**Instructions for Updating NY-DEx Client Computers for DCJS Data Power Server Certificate Updates**

**Purpose:** On 9/2/2015, the DCJS Data Power production servers will have their security certificates upgraded. These servers host the web service that allows the NY-DEx SJS clients to communicate with the server to submit records from SJS to the NY-DEx repository. In order to avoid disruption of the submission of records to the NY-DEx system, the certificates on the client computers must be updated before 9/2/2015. This document will document the steps to perform this update.

**What needs to be done:**

* The NY-DEx SJS client uses Java to call the web service on the DCJS Data Power servers.
* The security certificates used by Java to communicate with servers are located in a file called cacerts.
* The cacerts file is located under the lib\security folder found under the location where the Java version is located.
* This folder was special security rights on it, so when modifying the contents of the folder the user or updating process must have administration rights.
* There can be multiple versions of Java that need to be updated.
  + However, ***not all versions of Java need to be updated***.
  + Some versions of Java are installed as part of an application and we do not wish to interfere with the application by updating these versions of Java.
    - These versions will usually be under a vendor folder like Oracle or Adobe.
  + The NY-DEx client uses the common versions of Java found under their default locations under the folder ***C:\Program Files\Java or C:\Program Files (x86)\Java***
    - If a common version of Java is installed in a non-standard location, then if might need to be updated as well.
* The cacerts file will need to have the following certificates included in it.
  + GlobalSign-Intermediate.cer
  + GlobalSign-Root.cer
  + ITS-Intermediate.cer
  + ITS-Root.cer

**Who will perform the update:**

Since there is only about a two week window to avoid disruption of service, getting all NY-DEx SJS client computers updated in time will be a challenge. This document will describe the steps for performing an automated update that will hopefully prove easy enough for local agencies to perform on their own. It is estimated that the automated update should take about ½ hour to complete. However, if an agency does not feel comfortable or does not have the staff to perform the upgrade, they can schedule an Easy Assist session with the NY-DEx team to perform the update.

1. Agency self update.
   1. Review this document to determine if you are comfortable performing the automated process.
   2. If so let the NY-DEx team know:
      1. This is the update plan your agency decided to follow.
      2. When the update is completed, so we can monitor that we are receiving records.
2. If your agency is not comfortable doing the update contact the NY-DEx team to schedule a time for an Easy Assist session.
   1. However, prior to the session please download the update package from the link ***Data Power Certificates 9/2/2015 Update*** from under the NY-DEx client tab on the NY-DEx web site at <http://www.criminaljustice.ny.gov/xnysit/nysit.html>.

**Methods for updating cacerts file:**

These two methods are mutual exclusive, so pick the best method for your agency.

1. Replacing the local cacerts file with a copy of the cacerts that includes the new certificates.
   1. ***This is the preferred method because it can be automated up to a point.***
   2. The automated method is not destructive and can easily be backed out of by restoring the original cacerts file with a backed up copy created during the process.
   3. If a backup copy of the original cacerts file cannot be created, the cacerts file will not automatically be updated.
   4. An audit trail of what is to be affected and want was done will be provided via log files.
   5. The replacement copy of the cacerts file is based on the jre1.8.0\_51 release version of the cacerts file.
      1. This is the latest Java release available at this time.
      2. It will include the latest default certificates found in the cacerts file provided by Java plus the four required DCJS certificates.
2. Updating the local cacerts file in place using the keytool tool.
   1. ***This method is more difficult because they are multiple steps needing user interaction, so it is a manual process.***
   2. If you have applications on your computer that have updated the cacerts files in the common default Java locations with special certificates, then you will need to update the current cacerts with the new DCJS certificates.
      1. The common default locations are under the folders ***C:\Program Files\Java or C:\Program Files (x86)\Java.***
   3. Generally, if an application is using special certificates, it will have its own version of Java “*embedded*” somewhere under its installation path.
      1. Examples of “*embedded*” Java versions can be found under Oracle or Adobe product folders depending on what vendor software you have installed.
   4. This method of updating the cacerts file is not recommended because it is probably not necessary in most cases and is a manual process.

**Instructions for replacing cacerts file (preferred method – just the steps):**

See following section for detailedexplanation of what happens at each step**. *This process could be performed manually, but we have provided a safe automated method that will cover updating all common Java versions located in the default folders.***

1. Review this document for a general understanding of what needs to be done.
2. Download the update package.
3. Extract the contents of the zip file using the defaults.
   1. ***The contents of the update package must reside in the folder*** ***C:\NYDEX\_CLIENT\DataPowerCerts\_2015\_09\_02\_Update***.
4. Double click on DPCerts\_Upgrade.vbs.
5. Right click on the DPCerts\_Upgrade.bat file and ***select “Run as Administrator”.***
6. Open the DPCerts\_Upgrade\_Batch{run time of the batch file}.log file to verify that the updates where successful.
   1. ***If not successful, the batch file might have been run without administrator rights.***
   2. Run batch file again with administrator rights.
7. ***Optional:*** If you wish to see what folders have a cacerts file on the C: drive double click on the batch file cacert\_search.bat.
   1. Check the generated cacert\_search.log to see where cacerts files are located.
   2. The batch file may take a little time to run.
   3. Don’t update cacert files embedded under applications such as Oracle or under the path of other vendor installations.
8. ***Optional :*** If you discover cacerts files in the generated cacert\_search.log that need to be updated manually do the following:
   1. Make a backup of the cacerts file.
   2. Copy the cacerts\_DPCerts\_Upgrade\_Master to the cacerts file.
   3. These locations will be versions of Java that ***you have installed*** but not under the default locations.
9. If the cacerts files have been updated successfully, the NY-DEx client will submit records as normal during the regularly scheduled time.
10. If necessary revert back to original cacerts file using the backup copy.
11. Notify the NY-DEx team that you have updated the cacerts file(s).

**Instructions for replacing cacerts file (preferred method – detailed description):**

***See previous section for just the steps needed to be performed. This are the same steps with more detail provided****.*

1. Review this document for a general understanding of what needs to be done.
   1. If you don’t feel comfortable performing the update yourself contact the NY-DEx team to setup an Easy Assist session.
   2. ***Prior to the session, download the update package to the local computer.***
2. Download the update package
   1. The package is located on the NY-DEx website at <http://www.criminaljustice.ny.gov/xnysit/nysit.html> under NY-DEx client tab with the link ***Data Power Certificates 9/2/2015 Update***.
   2. The folder ***C:\NYDEX\_CLIENT*** should already exist on the client computer.
      1. If not create the folder.
      2. The folder must on the C: drive.
   3. Save the file to ***C:\NYDEX\_CLIENT***
      1. Or to a location that you can find and then copy to ***C:\NYDEX\_CLIENT***
   4. Extract the contents of the zip file using the defaults
      1. The contents will be extracted to a folder called ***DataPowerCerts\_2015\_09\_02\_Update*** under the folder ***C:\NYDEX\_CLIENT***.
   5. The contents of the downloaded package must reside in the folder ***C:\NYDEX\_CLIENT\DataPowerCerts\_2015\_09\_02\_Update.***
      1. ***Some parts of the automation process have a hard coded path to this exact location, so the contents must reside at this exact location.***
3. What the extraction folder contains
   1. DPCerts\_Upgrade.docx
      1. These are the instructions for updating the certificates for the 9/2/2015 change.
   2. cacerts\_jre1.8.0\_51
      1. This is the default cacerts file that comes with the latest Java runtime version to date jre1.8.0\_51.
      2. The cacerts file has been renamed from cacerts to cacerts\_jre1.8.0\_51.
      3. This cacerts file contains all of the latest default certificates provided by Java.
      4. ***Not needed for this process, but included as a reference.***
   3. cacerts\_DPCerts\_Upgrade\_Master
      1. This is the base cacerts jre1.8.0\_51 version file updated with the four DCJS certificates.
      2. This file will be used to replace the client copies of the cacerts file ***that need to be updated.***
   4. The DCJS certificate files (***not needed for this process, but included as a reference***).
      1. GlobalSign-Intermediate.cer
      2. GlobalSign-Root.cer
      3. ITS-Intermediate.cer
      4. ITS-Root.cer
   5. keytool.exe
      1. This the tool used to update the local cacerts files in place.
      2. ***Not needed for this process, but included as a reference.***
      3. Each version of Java has this tool located in its /bin folder.
      4. This version is from Java release jre1.8.0\_51.
      5. Provided here to make the manual update in place easier.
   6. DPCerts\_Upgrade.vbs
      1. This is a vbs script that will search for cacert files under the folders ***C:\Program Files\Java or C:\Program Files (x86)\Java.***
      2. The NY-DEx client will only use Java installed on the C: drive, so the automated script will only look here.
      3. ***The script will only look for Java installs under the folders C:\Program Files\Java and C:\Program Files (x86)\Java.***
         1. These are the common default locations for Java installed by the user.
      4. This is to avoid interfering with versions of Java installed with a specific application.
      5. If you have installed a version of Java not in the standard location under the folders mentioned above, you will need to
         1. Backup the current cacerts file in the folder.
         2. Copy the cacerts\_DPCerts\_Upgrade\_Master file to the folder naming it cacerts.
   7. cacert\_search.bat
      1. This batch file will search for cacerts files on the C: drive.
      2. It will write the results out to the file cacert\_search.log of what folder the file is located.
      3. Perform this step if you are curious about how many versions of Java you have installed on your C: drive.
   8. update\_cert\_in\_place.txt
      1. This file contains a text version of the commands necessary to update the cacerts file in place.
      2. ***Not needed for this process, but included as a reference.***
4. Double click on DPCerts\_Upgrade.vbs. This will cause the script to run and produce
   1. A generated batch file called DPCerts\_Upgrade.bat with commands for updating the cacerts files.
   2. A generated log file called DPCerts\_Upgrade\_On\_{runtime of the script}.log detailing the folders that will be updated by the batch file and a copy of the batch file in case needed for future reference.
   3. ***The script will not perform any actions other than creating the batch file and log file.***
5. Right click on the DPCerts\_Upgrade.bat file and ***select “Run as Administrator”***
   1. ***The security folder where the cacerts file is located needs administrator rights to update.***
   2. The batch file is want does the actual update work.
   3. The batch file will back up the cacerts files for Java versions ***under the folders C:\Program Files\Java and C:\Program Files (x86)\Java*** to a file with the long name cacerts\_nydex\_09\_02\_2015\_updated\_on\_{runtime of the script} .
   4. The batch file will update the cacerts files for Java versions ***under the folders C:\Program Files\Java and C:\Program Files (x86)\Java*** using the cacerts\_DPCerts\_Upgrade\_Master file.
   5. The batch file will generate a log file called DPCerts\_Upgrade\_Batch{run time of the batch file}.log that shows the result of the commands issued in the batch file.
6. Open the DPCerts\_Upgrade\_Batch{run time of the batch file}.log file to verify that the updates where successful.
   1. ***If not successful, the batch file might have been run without administrator rights.***
   2. ***If so, rerun the batch with administrator rights and repeat step 6.***
7. ***Optional:*** If you wish to see what folders have a cacerts file double click on the batch file cacert\_search.bat.
   1. Check the generated cacert\_search.log to see where cacerts files are located.
   2. The batch file may take a little time to run.
   3. ***Don’t update cacert files embedded under applications such as Oracle.***
   4. Java versions ***under the folders C:\Program Files\Java and C:\Program Files (x86)\Java*** will be updated, so there is little chance that files from other locations need to be manually updated.
      1. If in doubt send the cacert\_search.log file to NY-DEx team to examine before manually updating cacert files in additional locations.
8. ***Optional :*** If you discover cacerts files in the generated cacert\_search.log that need to be updated manually do the following:
   1. Make a backup of the cacerts file.
   2. Copy the cacerts\_DPCerts\_Upgrade\_Master to the cacerts file in the folder to be updated.
9. If the cacerts files have been updated successfully, the NY-DEx client will submit records as normal during the regularly scheduled time.
10. If the cacerts file needs to resorted to original copy
    1. Use the DPCerts\_Upgrade\_Batch{run time of the batch file}.log to determine which files where modified in which folders.
    2. Go to the folders in question.
    3. Delete the modified cacerts.
       1. This is a copy of the cacerts\_DPCerts\_Upgrade\_Master which still exists.
    4. Rename the cacerts\_nydex\_09\_02\_2015\_updated\_on\_{runtime of the script} file to cacerts
11. Notify the NY-DEx that you have updated the cacerts file(s).
    1. We can monitor we are getting your submissions.
    2. We need to track who is completed so we can focus on those agencies that might need help.
    3. You can self monitor by reviewing the submission emails you receive from NY-DEx for the next couple of days.

**Instructions updating the local cacerts file in place using the keytool tool:**

1. Determine if you need to do this process.
   1. ***If you have already performed the “replacing cacerts file” process you don’t need to do this process.***
   2. This process only needs to be performed where the cacerts file needs to be updated with the DCJS certificates for a cacerts file that already has application specific certificates in it.
      1. The DCJS certificates usually only need to be included in the Java versions ***under the folders C:\Program Files\Java and C:\Program Files (x86)\Java or in a user installed non-default location.***
   3. This is why we will not update cacerts files in embedded Java locations under applications such as Oracle.
2. Double click on the batch file cacert\_search.bat.
   1. Check the generated cacert\_search.log to see where cacerts files are located.
   2. The batch file may take a little time to run.
   3. ***Don’t update cacert files embedded under applications such as Oracle.***
   4. Java versions ***under the folders C:\Program Files\Java and C:\Program Files (x86)\Java*** will need to be updated plus any user installed Java versions not located in the default locations.
3. ***Make a backup of the cacerts file in the folder where the update will occur before you start the process.***
4. Copy the cacerts file from the folder you wish to update into the folder ***C:\NYDEX\_CLIENT\DataPowerCerts\_2015\_09\_02\_Update.***
5. Open a cmd window and for each Java version location that you wish to update do the following:
   1. Cd to the folder ***C:\NYDEX\_CLIENT\DataPowerCerts\_2015\_09\_02\_Update***.
   2. Note this is a word document and will not only be able to be run from the server directly if it has a copy of Word installed.
      1. The file update\_cert\_in\_place.txt contains the commands in a text file that can be easily opened from the server.
   3. ***You can copy the commands from this document or the file update\_cert\_in\_place.txt and paste into the cmd window by right clicking on the title bar of the window and selecting from the popup menu edit***🡪***paste.***
   4. Enter the command: **keytool -import -trustcacerts -alias GlobalSign-Intermediate -file GlobalSign-Intermediate.cer -keystore cacerts**
      1. When prompted for a password it will be “changeit”
      2. The default password is changeit, if it has been altered you will not be able to procede without knowing what is the new password.
      3. Answer yes to the questions.
   5. Enter the command: **keytool -import -trustcacerts -alias GlobalSign-Root -file GlobalSign-Root.cer -keystore cacerts**
      1. The password will be “changeit”
      2. Answer yes to the questions.
   6. Enter the command: **keytool -import -trustcacerts -alias ITS-Intermediate -file ITS-Intermediate.cer -keystore cacerts**
      1. The password will be “changeit”
      2. Answer yes to the questions.
   7. Enter the command: **keytool -import -trustcacerts -alias ITS-Root -file ITS-Root.cer -keystore cacerts**
      1. The password will be “changeit”
      2. Answer yes to the questions.
   8. The results can be verified by the following commands
      1. You will need the password for each command.
      2. If you updated successfully you will see the certificate listed under the alias in the file.

**keytool -list -alias GlobalSign-Intermediate -keystore cacerts**

**keytool -list -alias GlobalSign-Root -keystore cacerts**

**keytool -list -alias ITS-Intermediate -keystore cacerts**

**keytool -list -alias ITS-Root -keystore cacerts**

1. ***Copy the modified cacerts file back to the original lib\security folder*** under the Java version location you are updating.
2. Delete the modified cacerts file from the C:\NYDEX\_CLIENT\DataPowerCerts\_2015\_09\_02\_Update folder to avoid confusion for later updates.
3. Repeat steps 3 through 7 for each cacerts file you wish to update in place.
   1. If updated properly the NY-DEx will submit records during the next scheduled time.
4. Contact the NY-DEx team when you have made the update so they can
   1. Track the overall update progress.
   2. Monitor your submissions to confirm we are receiving records.
5. Check your daily submission log emails to confirm we are receiving your records.