Utility - CryptSharp

User Guide

Document Revision 1.0

Trademarks and copyrights

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom
Registered in England: Reg. No. 4260035. Tel: +44 870 879 3000. Web: www.blueprism.com

Contents

1. Introduction

CryptSharp is a C# library created by James F Bellinger. It provides a number of password algorithms. This VBO is a wrapper around that library to present the user with the ability to create and verify password hashes using these algorithms.

The options available are:

- BCrypt (Blowfish)
- LDAP
- MD5
- PHPass (Wordpress, phpBB, Drupal)
- SHA256/512
- Traditional and Extended DES.

2. Prerequisites

List any prerequisites necessary for the proper functioning of the Asset. Examples include:

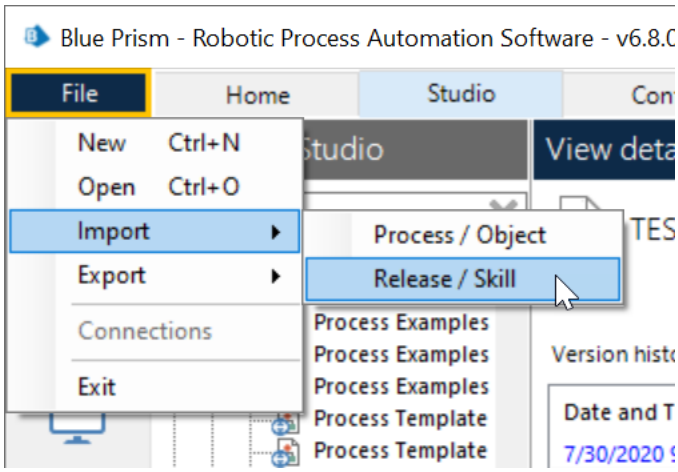
- Blue Prism V6.8 or later.
- CryptSharp dll (available from https://www.nuget.org/packages/CryptSharpOfficial/)
- The Utility – CryptSharp bprelease availabl at https://github.com/blue-prism/CryptSharp

3. Configuration

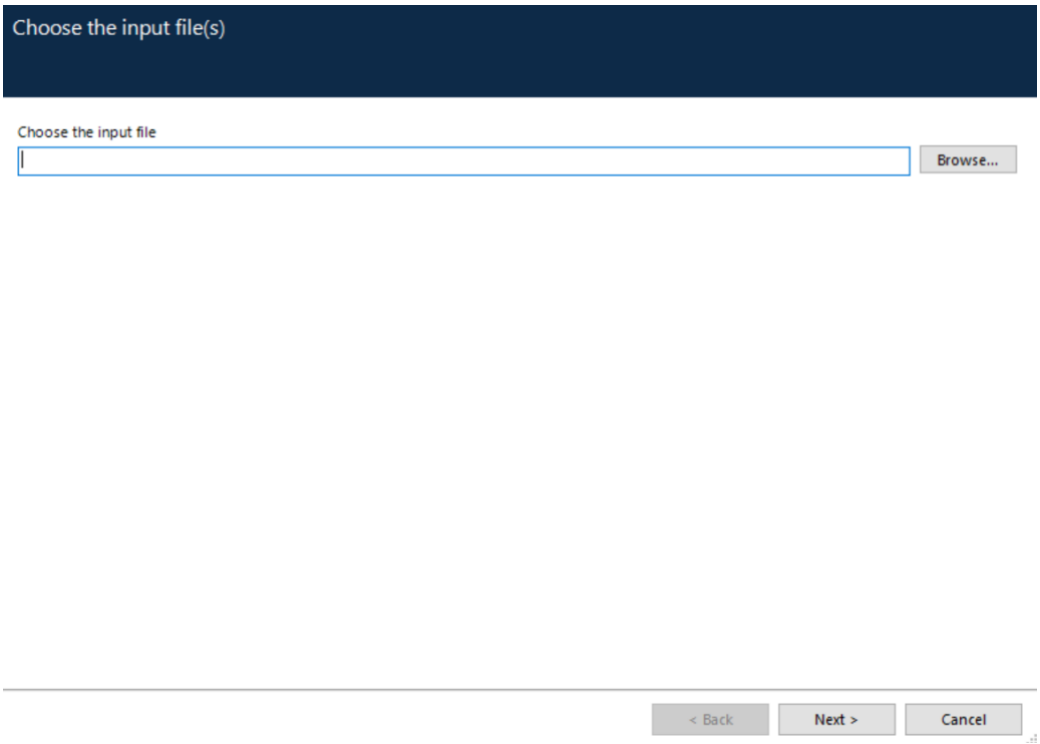
The asset can be downloaded from the Digital Exchange (DX) at or from Github at https://github.com/blue-prism/CryptSharp

The bprelease file contains the Utility CryptSharp VBO and also a process example of its use. The file can be imported as follows:

From the file menu, shown below, choose import, and then the Release/Skill pop-out.

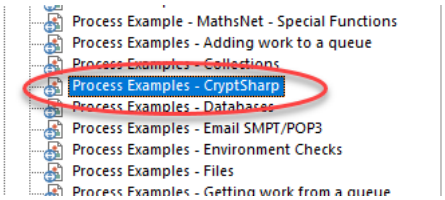


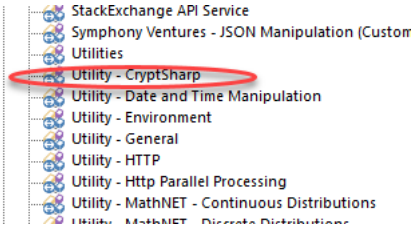
You will see the following dialog.



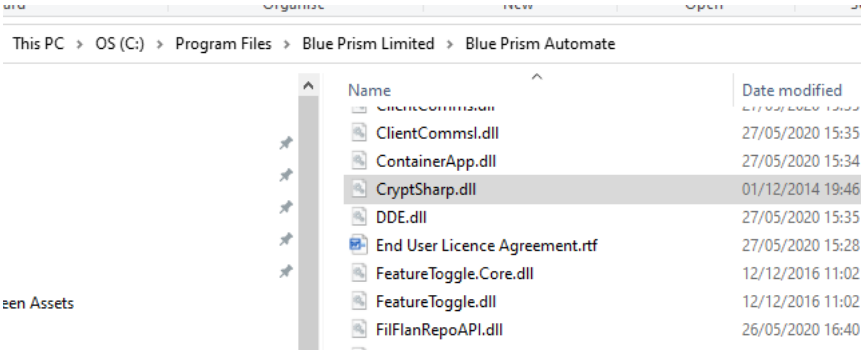
If you know the path to where you have the VBO stored, enter it into the text box, or navigate to it, using the browse button and file dialog that appears.

Once installed, your Blue Prism Studio should have the following entries in processes and objects.





The CryptSharp.dll (available from the nuget link above) should be placed into the Blue Prism Automate working directory. This is shown below.



Once you have all this setup, you are good to go.

4. Using the Asset

4.1 Blowfish

The Blowfish action, uses the Blowfish algorithm to encrypt a supplied password or passphrase.

Input:

Name	Description	Data Type
password	The password to encrypt using the blowfish algorithm.	Text

Output:

Name	Description	Data Type
ciphertext	The resulting ciphertext or hash output	Text

4.2 Blowfish Verify

The Blowfish Verify action takes in a password and a previously completed hash and they are compared. If they match, an isValid result of True will be returned.

Input:

Name	Description	Data Type
password	The password to be verified.	Text
Ciphertext	The ciphertext to verify the password against.	Text

Output:

Name	Description	Data Type
IsValid	A true/false value stating whether the password hash matches that of the supplied ciphertext.	Flag

4.3 ExtendedDESEncrypt

The ExtendedDESEncrypt action, uses the ExtendedDES algorithm to encrypt a supplied password or passphrase.

Input:

Name	Description	Data Type
password	The password to encrypt using the ExtendedDES algorithm.	Text

Output:

Name	Description	Data Type
ciphertext	The resulting ciphertext or hash output	Text

4.4 ExtendedDESEncrypt Verify

The Blowfish Verify action takes in a password and a previously completed hash and they are compared. If they match, an isValid result of True will be returned.

Input:

Name	Description	Data Type
password	The password to be verified.	Text
Ciphertext	The ciphertext to verify the password against.	Text

Output:

Name	Description	Data Type
IsValid	A true/false value stating whether the password hash matches that of the supplied ciphertext.	Flag

4.5 LDAPEncrypt

The LDAPEncrypt action, uses the LDAP algorithm to encrypt a supplied password or passphrase.

Input:

Name	Description	Data Type
password	The password to encrypt using the LDAP algorithm.	Text

Output:

Name	Description	Data Type
ciphertext	The resulting ciphertext or hash output	Text

4.6 LDAPEncrypt Verify

The LDAPEncrypt Verify action takes in a password and a previously completed hash and they are compared. If they match, an isValid result of True will be returned.

Input:

Name	Description	Data Type
password	The password to be verified.	Text
Ciphertext	The ciphertext to verify the password against.	Text

Output:

Name	Description	Data Type
IsValid	A true/false value stating whether the password hash matches that of the supplied ciphertext.	Flag

4.7 MD5Encrypt

The MD5Encrypt action, uses the MD5 algorithm to encrypt a supplied password or passphrase.

Input:

Name	Description	Data Type
password	The password to encrypt using the MD5 algorithm.	Text

Output:

Name	Description	Data Type
ciphertext	The resulting ciphertext or hash output	Text

4.8 MD5Encrypt Verify

The MD5Encrypt Verify action takes in a password and a previously completed hash and they are compared. If they match, an isValid result of True will be returned.

Input:

Name	Description	Data Type
password	The password to be verified.	Text
Ciphertext	The ciphertext to verify the password against.	Text

Output:

Name	Description	Data Type
IsValid	A true/false value stating whether the password hash matches that of the supplied ciphertext.	Flag

4.9 PhpassEncrypt

The PhpassEncrypt action, uses the Phpass algorithm to encrypt a supplied password or passphrase.

Input:

Name	Description	Data Type
password	The password to encrypt using the Phpass algorithm.	Text

Output:

Name	Description	Data Type
ciphertext	The resulting ciphertext or hash output	Text

4.10 PhpassEncrypt Verify

The PhpassEncrypt Verify action takes in a password and a previously completed hash and they are compared. If they match, an isValid result of True will be returned.

Input:

Name	Description	Data Type
password	The password to be verified.	Text
Ciphertext	The ciphertext to verify the password against.	Text

Output:

Name	Description	Data Type
IsValid	A true/false value stating whether the password hash matches that of the supplied ciphertext.	Flag

4.11 SHA256Encrypt

The SHA256Encrypt action, uses the SHA256 algorithm to encrypt a supplied password or passphrase.

Input:

Name	Description	Data Type
password	The password to encrypt using the SHA256 algorithm.	Text

Output:

Name	Description	Data Type
ciphertext	The resulting ciphertext or hash output	Text

4.12 SHA256Encrypt Verify

The SHA256Encrypt Verify action takes in a password and a previously completed hash and they are compared. If they match, an isValid result of True will be returned.

Input:

Name	Description	Data Type
password	The password to be verified.	Text
Ciphertext	The ciphertext to verify the password against.	Text

Output:

Name	Description	Data Type
IsValid	A true/false value stating whether the password hash matches that of the supplied ciphertext.	Flag

4.13 SHA512Encrypt

The SHA512Encrypt action, uses the SHA512 algorithm to encrypt a supplied password or passphrase.

Input:

Name	Description	Data Type
password	The password to encrypt using the SHA512 algorithm.	Text

Output:

Name	Description	Data Type
ciphertext	The resulting ciphertext or hash output	Text

4.14 SHA512Encrypt Verify

The SHA512Encrypt Verify action takes in a password and a previously completed hash and they are compared. If they match, an isValid result of True will be returned.

Input:

Name	Description	Data Type
password	The password to be verified.	Text
Ciphertext	The ciphertext to verify the password against.	Text

Output:

Name	Description	Data Type
IsValid	A true/false value stating whether the password hash matches that of the supplied ciphertext.	Flag

4.15 DESEncrypt

The DESEncrypt action, uses the DES algorithm to encrypt a supplied password or passphrase.

Input:

Name	Description	Data Type
password	The password to encrypt using the DES algorithm.	Text

Output:

Name	Description	Data Type
ciphertext	The resulting ciphertext or hash output	Text

4.16 DESEncrypt Verify

The DESEncrypt Verify action takes in a password and a previously completed hash and they are compared. If they match, an isValid result of True will be returned.

Input:

Name	Description	Data Type
password	The password to be verified.	Text
Ciphertext	The ciphertext to verify the password against.	Text

Output:

Name	Description	Data Type
IsValid	A true/false value stating whether the password hash matches that of the supplied ciphertext.	Flag

5. Support

This asset is provided free-of-charge by Blue Prism. Blue Prism does not provide formal support of this asset. Please direct any questions you have, related to this asset, to the Digital Exchange Community page:

https://community.blueprism.com/communities/community-home?CommunityKey=1e516cfe-4d1f-4de9-a9eb-58d15bf38c81