**Cannot Connect to Ariba SN - PKIX Path Building Failed:**

**Issue**

***Issue Scenario:***

SAP ECC --> SAP PI --> Ariba Network

Customers are trying to send a PO from SAP ECC to Ariba Network and the PO fails in PI with the following error.

[Error Level] 2[Error Code] ECC103[Error Desc] Ariba SN Not Available[Error Message] Cannot connect to Ariba SNcom.ariba.asc.connector.exception.AribaSNException: ***Cannot connect to Ariba SN***

***Caused by: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target***

***Caused by: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target***
***at sun.security.validator.PKIXValidator.doBuild(PKIXValidator.java:323)***
 at sun.security.validator.PKIXValidator.engineValidate(PKIXValidator.java:217)
  at sun.security.validator.Validator.validate(Validator.java:218)
  at com.sun.net.ssl.internal.ssl.X509TrustManagerImpl.validate(X509TrustManagerImpl.java:126)
  at com.sun.net.ssl.internal.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:209)
  at com.sun.net.ssl.internal.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:249)
  at com.sun.net.ssl.internal.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1185)
  ... 30 more

***Caused by: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target***
***at sun.security.provider.certpath.SunCertPathBuilder.engineBuild(SunCertPathBuilder.java:174***)
 at java.security.cert.CertPathBuilder.build(CertPathBuilder.java:238)
  at sun.security.validator.PKIXValidator.doBuild(PKIXValidator.java:318)

**Cause**

The Error “***sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target***” generally means that the certificate chain is not complete. This can occur if there is no trusted Certificate Authority's root certificate installed in the Trusted Key Store or the Certificates have not been installed on the correct path.

**Solution**

We have provided the following suggestions to the Customers and need to ensure the following:

1) To ensure that the certificates are installed properly on the JDA KeyStore and the root certificate being used is a valid CA that Ariba trusts.
The listed certificate authorities Ariba trusts can be found at: <https://connect.ariba.com/AC_Content_Details_Page/1%2C%2C161_142424%2C00.html>

2) Ariba related Certificates & Third Party Certificates provided by CA's (Certificate Authority) are to be installed in the Trust Store View "***TrustedCAs***" and the Key Store view must have ALL Permissions. Ariba always recommends to use "***TrustedCAs***" to import Ariba related Certificates.

3) The Key Store View "***TrustedCAs***" need to be mentioned in PI Communication Channel.

Additionally, we have provided the below Solution which resolved the issue.

The steps to import the security certificates for SAP NetWeaver® Adapter follow:

1. Download the VerisignCerts.zip, attached to the Service Request (SR) and unzip the contents. You find two certificates.
2. On the NetWeaver application server, issue the following command from the command line : echo $JAVA\_HOME, which gives you the location of your Java® home.
	1. Go to your JAVA\_HOME/bin and issue the following command: keytool –list –keystore /jre/lib/security/cacerts. (**This is the location of the keystore in your JAVA\_HOME directory**).
	2. This command should list a number of certificates in the keystore. If none exist, this is not the correct keystore.
	3. If it has multiple certificates, this is likely the correct location to import the new certificates and go to the next step.
3. Issue the following command to import the certificates to the keystore :
	1. Go to Java\_Home/bin; then, copy VeriSignClass3SecureServerCAG3.der and the VeriSignClass3PublicPrimaryCertificationAuthorityG5.der to bin directory.
	2. On the command line, enter:

	keytool –import –trustcacerts –alias certfile –file VeriSignClass3SecureServerCAG3.der -keystore <JAVA\_HOME>/jre/lib/security/cacerts
	3. If everything is correct, it prompts you for a password; the password is "changeit".
	4. Repeat steps a and b for the sst certificate.

Next, you must restart the Ariba XI adapter. If you still have issues, restart the J2EE® server by following these steps:

* 1. From the ICM Monitor, Admin menu, **Restart > Yes**.
	2. **Send Hard Shutdown > With Restart**.

**Additional Information**

Questions to be asked to Troubleshoot Certificate Issues:

1)      Has the KeyStore (cacerts) value configured properly in the Configuration Properties?

2)      Do the KeyStore / Trust Store View have all Permissions needed?

3)      Check, validate the Certificates and ensure all the Certificates are available in **TrustedCAs**. After this try testing with a PO / Invoice.

4)      Are latest Certificates being used?

5)      Does PROD and other Non-PROD Environments are working fine?

6)      Could you please compare the Network, (Ports) Firewall and Connectivity Settings for them? Has anything changed?

7)      Could you please check whether any Network / Firewall related changes are there? Any changes happened to JDK Key Store or JVM?

8)      When is the last successful PO sent to AN?

9)      Any recent SAP PI Upgrade or any other upgrades have been done?

10)   Restart the AN Adapter for SAP and do full PI restart if required.

***Note:***

1) PI Upgrade / Changes in PI Communication Channel would overwrite the Certificate Information and it is advisable to check the Certificates and Configurations after System / OS Upgrades.

2) Changes in Network / Firewall would also result in the same error and Customers need to check and validate whether Certificates are imported, necessary configurations are in place and Ports are opened from SAP PI to connect to Ariba Network.