CDSL/OPS/DP/EASIE/2800 **January 09, 2012**

MIGRATION OF DIGITAL CERTIFICATE TO SHA-2 DIGITAL SIGNATURES CERTIFICATES (DSC)

The Controller of Certifying Authorities of India **(CCA)** has published **Digital Signature Certificate (DSC)** Interoperability Guidelines in December 2009, with a view to unify the profiles of the DSCs issued by the various Certifying Authorities (CAs) in India. The difference in the certificates issued by various CAs resulted in end users having to procure DSCs from multiple CAs, for use across different applications. The Interoperability Guidelines aims at facilitating the user to use a DSC procured from any licensed Certifying Authority across various applications, thus simplifying the usage of DSCs.

The Guidelines recommend the use of SHA-2 as the Hashing Algorithm while creating Digital Signatures and use of a 2048 bit RSA key during generation of DSCs. TCS-CA being a licensed Certifying Authority has made necessary changes and hence CDSL will be carrying out release at CDSL end on **Friday, 13 January 2012** in order to accommodate SHA-2 Certificates and SHA-2 based signing.

All users i.e. BO / CBO / CM and DP who are using e-tokens with digital signature are required to download and install the new SafeNet drivers at their machine from where the easiest facility (eToken) is used. The old drivers will not work after this release and hence users are requested to complete download and installation of new drivers by **Friday, January 13, 2012.**

To identify the List of users with Account of Choice users, DP is requested to visit their DP login and select List of Easiest Users from their Login.

DPs are advised to note the details of this communiqué and also instruct their clients who have opted for Account of Choice facility in their Easiest Login.

- **Annexure A - Download and Installation procedure of Safenet drivers by the Clients / Users.**
- **Annexure B -Changes in the Screen while using Digital Signature.**
- **Annexure C - Pre requisites of Operating Systems, Browsers and Java**

Queries regarding this communiqué may be addressed to:

CDSL – Helpdesk (022) 2272-8642, 2272-8427, 2272-8624, 2272-8693, 2272-8639, 2272-1261, or 2272 2075. Emails may be sent to: helpdesk@cdslindia.com.

sd/-

Jitendra Chad
Vice President – Information Technology

Annexure A:

Download and Installation procedure of Safenet drivers by the Clients / Users

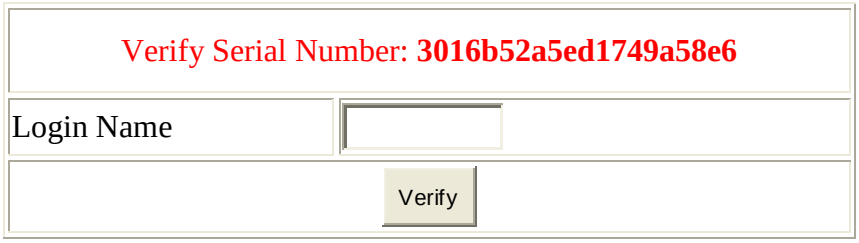
1. This driver is compatible to the existing as well as the newer version of Signing to be migrated after 13 January 2012.
2. Download new Safenet drivers from link: www.cdslindia.com/help.html. -click on 'Download Ikey 2032 Drivers(New)'. Select option to save on your machine.
3. The following is the process for installation of the drivers:
    - Uninstall the Safe Net drivers already present.

      Windows XP:

        a. Go to Start,
        b. Control Panel,
        c. Add or Remove Programs,
        d. Look for the name "SafeNet" and Remove/Uninstall the drivers,
        e. Look for the name "iKey" and Remove/Uninstall the drivers,
        f. Look for the name "CIP Utilities" and Remove/Uninstall the drivers.
        g. Once successfully done, reboot the system.

      Windows 7:

        a. Go to Start,
        b. Control Panel,
        c. Programs and Features,
        d. Look for the name "SafeNet" and Right click on the name, select Remove/Uninstall.
        e. Look for the name "iKey" and Right click on the name, select Remove/Uninstall,
        f. Look for the name "CIP Utilities" and Right click on the name, select Remove/Uninstall.
        g. Once successfully done, reboot the system.
    - Install the New Safe Net Drivers as downloaded from the site. The driver is zip file named " SafeNetAuthenticationClient_latest.zip" (To install: Double click on the ZIP file to extract the drivers and then to install the drivers right click on SafeNetAuthenticationClient-x32-8.1.msi and install. After installation, Reboot the system.
    - Check the correctness of the installation from the following URL: www.cdslindia.com/verifytoken.jsp. For this the client has to keep his token in the USB slot. Enter the Login name and select Verify.
    - In case the drivers are correctly installed the Certificate Serial Nos. will appear above login name and will indicate that the Drivers are perfectly installed. (Screen attached below)



- In case the certificate serial numbers are not displayed, it indicates that installation of drivers are not proper, please proceed again with the installation or Contact Help Desk Team at CDSL.

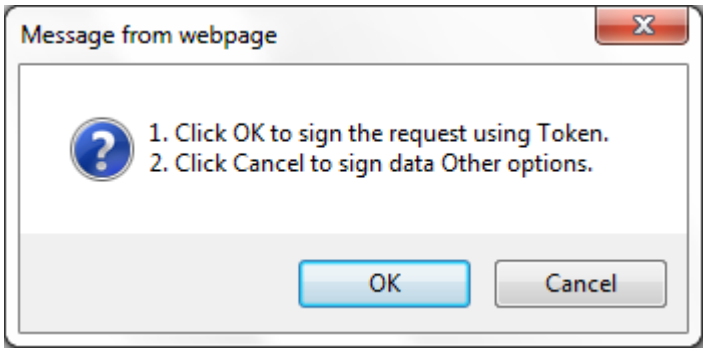
Annexure B:

Changes in the Screen when Digital Signature is invoked.

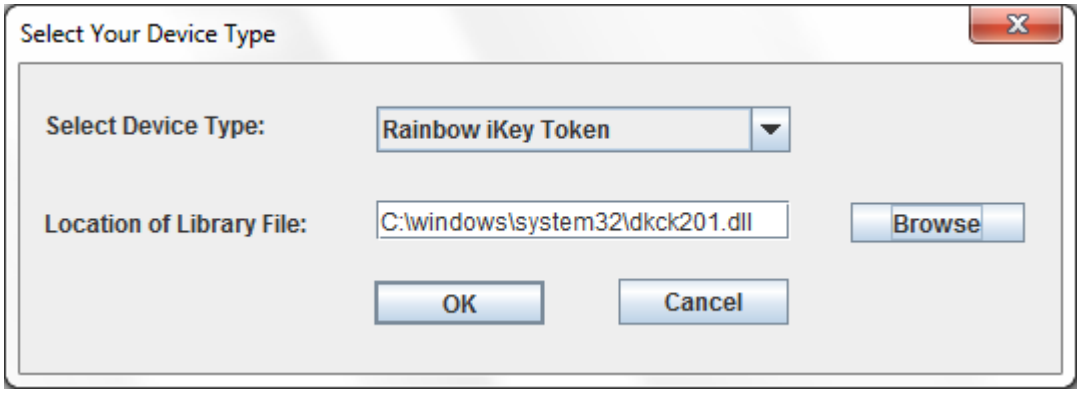
When the user goes in for authentication using digitally signature for any of the Transaction / Upload / Authenticate / Reject the entries the following screen shots will appear in the first instance:

(These screens are effective after 13-January -2012 releases)

1. The user using the token provided by CDSL shall select the Option 1

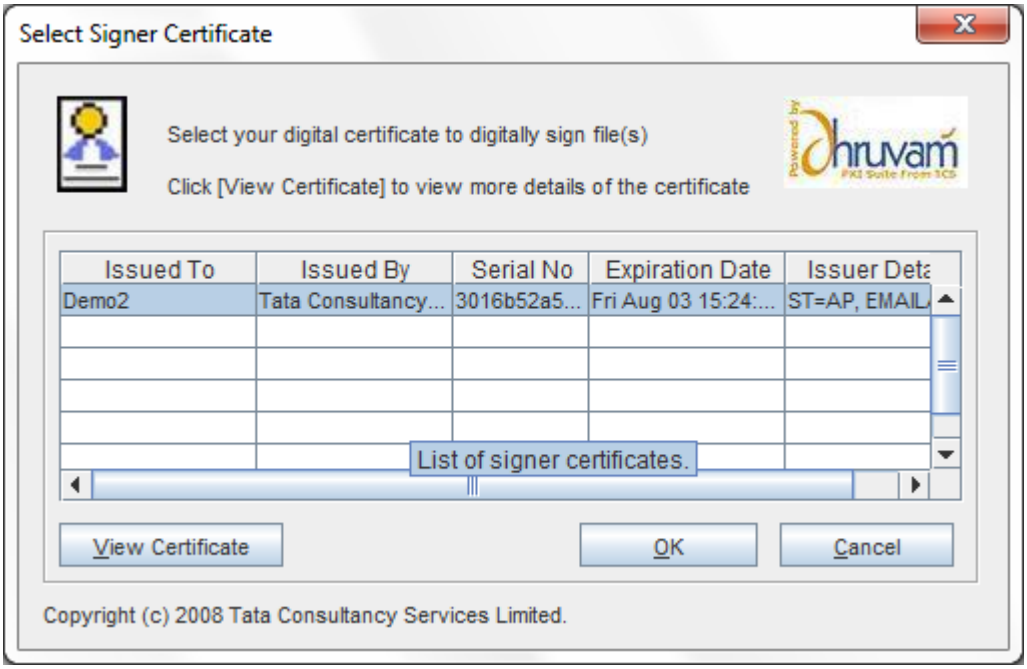


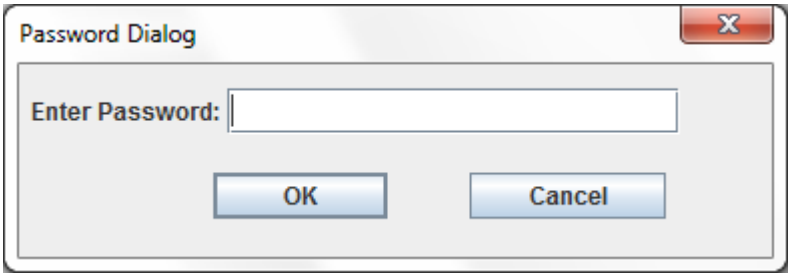
2. The option to be selected will be: Rainbow ikey Token for CDSL issued tokens



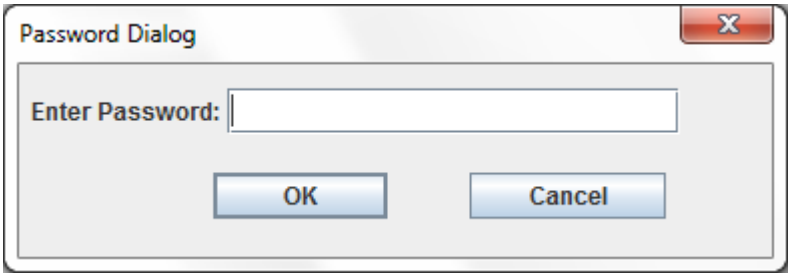
The default dll is set to c:\windows\system32\dkck201.dll

3. The TCS Select Signer Certificate pop up appears for the user to sign the entry.

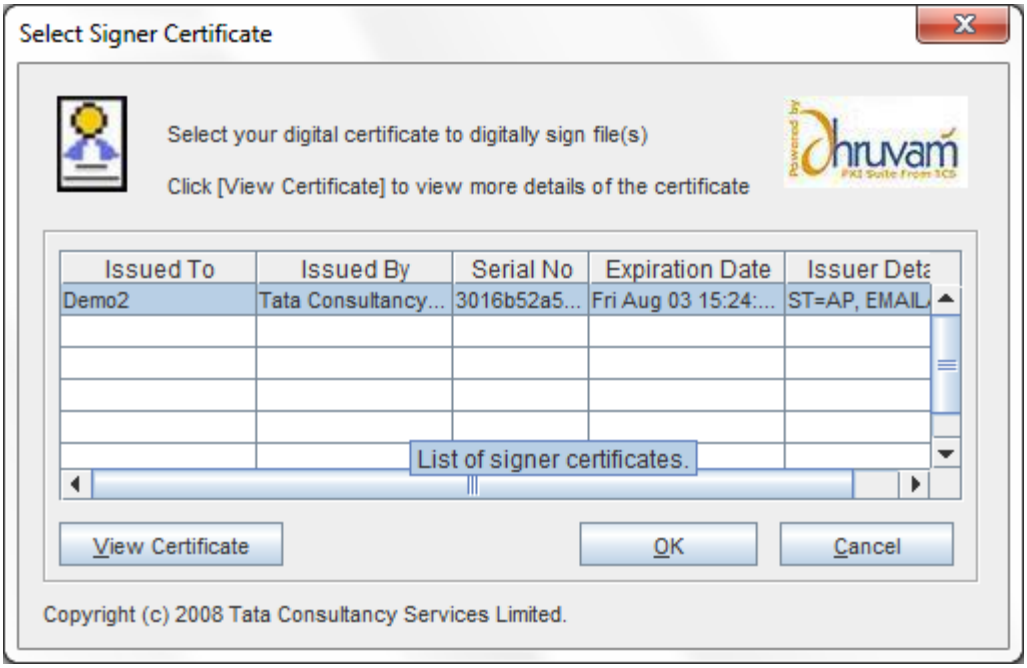




4. The Password of the ikey 2032 will have to be entered
5. The final "Authentication Successfully" appears presently remains unchanged
6. The second time when the user uses digitally signature for any of the Transaction / Upload / Authenticate / Reject the entries only the following screen will appear:



7. After the successful password identification the TCS Select Signer Certificate pop up appears:



8. The final “Authentication Successfully” appears presently remains unchanged

Annexure C:

Pre Requisites of Operating Systems, Browsers and Java

Pre-requisites

1. Supported Operating Systems : Windows XP SP3, Windows 7, Windows Vista
2. Supported Browsers: Internet Explorer 7 and above
3. Java : JRE 1.6.0_29 or above
4. Only JRE 32-bit should be used even if the Operating System is 64-bit.
5. The subscriber Signing Certificate should be available only in the Crypto Token to be accessible to download the corresponding encryption certificate from TCS-CA website.
6. Supported Crypto tokens : SafeNet iKey 2032
   Available for download from:

CDSL:

To update the latest Java Version:

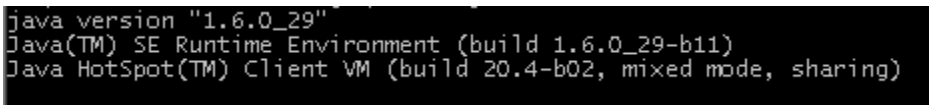
Download from http://download.oracle.com/otn-pub/java/jdk/6u30-b12/jre-6u30-windows-i586.exe

or

Visit www.java.com and update your system.

How to know JRE installed is 32-bit:

1. Go to Start,
2. Click on Run,
3. Type “cmd” and click on enter,
4. Type “java –version”
5. Output will look like below if it is 32-bit JRE



6. If you find “64-bit” in the output then it is a 64-bit java