

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 <u>https://www.globalsign.com/en/ssl-information-center/what-is-anssl-certificate/</u> 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





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 DER-encoded binary file o Double click "SSL System Client SSL Client" o
 Download the new certificate and convert to to transaction code (tcode) STRUST o Click the Import Certificates button





- Choose the certificate you exported from step 1 > click Check icon > click Allow on security question 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 • 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.

	Key	Storage Certifi	icate Revocation Chec	k					
Co	Content Security								
Key	Key Storage Views								
	Add View	Remove View	Import Entries From	File Expo	rt Entries To File Export View to PSE	C B - B			
ē	Status	Name	<u>ـ</u>	Туре	Description				
7	•			•					

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

New Key Storag	e View	
View Name: * Description: PSE Image:	ITK_Certificates Stores Server and Client Certificates Create Cancel	
		11





Importing Server and Client Certificates into a View Procedure

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

Det	etails of view 'ITK_Certificates''									
	View E	intries	View	Properties						
	Create De	elete	Rename	Copy Entry	Import Er	ntry Export	Entry Ger	nerate CSR Request Impo	rt CSR Response	B1 F
Ē	Status	Name			۵	Entry Type	Algorithm	Valid From	Valid To	
8	•					•	-			
	i There	are no e	ntries to disp	blay						
										747

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

Entry Import	
Select entry type: * X.509	Certificate
Enter path to certificate file:	C:\Users\pvenkatachalam\Desktop\ClientCert\qa Browse
	11

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.





Entry Import		[
Select entry type: * PKCS#8	Key Pair	•			
Enter path to PKCS#8 key file:	C:\Users\pvenkatachalam\Desktop\ClientCert\ke Browse				
Add PKCS#8 certificate(s):	C:\Users\pvenkatachal	am/Desktop/ClientCert/ce Browse			
Subject DN	Issuer DN	Source File			
		Import Reset Cancel			

9. Click Add.

Entry Import	
Select entry type: * PKCS#8 Key Pair	
Enter path to PKCS#8 key file:	Browse
Add PKCS#8 certificate(s):	Browse Add
Subject DN	Issuer DN
CN=*.ariba.com,OU=Engineering,O=Ariba, Inc.,C=US	CN=Ariba Engineering Test CA (not for production use),OU=Engineering,O=Ariba, Inc.,C=US

10. Click Import.

Results

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





Details of view "ITK_Certificates"									
1	View Entries View Properties								
Create Delete Rename Copy Entry Import Entry Export Entry Generate CSR Request Import CSR Response								818	
6	Status	Name	۵	Entry Type	Algorithm	Valid From	Valid To		
F	-			-	-				
		cert		CERTIFICATE	RSA	Mon Jul 15 03:23:46 PDT 2	Thu Jul 13 03:23:46 F	DT 2	
		key		PRIVATE KEY	RSA	Mon Jul 15 03:23:46 PDT 2	Thu Jul 13 03:23:46 F	PDT 2	
		qabuyer		CERTIFICATE	RSA	Wed Sep 22 11:02:11 PDT	Sat Sep 19 11:02:11	PDT 2	
					1			-	
De	tails of e	ntry "cert"							
CERTIFICATE entry: Creation date : Mon Aug 12 03:03:47 PDT 2013 (12 Aug 2013 10:03:47 GMT) Version : ver.3 X.509 Algorithm : RSA Key Size : 1024 bits Subject name : CN=*.ariba.com,OU=Engineering,O=Ariba, Inc.,C=US Issuer name : CN=4riba Engineering Test CA (not for production Use),OU=Engineering,O=Ariba, Inc.,C=US Serial number : 7512 Signature Algorithm : shalWithRSAEncryption (1.2.840.113549.1.1.5) Validity: not before : Mon Jul 15 03:23:46 PDT 2013 (15 Jul 2013 10:23:46 GMT) not after : Thu Jul 13 03:23:46 PDT 2023 (13 Jul 2023 10:23:46 GMT)									

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.



SAP Ariba /

Key Storage Certificate Revocation Check				ficate Revocation Check		
c	on	tent Sec	urity			
K	ey :	Storage V	liews			
	A	dd View	Remove View	Import Entries From File	Export E	Entries To File Export View to PSE
		Status	🖗 Name	à	Туре	Description
5	▼ 5		-	-		
			ITK_Certificates		USER	t a

3. Click the Permissions per Domain tab.

Content Security								
Domains per Permission Permissions per Domain								
Domain Name								
8								
ariba.com/ariba_JobBean								
ariba.com/com.ariba.asc.sap.netweaver.xiadapter.ra								
ariba.com/test_ariba_JobBean								
com.adobe/AdobeDocumentServices								
com.adobe/DocumentServicesLicenseManager								
heavy:sap.com/tc~bcf~lib~ear								
redwood.com/scheduler-ear								
sap.com/bi~alv								
sap.com/bi~alv~common								
sap.com/bi~alv~pdf								
Cranted and a based permissions for domain Variba com/ariba JabPaanV								
Show Grouped by Views								

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



SAP Ariba 🎊

Granting New Keystore Permission							
Keystore Action:	CREATE_VIEW	All Actions					
Reyslore view.		OK Cancel					
		//					

- 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 <u>here</u> 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.

Copyright/Trademark

