

# CATIA Data Security (DS9)

## **BPA Delivery 8 for V5R20 (V5.8)** ***Implementation Guide***

---

# Table of Contents

---

Table of Contents .....	2
Introduction .....	3
Security Implementation .....	4
Standard Security .....	4
High Security .....	5
Full Security .....	7

# ***Introduction***

---

This document describes the different levels of security in the BPA DS9 and the way to implement them.

# Security Implementation

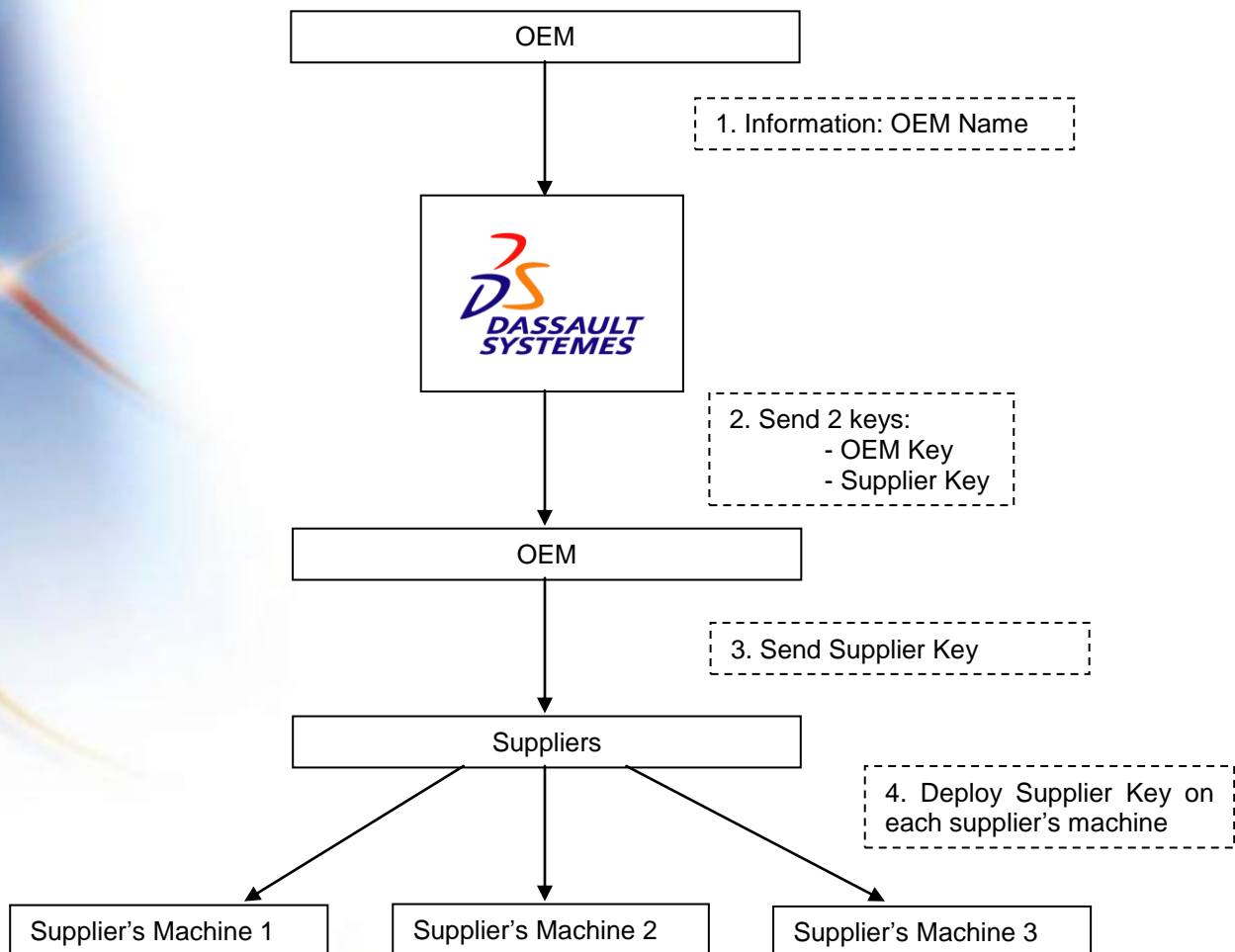
## Description:

There are 3 types of security level defined in DS9: Standard, High, and Full.  
OEM can decide which security level is suitable for its data security needs.

## Standard Security

In the standard security level, the same license key is sent to all the suppliers. No specific information is required from the suppliers.

After successful registration of the key on their machines, suppliers will be able to open and modify the encrypted data using the right login/password.



## High Security

In the high security level, a unique license key is generated for each authorized machine. At the OEM site, only the machines with their unique license can encrypt and decrypt data. On the supplier side, only the machines with their unique license can open and edit the encrypted data using the right login/password.

Each authorized machine is identified by its MAC\_ID.

This unique identifier is required in order to generate the licenses. On each machine on which DS9 Supplier Application or DS9 OEM Application is installed, a tool "DS9\_MAC\_ID.exe" gives the MAC\_ID information of the current machine. Here is an example:

```
IP : 10.90.131.177
MAC Address : 02-00-4C-4F-4F-50
MAC ID : 02004C4F4F50
Press and key to continue
```

In this example, the MAC\_ID is: 02004C4F4F50.

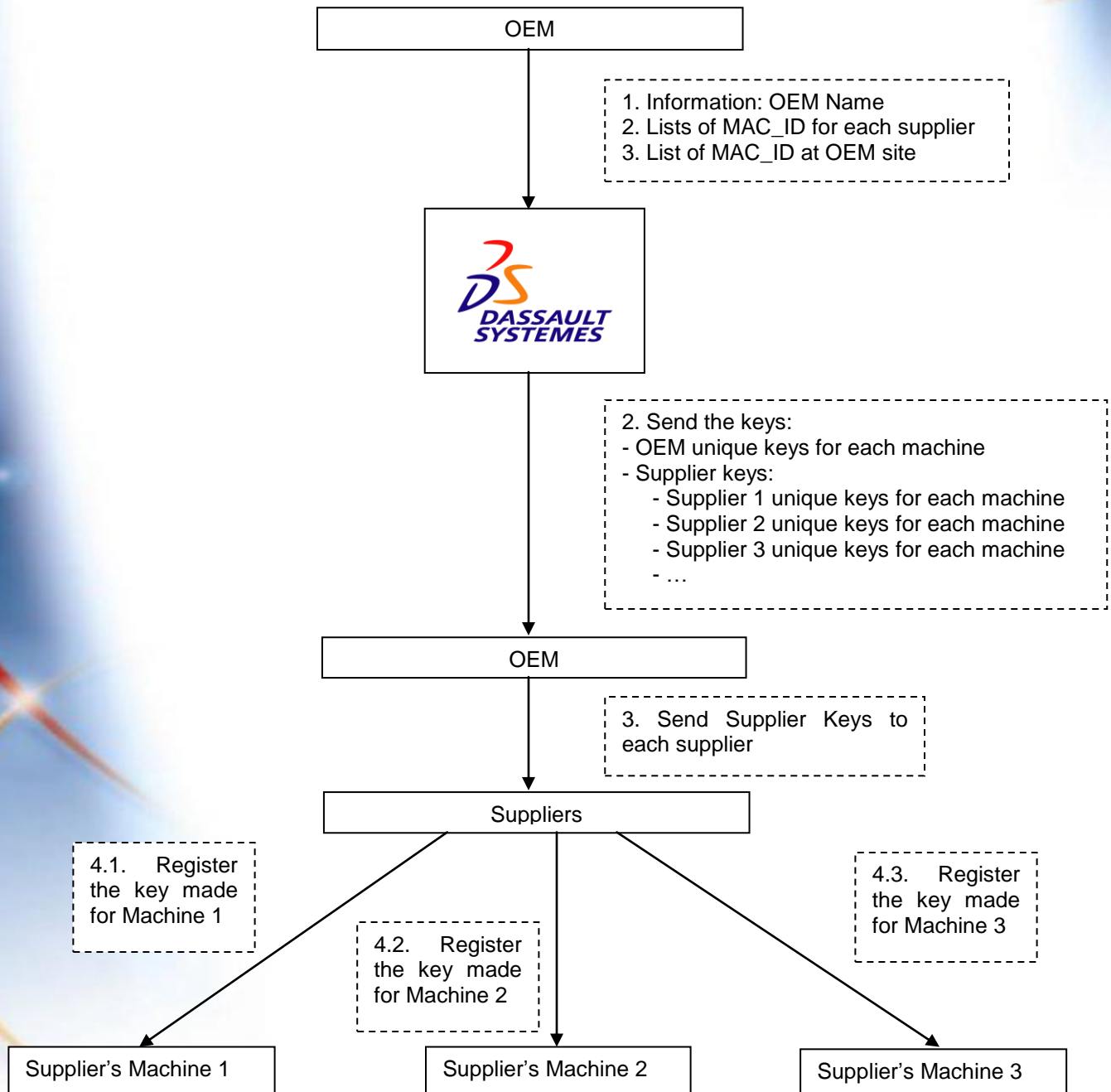
Suppliers must provide their OEM with the list of MAC\_ID of the machines they want to use to open and edit encrypted data. This list must be a text file (Name\_of\_the\_supplier.txt) in which each line correspond to one MAC\_ID. Here is an example:

Supplier1.txt

```
02004C4F4F50
00564ACF4D78
1300554F4E10
...
```

OEM must create the same document for its own machines which will be able to encrypt/decrypt data (Name\_of\_the\_OEM.txt).

All the lists must be sent to Dassault Systemes by the OEM so the licenses can be generated.



## Full Security

In the full security level, the same license key is sent to all the suppliers so they can request the authorization to decrypt the data from a server on the OEM side. OEM can manage in real-time the list of authorized users and keep information on the file accesses.

The authorized users can be identified by the server by one of the following information:

- 1) MAC Address
- 2) Public + Private IP
- 3) MAC Address + Public + Private IP

To get the MAC Address info and Private IP of a machine, you can use "DS9\_MAC\_ID.exe" command provided by DS9.

Public IP can be provided by IT department.

The number of simultaneous connected users on the server is limited by the Server License. This license is unique and will work only for one OEM server identified by his public IP.

