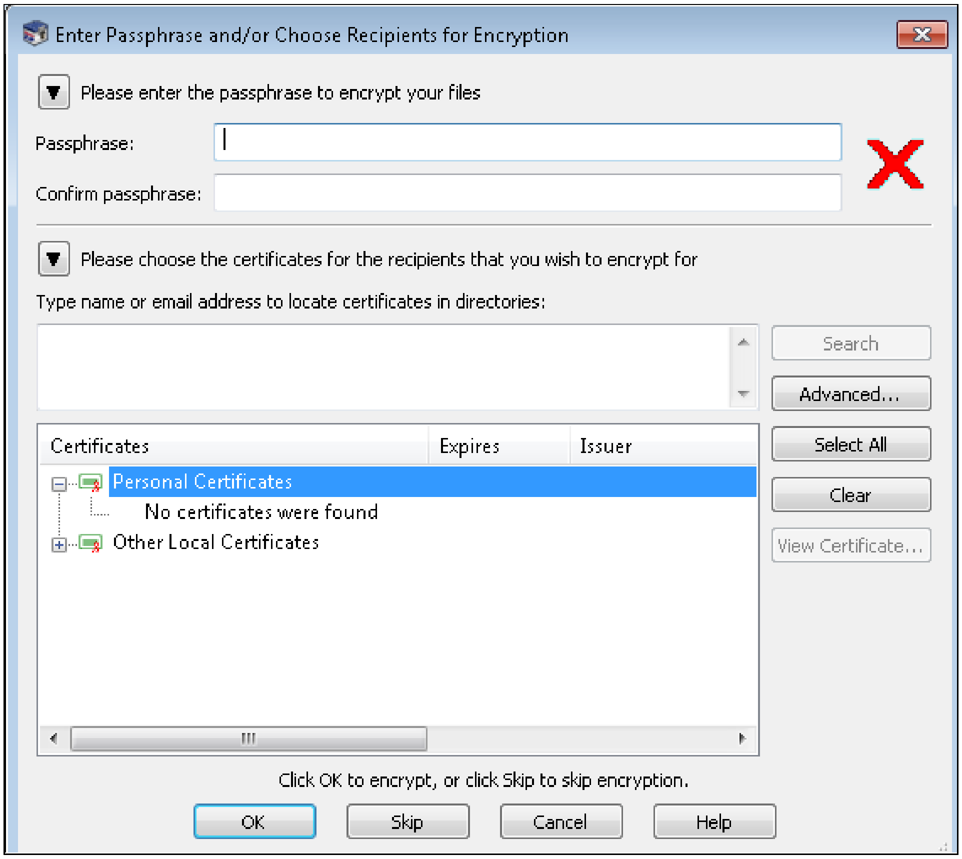
The files/folders you selected will be saved in a new archive. Choose a name for the new archive and enter it in the 'New file name' box. Click 'Browse' if you want to choose a different folder.

New file name: C:\Users\Test\Desktop\bob

Archive Type: ZIP Files (*.zip;*.zipx)

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

7. On the **Enter Passphrase and/or Choose Recipients for Encryption** window, click **Advanced**.



Enter Passphrase and/or Choose Recipients for Encryption

Please enter the passphrase to encrypt your files

Passphrase:

Confirm passphrase:

Please choose the certificates for the recipients that you wish to encrypt for

Type name or email address to locate certificates in directories:

Certificates	Expires	Issuer
Personal Certificates		
No certificates were found		
Other Local Certificates		

Click OK to encrypt, or click Skip to skip encryption.

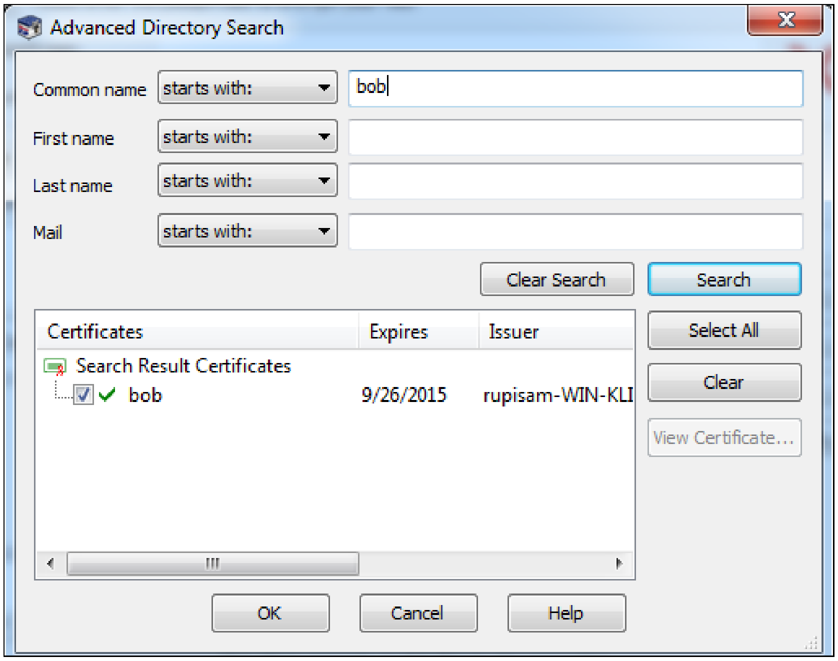
(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

8. On the **Advanced Directory Search** window, perform the following steps:

   a. Use the **Common name**, **First name**, **Last name**, and **Mail** fields to search the certificates.

   b. Under **Search Results Certificates**, select the certificate.

   c. Click **OK**.



Advanced Directory Search

Common name: starts with: bob

First name: starts with:

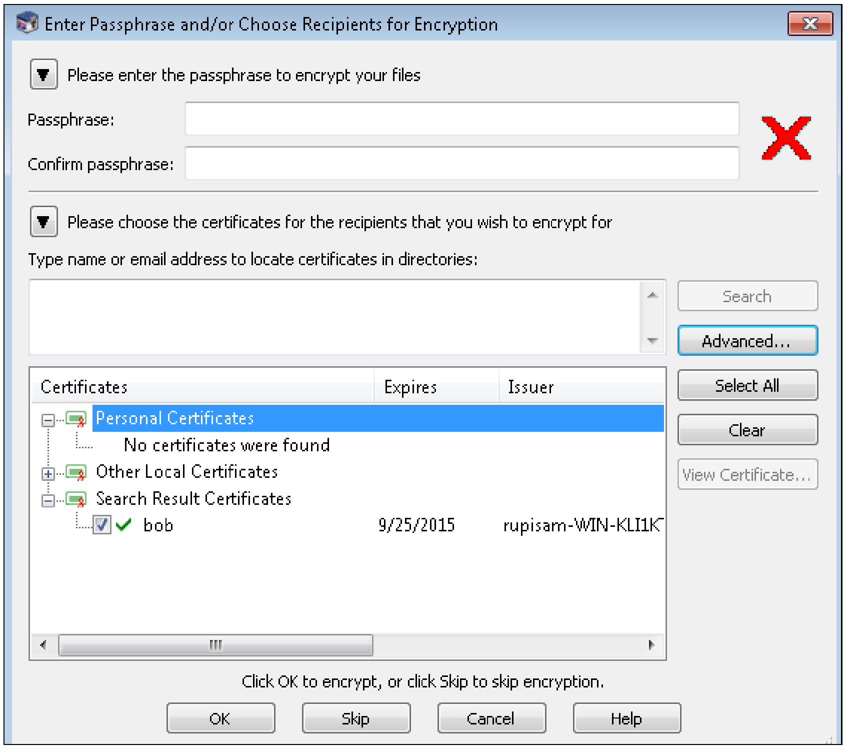
Last name: starts with:

Mail: starts with:

Certificates	Expires	Issuer
Search Result Certificates		
☑ ✓ bob	9/26/2015	rupisam-WIN-KLI

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

9. On the **Enter Passphrase and/or Choose Recipients for Encryption** window, click **OK**.



Enter Passphrase and/or Choose Recipients for Encryption

Please enter the passphrase to encrypt your files

Passphrase:

Confirm passphrase:

Please choose the certificates for the recipients that you wish to encrypt for

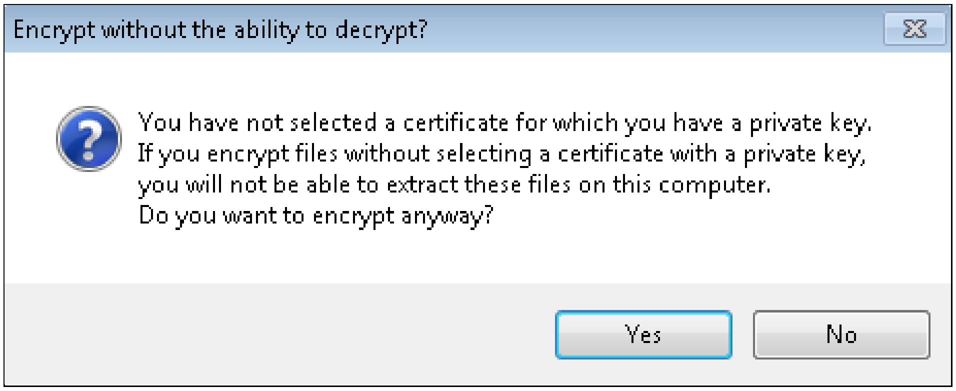
Type name or email address to locate certificates in directories:

Certificates	Expires	Issuer
Personal Certificates		
No certificates were found		
Other Local Certificates		
Search Result Certificates		
☑ ✓ bob	9/25/2015	rupisam-WIN-KLI1K

Click OK to encrypt, or click Skip to skip encryption.

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

10. As we already have a private key in the token, click **Yes**.

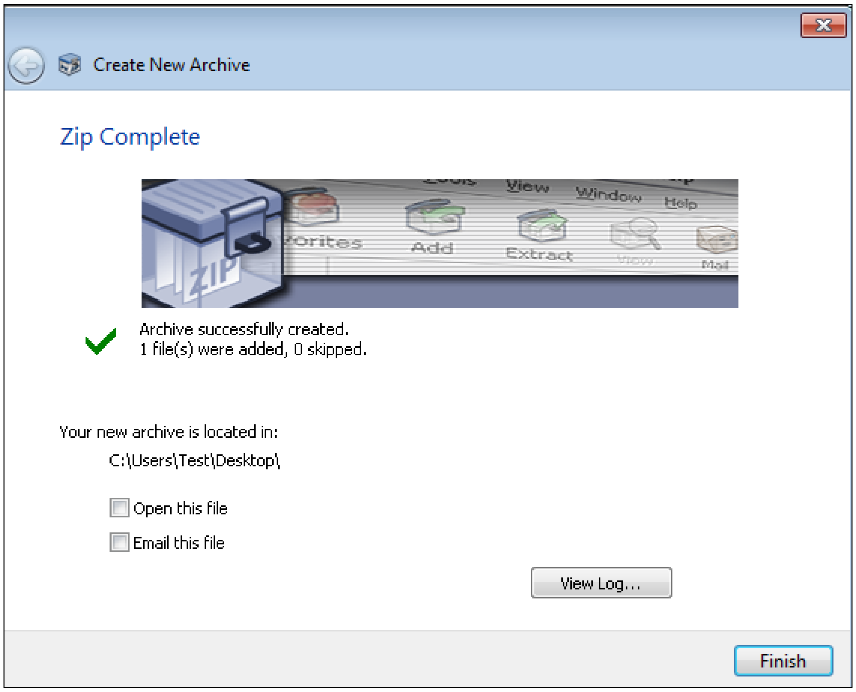


Encrypt without the ability to decrypt?

You have not selected a certificate for which you have a private key. If you encrypt files without selecting a certificate with a private key, you will not be able to extract these files on this computer.
Do you want to encrypt anyway?

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

11. A new encrypted archive is created. Click **Finish**.



Create New Archive

Zip Complete

✓ Archive successfully created.
1 file(s) were added, 0 skipped.

Your new archive is located in:
C:\Users\Test\Desktop\

□ Open this file
□ Email this file

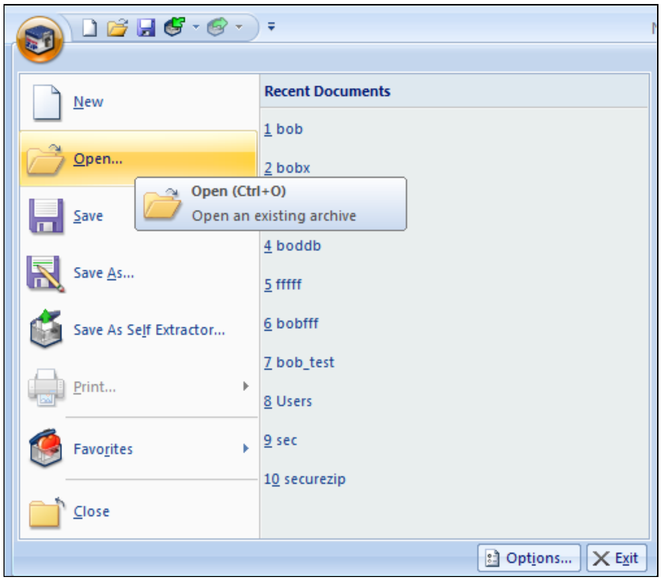
(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

Decrypting a File

For this integration solution, the SafeNet eToken PRO 72K is used.

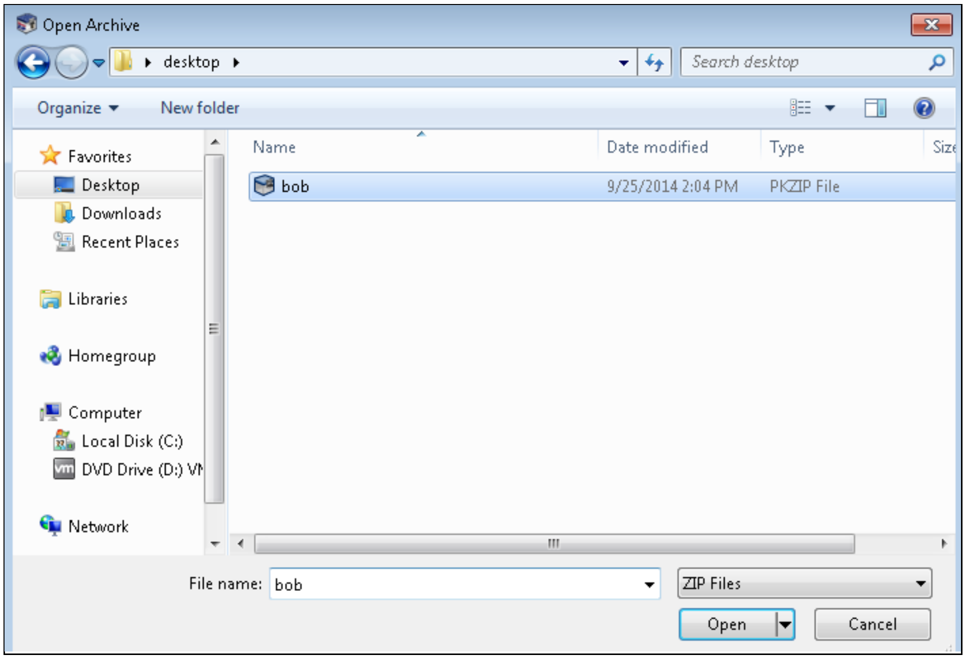
If you want to open the encrypted file on any Windows system where SecureZIP is installed, perform the following steps:

1. Insert the SafeNet eToken PRO 72K (with the certificate of the user) into the USB port.
2. To start the SecureZIP application, click **Start > Programs > SecureZIP > SecureZIP for Windows**.
3. Click the SecureZIP icon on the upper left corner, and then click **Open**.



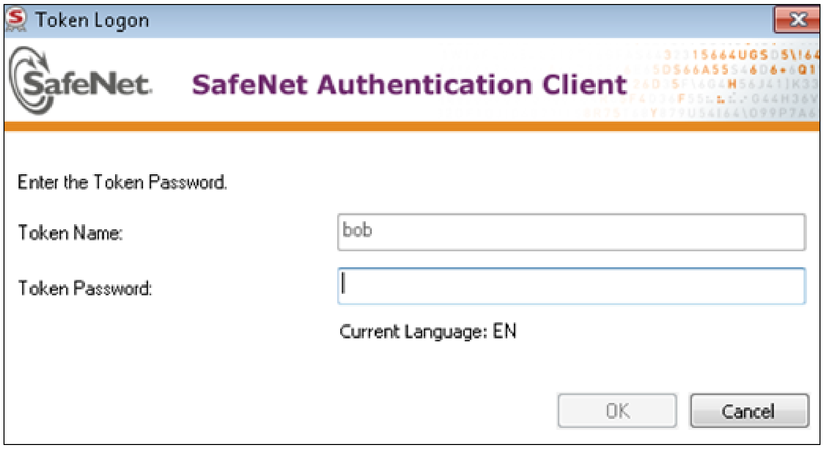
(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

4. On the **Open Archive** window, locate and select the encrypted file (for example, **bob.txt**), and then click **Open**.



(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)

5. On the **Token Logon** window, in the **Token Password** field, enter the token password, and then click **OK**.



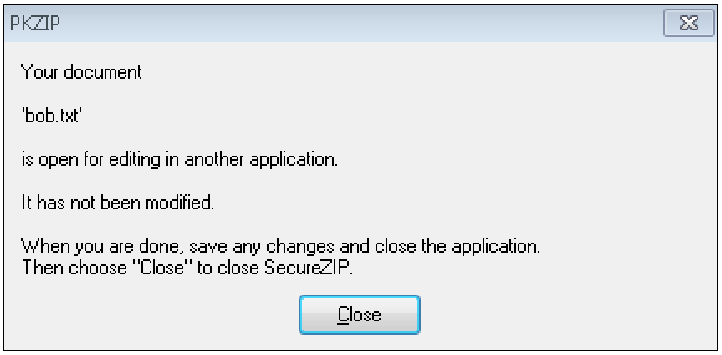
Enter the Token Password.

Token Name: bob

Token Password:

Current Language: EN

When the validation is successful, the file is decrypted using the private key present on the token and is then opened.



Your document

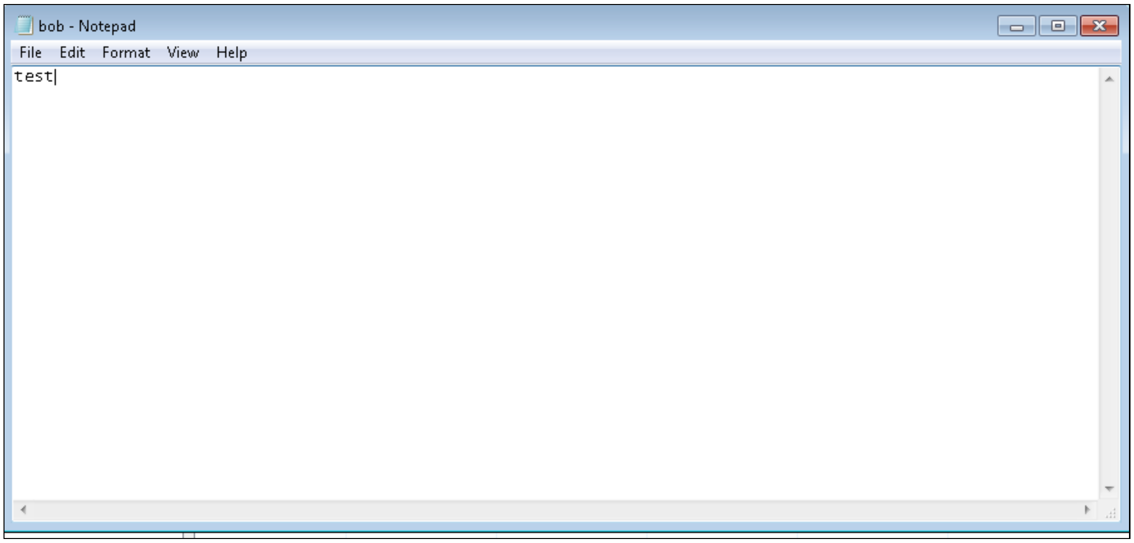
'bob.txt'

is open for editing in another application.

It has not been modified.

When you are done, save any changes and close the application.
Then choose "Close" to close SecureZIP.

(The screen image above is from SecureZIP® software. Trademarks are the property of their respective owners.)



```
test
```

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	