

# Data Exchange Security (DS9) – Supplier application

**BPA Delivery 6 for V5R19 (V5.6)**

***User Guide***

---

# Table of Contents

---

Table of Contents .....	2
Introduction.....	3
OEM ID enrollment .....	4
Usage .....	5

# *Introduction*

---

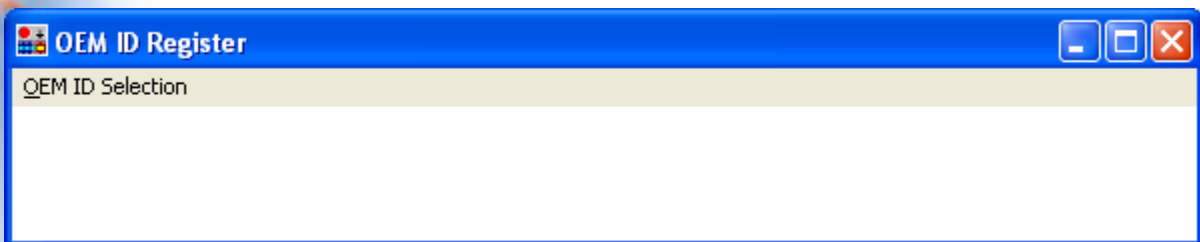
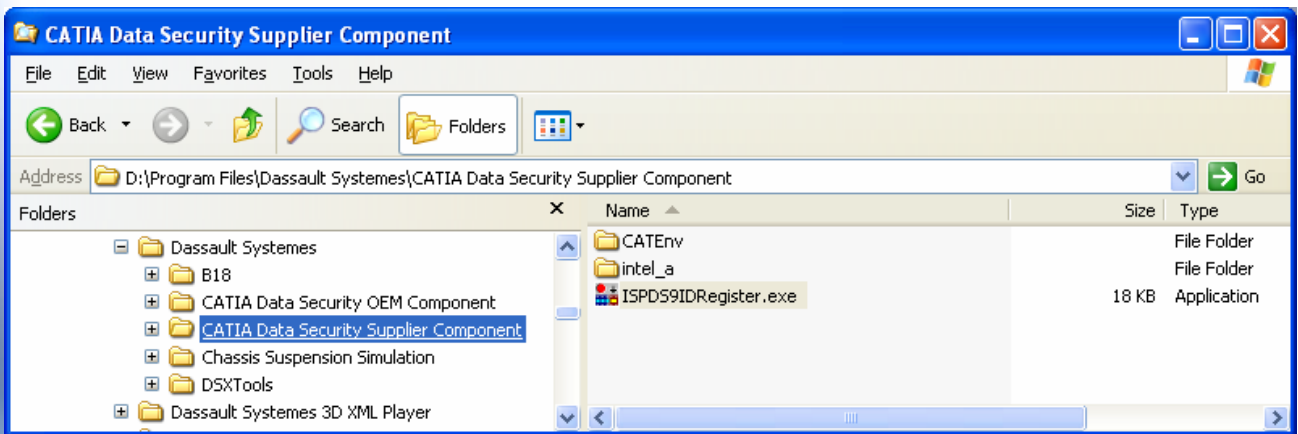
This document describes the usage of the BPA DS9 at Supplier site.

## OEM ID enrollment

After successful installation of BPA DS9 application, you must set your supplier ID information 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 called ISPDS9IDRegister.exe which was installed with the BPA DS9 in the directory "CATIA Data Security Supplier Component".



Select "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 your OEM.  
With this file the OEM should provide you with a login / password. Please keep it secret.

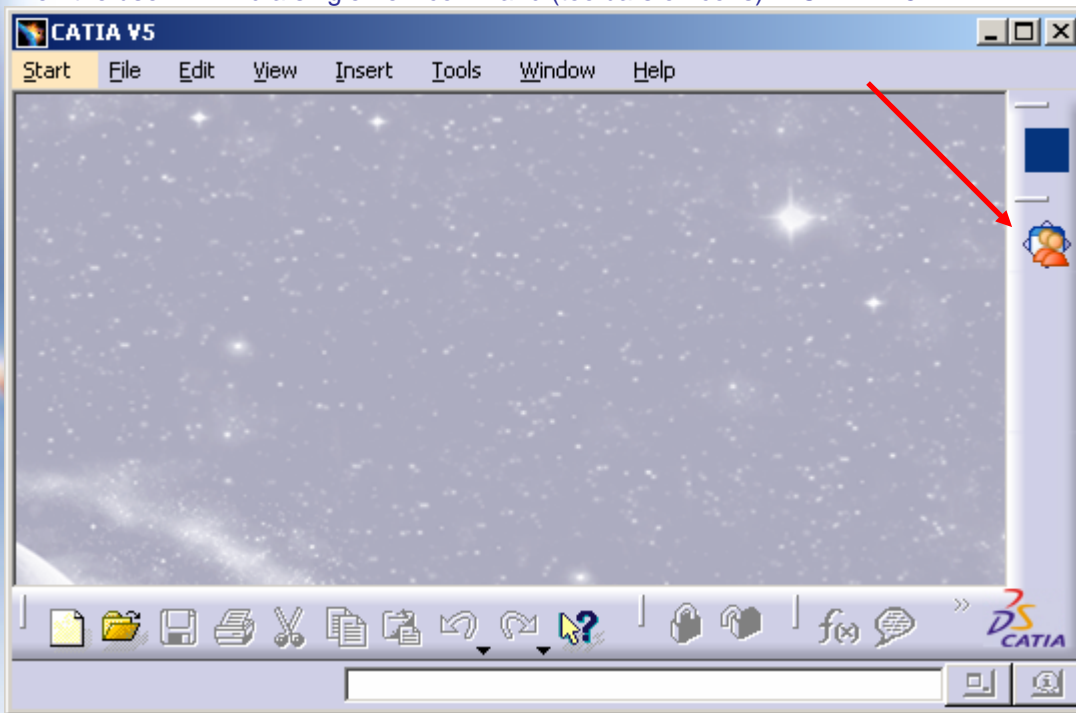
Once this setup is completed, you will be able to open any file which was encrypted by this OEM, using the same ID.

# Usage

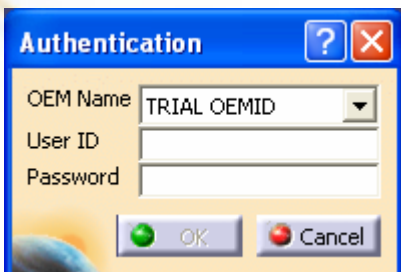
When launching the application with the new icon created on the desktop, the following message is displayed to the user:



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 for instance).

Once this operation 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 can not be done. The information about the "Read-Only" encryption can be found in the file "DS9ReadMe.txt".

Encryption is supported by the following file types:

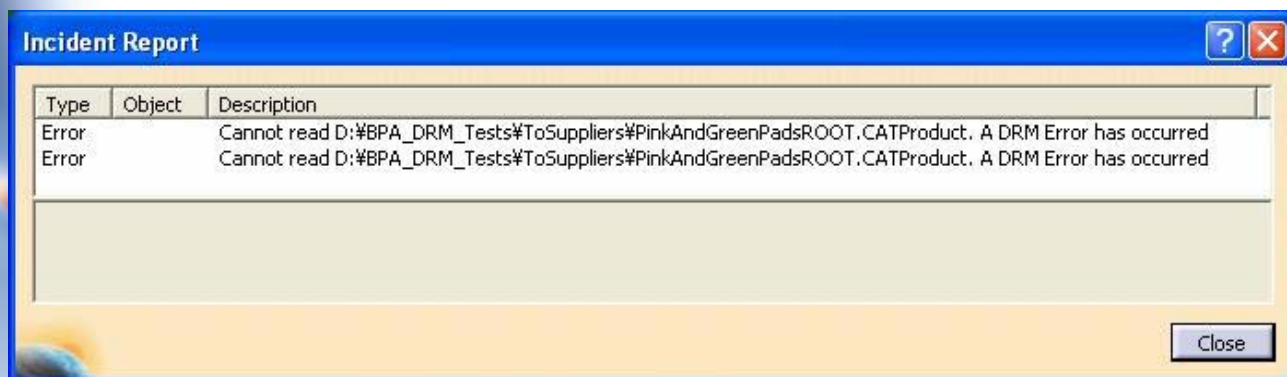
- All CATIA V5 format files, which extension starts with CAT
- 3dxml
- cgr

As long a 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).

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".