CATIA Data Security (DS9) – Supplier application

BPA Delivery 7 for V5R19 (V5.7)

User Guide

Table of Contents

Introduction

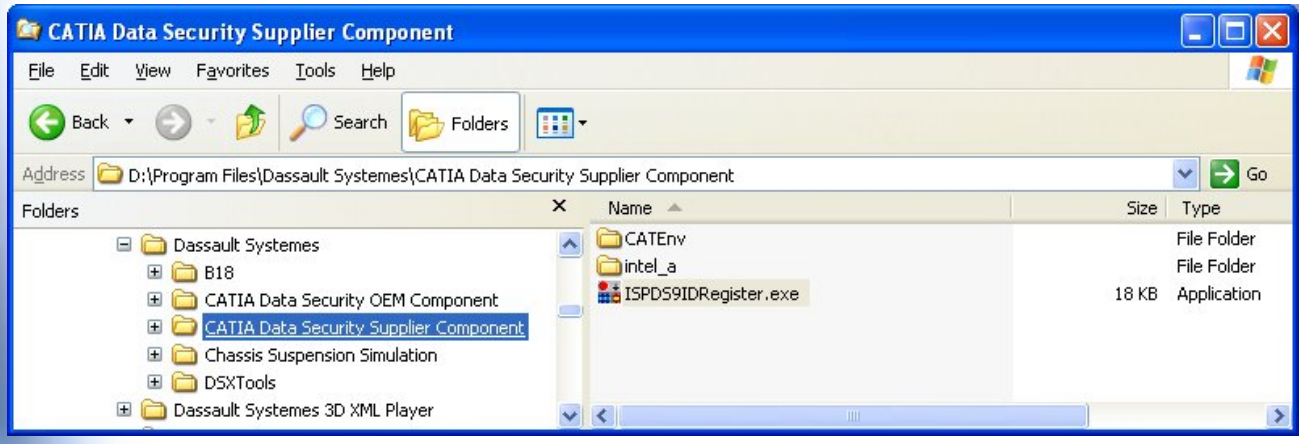
This document describes the usage of the BPA DS9 at Supplier site.

OEM ID enrollment

After successful installation of BPA DS9 application, you must register at least one OEM ID Key into the system.

You will receive from your OEM a file named XXX.txt (XXX is your OEM name).
Copy it to the machine(s) where the BPA DS9 has been installed.

Launch the application “ISPDS9IDRegister.exe” located in the DS9 Supplier Application installation folder.



Click “OEM ID Selection” and then select the file sent by the OEM.

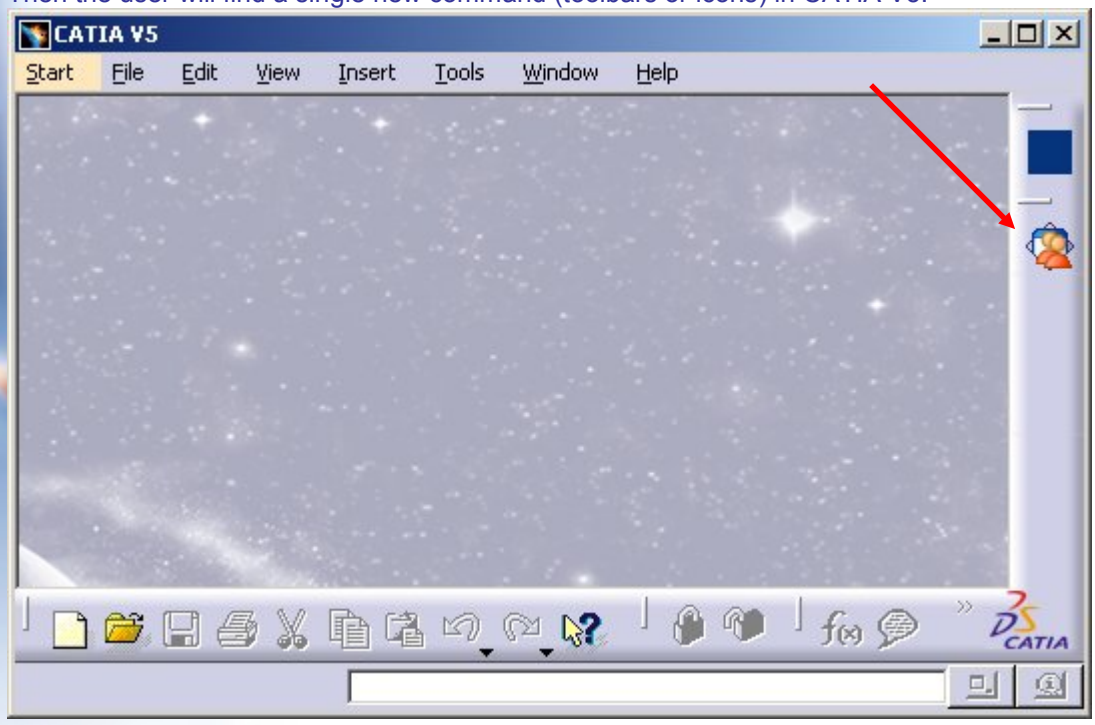
This task must be performed only once every time you receive a new XXX.txt file from an OEM.
With this file the OEM should provide you with a login / password. Please keep it secret.

Once this setup is completed, you will be able to open any file which was encrypted by this OEM, using the same ID.

Usage for CATIA V5 Files

When launching the application with the new icon created on the desktop, the following message is displayed to the user:

Then the user will find a single new command (toolbars or icons) in CATIA V5.



Before opening any encrypted data the user must first login to the application by using this command.

User ID and Password should have been given by the OEM (by phone, e-mail or encrypted excel file).

The User ID and Password can be kept persistent until the next login by checking the “Keep Persistent” box. If this option is checked, you will not need to login again when you will restart the application, except if you want to change login information. Furthermore, batch applications will be able to open encrypted data using the kept information. To remove the kept information, launch the command and login without checking the “Keep Persistent” box.

Once the login is done, the usage of the BPA DS9 is completely transparent for the CATIA user.

Once an encrypted file has been successfully opened, it can be edited and saved, in exactly the same manner as a standard (not encrypted) document, except if it has been encrypted by the OEM in “Read-Only” mode. In this case, save cannot be done. The information about the “Read-Only” encryption can be found in the file “DS9ReadMe.txt”.

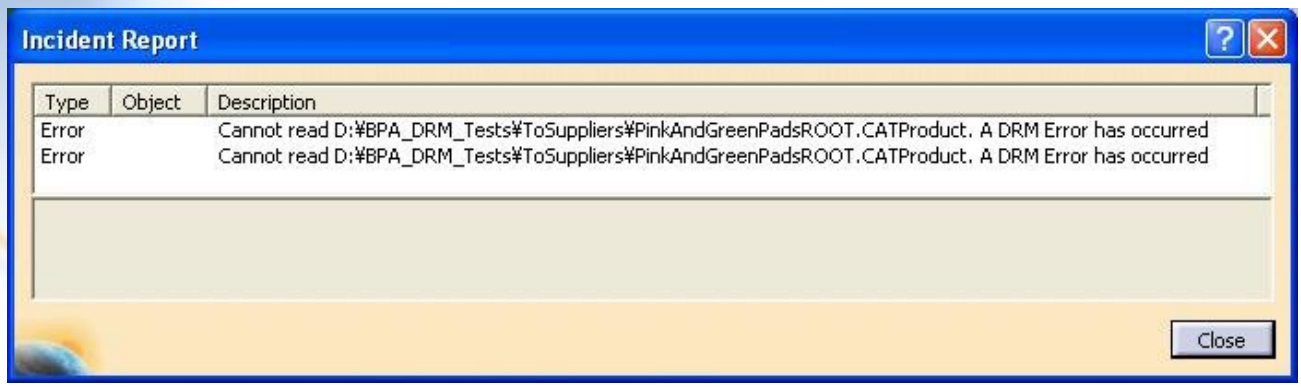
DRM protection is supported in the CATIA session by the following file types:

- CATPart
- CATProduct
- CATDrawing
- CATShape
- CATAnalysis
- CATMaterial
- CATProcess
- CATSystem
- CATSwl
- 3dxml
- cgr
- catalog

For all the other types of file, see “Usage for other files”.

As long as no encrypted file has been opened in the session, working on non encrypted files is possible, as well as saving them.
Once an encrypted file has been opened in the CATIA session, edition of non encrypted files is possible, but saving them is no more allowed. However, creating a new file, editing it, and saving it are possible, as this new file will be saved in an encrypted format.
It is not possible to *SaveAs* an encrypted file into a non CATIA V5 format (IGES, STEP for example), except if the OEM gave the authorization. In that case, this information can be found in the file “DS9ReadMe.txt”.

You may encounter the following error when trying to open an encrypted file:

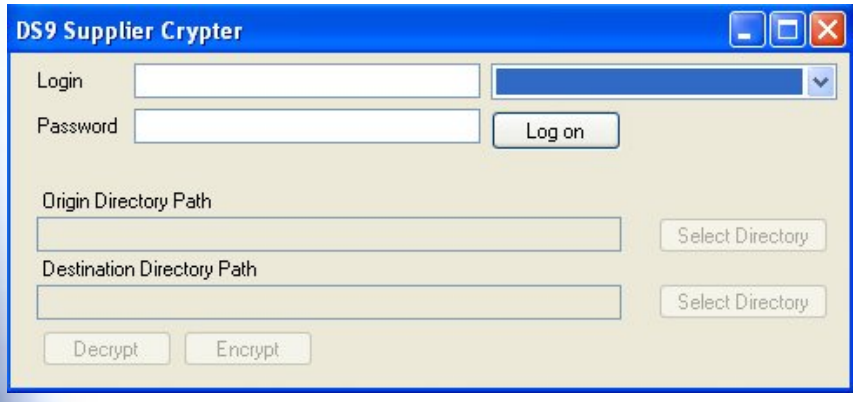


This means that your ID information does not match the ID information embedded in the protected file: you do not have the right to open this file.

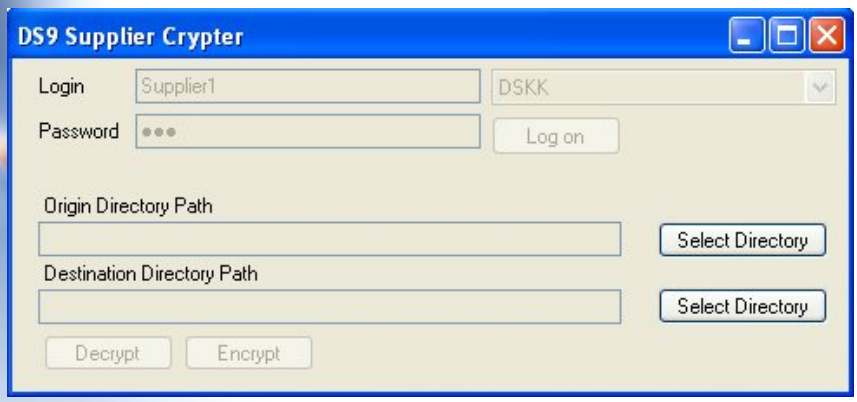
You may not be able to open an encrypted file after a certain date. This means that the OEM gave an expiry date to the encrypted file. In this case, the information about the expiry date can be found in the file “DS9ReadMe.txt”.

Usage for other files

To decrypt all the other files sent by the OEM, launch the application ISPDS9SuppCrypter.exe from the installation directory.



Select the OEM, input the correct login/password and click on “Log on” button.



Select the “Origin Directory” where the encrypted data are stored, then select the “Destination Directory” where the decrypted data will be stored. The “Decrypt” and “Encrypt” buttons will become active.

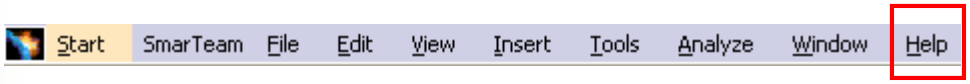
Click on “Decrypt” button to decrypt the data into the destination directory.

To encrypt the data before sending them back to the OEM, select the “Origin Directory”, where the decrypted data are stored, then select the “Destination Directory”, where the encrypted data will be stored.

Click on “Encrypt” button to encrypt the data into the destination directory.

Help About- CATIA Data Security

1. Click on Help in the Menu bar.



2. Now click on About CATIA Data Security.