Certificate Change FAQ and Installation Instructions

What is a web server certificate?

A certificate is a small file that uses cryptography to bind a public key used to encrypt traffic to a website with the website's ownership and identity details. See https://www.globalsign.com/en/ssl-information-center/what-is-anssl-certificate/ for more details.

What is a Certificate Authority and what is SHA1 and SHA2?

A Certificate Authority is an organization that has been established to issue digital certificates. To be trusted by web browsers and other web clients, Certificate Authorities (CA) are independently audited to ensure that they meet security requirements to protect the trust of the Internet community. When a CA issues a certificate for a web server, it signs the certificate with a digital hashing algorithm. This digital signature is used to prevent an attacker from impersonating the website. A SHA2 (aka SHA256) hash is much longer than a SHA1 hash and is therefore considered stronger cryptography. In 2014, a collective of certificate authorities and browser software developers called the CA/Browser Forum passed a resolution to deprecate SHA1 certificates in favor of SHA2 during 2016.

Certificate Pinning

Some integrations with Ariba may use "certificate pinning." This means that the system interface that connects to Ariba cloud systems only trusts a specific web server certificate and not just any valid web server certificate that is signed by a trusted certificate authority. Please be aware that you will need to import our new certificate if you use certificate pinning.

Login using Single Sign On (SSO)

Which customers are impacted?

- Customers who store or require the Ariba certificate in the configuration on their SSO application

Suggestion on what customer should do:

- Customer needs to work with their IT to confirm if they store or require the Ariba certificate in their SSO application
- Customer should also check if their configuration requires the Secure Hash algorithm to be specified (like for ADFS) and if yes, that needs to be set to SHA-256

SAP Ariba

Inbound Web service (customer to Ariba)

Which customers are impacted?

- Customers who have enabled an inbound web service are impacted regardless of their authentication mode (shared secret or certificate)

Suggestion on what customer should do:

- Customer must trust the new Ariba certificate in order to establish the HTTPS connection. Add the new Ariba certificate to the customer's truststore/keystore
- No general instructions can be given as this depends on the application customer is using and whether they require only the root, intermediate or leaf certificate
- See section "Creating a View and Importing Certificates into SAP NetWeaver Keystore" in this document for steps on how to add new certificate in PI

Outbound Web service (Ariba to customer)

Which customers are impacted?

- Customers who have enabled "Sign with Ariba Private Key" in the web services security of their Ariba outbound end point

Suggestion on what customer should do:

- Modify the authentication settings in their application to replace the existing Ariba public key with the new one
- No general instructions can be given as this depends on the application customer is using
- See section "Creating a View and Importing Certificates into SAP NetWeaver Keystore" in this document for steps on how to add new certificate in PI

Standalone ITK (using batch/script)

Which customers are impacted?

- All customers who are using ITK are impacted regardless of their authentication mode (shared secret or certificate)

Suggestion on what customer should do:

- Add the new certificate to the JAVA keystore
- Here are instructions for Windows o Download the new certificate and convert to DER-encoded binary file o Save the file to a specific location and save with filename "root.cer" (for example, C:\ITK\root.cer) o Open CMD and go to JRE location (for example, C:\Program Files\Java\jre7\bin) o Run keytool -list -keystore ..\lib\security\cacerts o Password: changeit (unless this has been manually changed by your company) o Run
  keytool -importcert -keystore ..\lib\security\cacerts -file C:\ITK\root.cer o If it fails, change the permission on the ..\lib\security\cacerts file

Standalone ITK (using SAP Netweaver)

Which customers are impacted?

- All customers who are using ITK on PI are impacted regardless of their authentication mode (shared secret or certificate)

Suggestion on what customer should do:

- Add the new certificate to PI keystore
- See section "Creating a View and Importing Certificates into SAP NetWeaver Keystore" in this document for steps on how to add new certificate in PI

ERP integration using Direct or Mediated Connectivity (master data/SIPM)

Which customers are impacted?

- All customers who are using ERP integration that connect to S4 like master data/SIPM via direct or mediated connectivity and NOT through AN are impacted

Suggestion on what customer should do:

- For mediated connectivity, see section "Creating a View and Importing Certificates into SAP NetWeaver Keystore" in this document for steps on how to add new certificate in PI
- For direct connectivity, steps are as follows: o Download the new certificate and convert to DER-encoded binary file o Login to SAP o Go to transaction code (tcode) STRUST o Double click "SSL System Client SSL Client" o Click the Import Certificates button

- Choose the certificate you exported from step 1 > click Check icon > click Allow on security question o Click Add to Certificate List button
- You should get a message at the bottom about successful import and also you should see the certificate in the certificate list
- Click Save icon at the top to save the certificate changes o You should get a message at the bottom about the save

Creating a View and Importing Certificates into SAP NetWeaver Keystore

Creating a View in SAP NetWeaver PI Keystore

Procedure

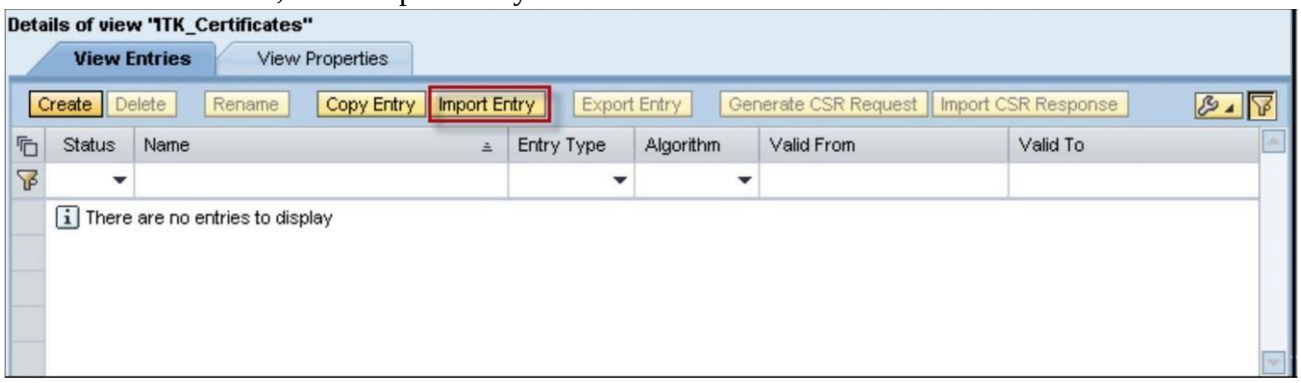
1. Log on to SAP NetWeaver PI Administrator.
2. Click the Configuration tab and click Certificates and Keys.
3. In the Key Storage tab, click Add View.

4. Enter a name and description for the view and click Create.

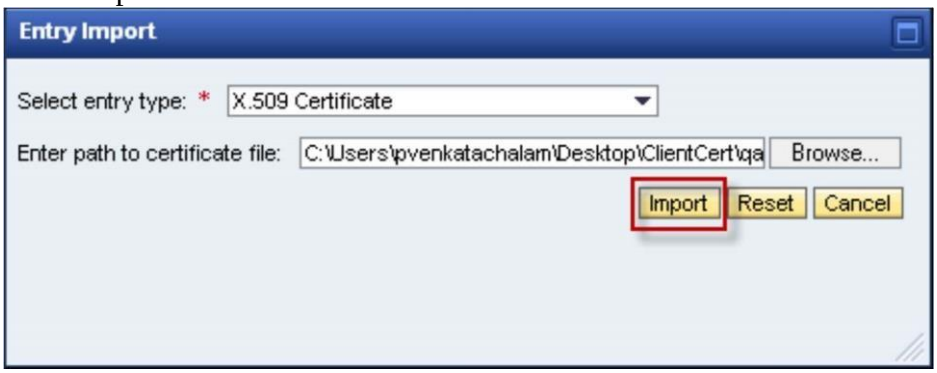
SAP Ariba

Importing Server and Client Certificates into a View Procedure

1. In the View Entries tab, click Import Entry.



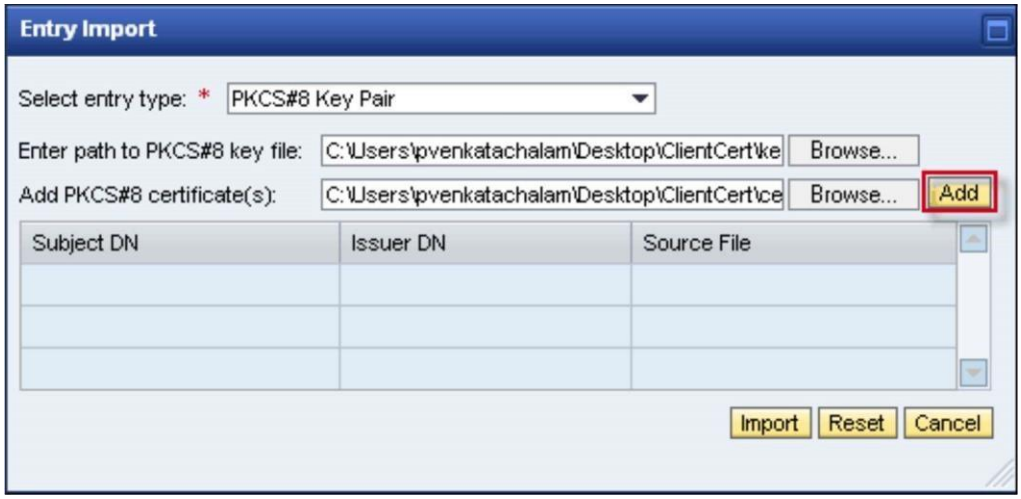
2. Click Select entry type pull-down and select X.509 Certificate.
3. Enter the path to the location of the server certificate.



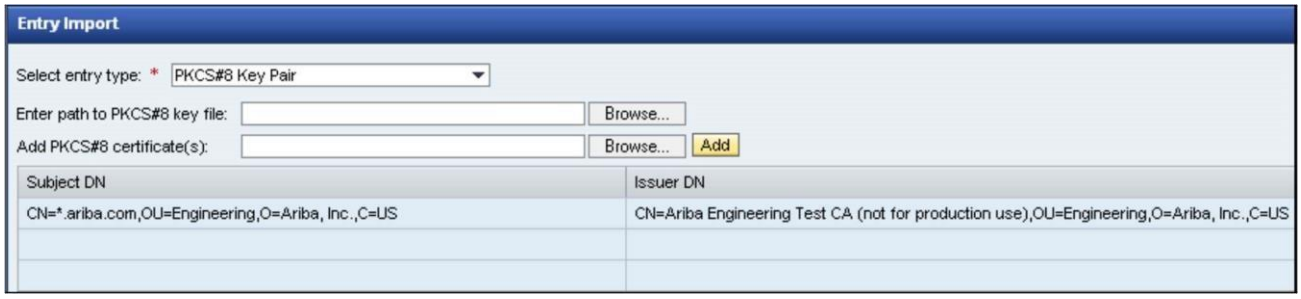
4. Click Import.

   Note
   To import the client certificate, repeat steps 1 to 4 above

5. To import the key pair, in the View Entries tab, click Import Entry again.
6. Click Select entry type pull-down and select PKCS#8 Key Pair.
7. Enter the path to the location of the key file.
8. Enter the path to the location of the client certificate.



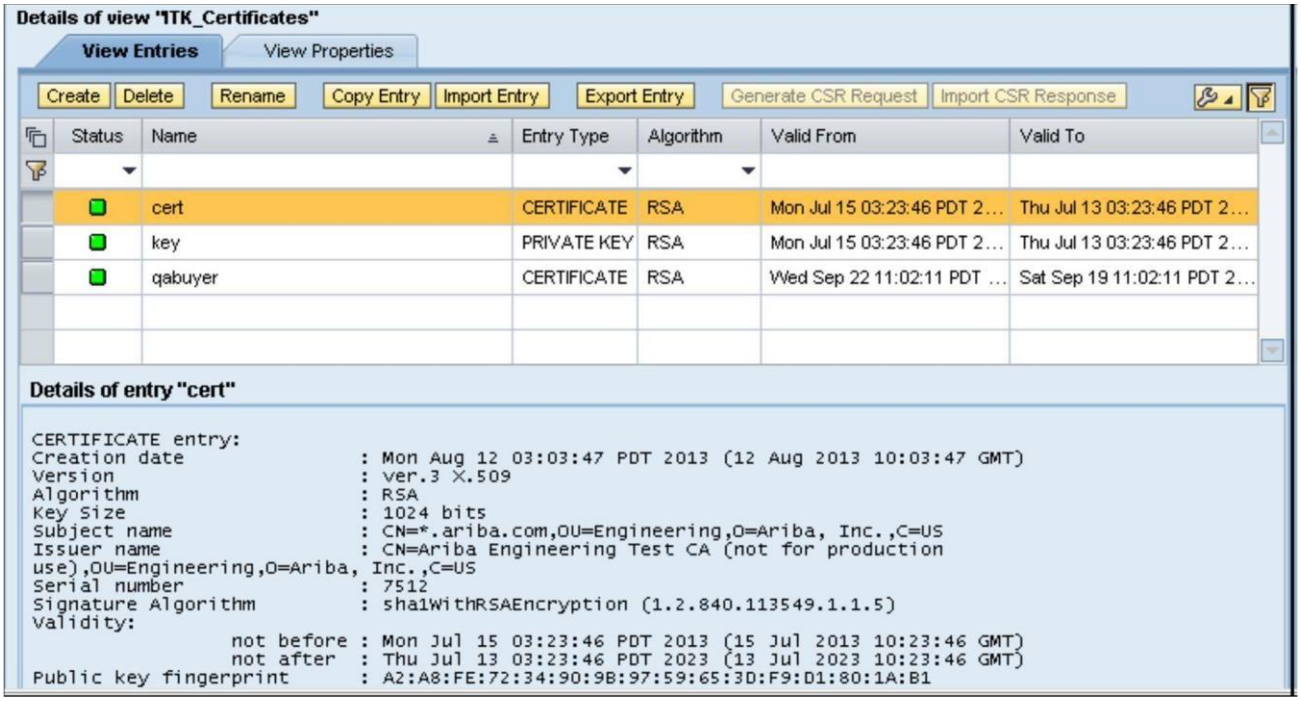
9. Click Add.



10. Click Import.

Results

The following graphic displays the details of the certificates imported into the ITK_Certificates view.



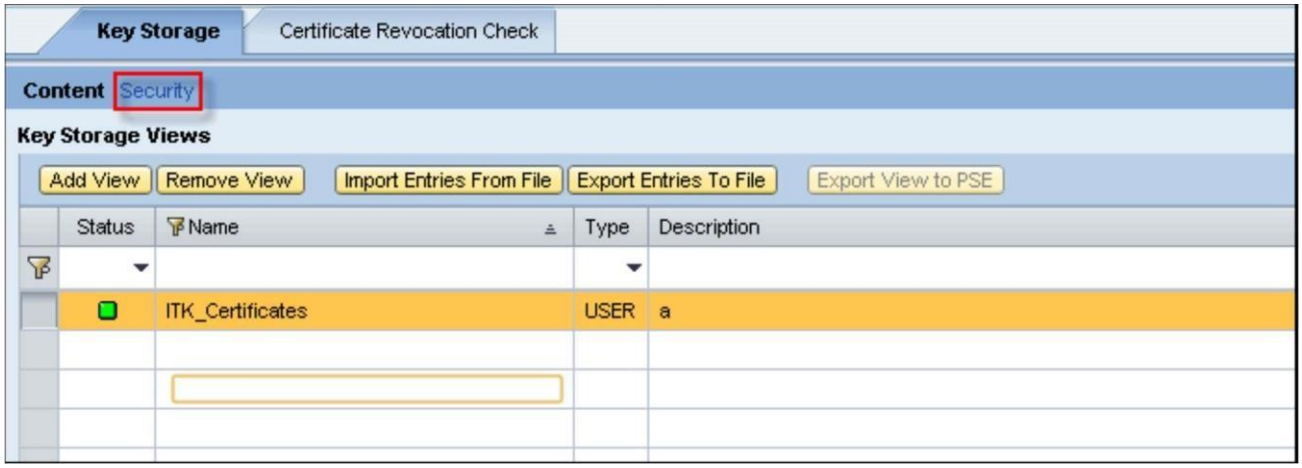
Note

In the above graphic, the server and client certificates are imported into the same view. However, you can have different views for server and client certificates.

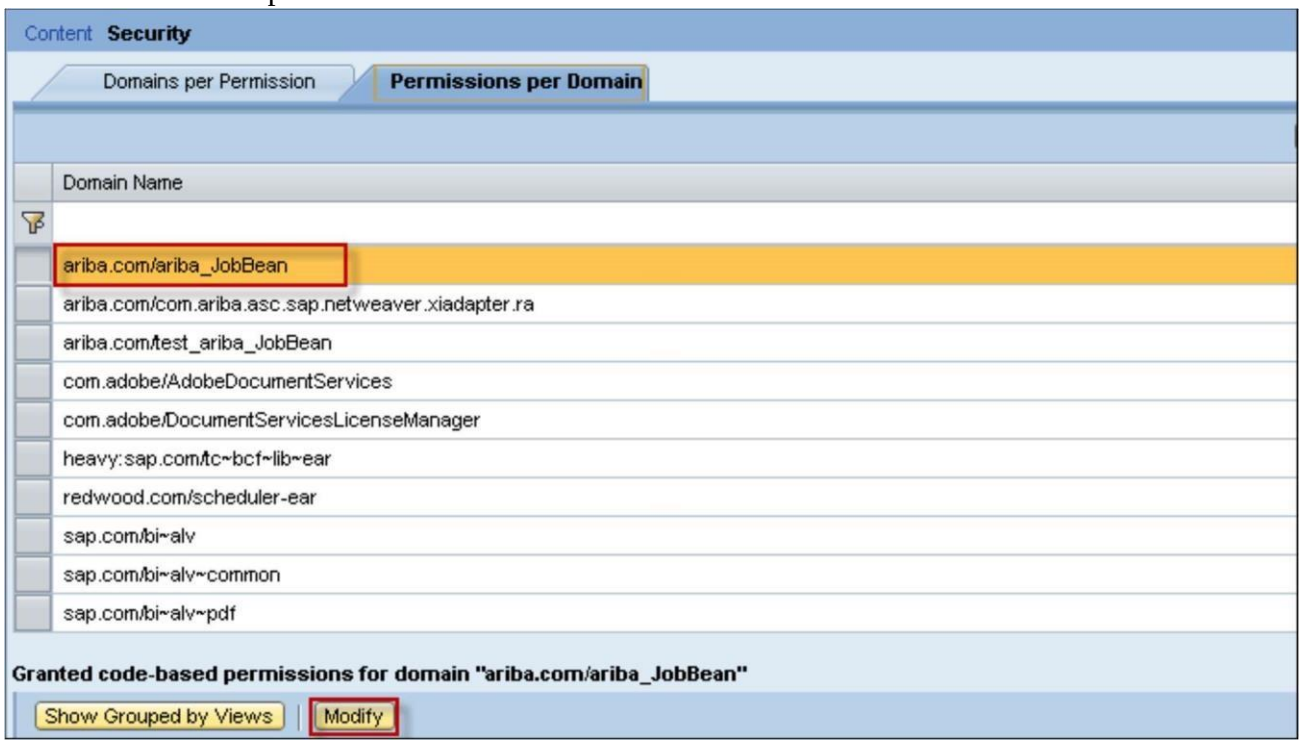
Granting Permissions for the Keystore

Procedure

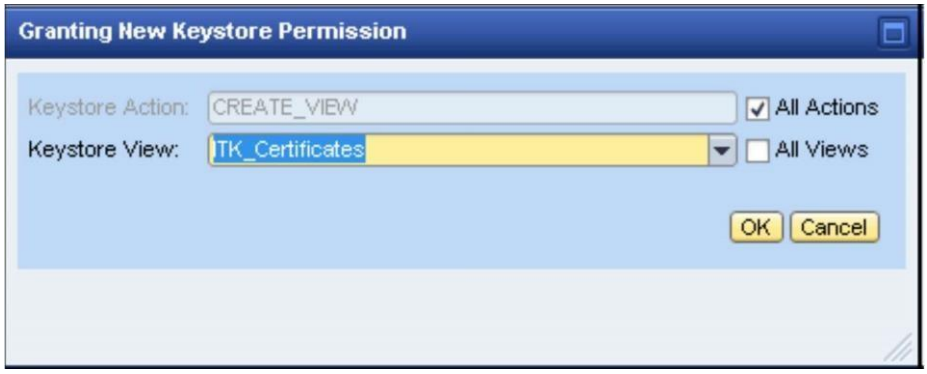
1. In the Key Storage tab, select the view for which you want to assign permissions.
2. Click the Security link next to the word Content.



3. Click the Permissions per Domain tab.



4. Select ariba.com/ariba_JobBean and click Modify.
5. Click Grant New Permission.



6. Select All Actions check box.
7. In the Keystore View field, select the view name and click OK.

SHA2 Certificate Installation for On-Premise customers:

The directions are VERY simple. It requires that the appropriate certificates get places on the file system
AND a parameter is added to the Parameters.table (for both downstream as well as upstream). Furthermore, applying the certificate to the On-Premise environment can be done at any time prior to March 16th. We suggest applying the certificate(s) when the ONP customer performs their periodic node restarts which are usually scheduled on the weekend.

1. Which certificates need to be downloaded and placed on the file system?
   - ALL On-Premise customers should download the service.ariba.com certificate and place it on their file system.
   - In addition, On-Premise customers that are hybrid integrated with an OND service (i.e. those who use APC, Spot Buy, or are integrated with OND Upstream) will also need to place the s1.ariba.com certificate on their file system as well.

2. Download the certificate(s) from Connect here and simply place them on the ONP file system under
   .../Server/etc/certs

- DO NOT click on the certificate and open it up to install it (it will pop up a window if you do this – do not proceed).
- Do this for downstream and/or upstream; both environments if suite integrated.

3. Add the following parameter to the Parameters.table(s); System.Base.CertificateAuthoritiesExtensions:

   CertificateAuthoritiesExtensions = (.der, .pem, .crt);

   Here is why. Notice that by default, the application will load certificates from "etc/certs" and "internal/etc/certs" directories. Additionally, by default it will only load certificates with extensions of ".der" and ".pem".

   The new certificates contain the extension "crt", so the Ariba ONP server will not load it by default. By modifying the parameter "System.Base.CertificateAuthoritiesExtensions" to add ".crt" to the list this addresses that issue.

4. Restart the server. DONE.