FAQ - CIG Certificate Change – October 26, 2020

Introduction

Recently, SAP Ariba has unified the certificate infrastructure load balancer (testacig.ariba.com and acig.ariba.com) and tenant certificates (e0397-iflmap.hcisbp.eu1.hana.ondemand.com and l0397 iflmap.hcisbp.eu1.hana.ondemand.com) to single certificates for simplifying the certificate infrastructure. However, due to recent security standards and scalability concerns, we need to separate the certs again.

This FAQ is intended to provide additional configuration and change suggestions regarding that change.

When will the change occur?
October 26, 2020 12:00pm – 3:00pm PST/ 9:00 PM -12:00 AM CET

What is changing?
SAP Ariba Cloud Integration Gateway is separating the tenant and the load balancer certificate for the test and production environments respectively due to security standards.

Load Balancer certificates (these are used for Customer to Cloud Integration Gateway connectivity) – testacig.ariba.com and acig.ariba.com and these are not changing.

Client Certificates (used for Mutual authentication) / Sign-Verify/Encrypt-Decrypt new URLs are being implemented

- **TEST: testacig.ariba.com** will be replaced with **aribacloudintegration-test.ariba.com**
- **PRODUCTION: acig.ariba.com** will be replaced with **aribacloudintegration.ariba.com**

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-an- ssl-certificate/ for more details.

What is a Certificate Authority?
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.

What is Certificate Pinning?

SAP Ariba

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.

AS2 connections between Cloud Integration Gateway (CIG) and Suppliers

Which customers are impacted?

- Suppliers who use CIG as their integration mechanism and transact using AS2 EDI formats
- Suppliers currently using certificates with Common Name (CN) **testacig.ariba.com and acig.ariba.com** for SSL authentication and message encryption/verification in their test and production environments, respectively

What customers should do:

Customers **must replace** the certificates with Common Name (CN) testacig.ariba.com and acig.ariba.com with the new certificates attached with Common Name (CN) **aribacloudintegration-test.ariba.com** and **aribacloudintegration.ariba.com** respectively in their B2B middleware configuration.

ERP customers

Which customers are impacted?

Buyers for whom all the following apply:

- **Testacig.ariba.com and acig.ariba.com** are currently in use in their PI/CPI/middleware landscape for client certificate-based authentication.
- Where CIG is the client and customer’s middleware is the server
- CIG presents its certificate at runtime and customer’s middleware validates the CIG certificate to decipher the message
- For SAP ECC customers, please ensure that support for Server Name Indication (SNI) is enabled, please refer to this document for configuration steps: SAP Note # 2124480 - ICM / Web Dispatcher: TLS Extension Server Name Indication (SNI) as client (https://launchpad.support.sap.com/#/notes/2124480)

What customer should do:

Customers who have implemented **testacig.ariba.com and acig.ariba.com** certificates for client certificate-based authentication must update their PI/CPI KeyStore configuration to reflect the new attached certificates with Common Name (CN) **aribacloudintegration-test.ariba.com** and **aribacloudintegration.ariba.com** in their test and production environments, respectively

SAP Ariba

Customers who DO NOT use independent endpoints for CIG authentication

Which customers are impacted?

Buyers who have manually copied the CIG **testacig.ariba.com and acig.ariba.com** certificates into Ariba on demand realms- IntegrationManager->Integration Tool Kit Security->Certificate

What customer should do:

Manually copy the new certificates with Common Name (CN) **aribacloudintegration-test.ariba.com** and **aribacloudintegration.ariba.com** into the test and production realms into the Integration Tool Kit Security-> Certificate section

Why am I not able to connect to CIG and still get an error?

Ensure that your systems that connect to CIG are configured to accept SNI (Server Name Indication) TLS (Transport Layer Security) extension.

Server Name Indication (SNI) is a TLS extension, defined in RFC 6066. It enables TLS connections to virtual servers, in which multiple servers for different network names are hosted at a single underlying network address https://www.ietf.org/rfc/rfc6066.txt In most systems, this parameter comes enabled by default however you will need to ensure it is enabled.

Without this, customers will not be able to connect to CIG and will result in errors SSL handshake, CERTIFICATE ERROR SSSLRC_CONN_CLOSED, SI_ECONN_BROKEN, ICM_HTTP_SSL_ERROR, incomplete SSL handshake, SSLHostnameVerifier: could not match hostname

If you are integrating your Non-SAP system with CIG:

You will need to ensure that corresponding parameter in your systems (e.g. JVM parameter jsse.enableSNIExtension) is configured to accept SNI (Server Name Indication) TLS (Transport Layer Security) extension

You will need to ensure the above in both Production & Non-Production systems prior to **October 26, 2020** to align with TLS 1.2 Cipher Suites Hardening

If you are integrating your SAP ECC or S/4HANA with CIG:

Please refer to SAP Note # 2124480 - ICM / Web Dispatcher: TLS Extension Server Name Indication (SNI) as client (https://launchpad.support.sap.com/#/notes/2124480)

As detailed in SAP Note,

1. Ensure that ERP profile parameter icm/HTTPS/client_sni_enabled is "true". Make sure it is **not set to "false"** in the profile

   You will need to ensure the above in both Production & Non-Production ERP systems **prior to October 19th 2020** to align with TLS 1.2 Cipher Suites Hardening

2. In addition, you must also ensure that parameter icm/HTTPS/client_sni_blacklist does not contain **testacig.ariba.com and acig.ariba.com.** In other words, these two Ariba host names **should not be blacklisted.**

   You will need to remove blacklist **only after** CIG Certificate changes are deployed on **October 19th 2020 3:00 PM PST** in both Production & Non-Production ERP systems

In order to verify a successful SSL handshake, ERP customers can do a connectivity test by following the steps described in below note

2970307 - How to confirm and test if the SNI (Server Name Indication) extension is active in my ERP? (https://launchpad.support.sap.com/#/notes/2970307)

If you are integrating using SAP PI/PO with CIG:

Please refer to SAP Note # 2492386 - SSLException: Peer sent alert: Alert Fatal: unrecognized name (https://launchpad.support.sap.com/#/notes/0002492386)

You will need to ensure the above in both Production & Non-Production systems **prior to October 26 2020** to align with TLS 1.2 Cipher Suites Hardening

In order to verify a successful SSL handshake, SAP PI customers can do XPI inspector test by following the steps described in below.

1. Launch XPI inspector

2. Provide SSL Server URL Address **https://cig-qa-test-proxy.ariba.com/**
3. Maintain SSL Protocol version the value **Auto (default option)**
4. Maintain SSL Cipher Suite the value **Auto (default option)**
5. Maintain Trusted CA Keystore view the value **Trusted CAs (default option)**
6. Select use proxy and provide proxy host and port if applicable
7. Select start
8. Select stop when we can see below Warning message

Warning: *No traces will be written in the default trace files during inspection.*
You can switch this off by using menu "Options"Reproduce the failing scenario right now and click "Stop" as soon as the problem arise

9. In the results page an entry with message “handshake completed” should exist

Please refer to additional FAQ on TLS 1.1 deprecation and TLS 1.2 cipher suites hardening for SAP Ariba Cloud Integration Gateway (https://support.ariba.com/item/view/190213)