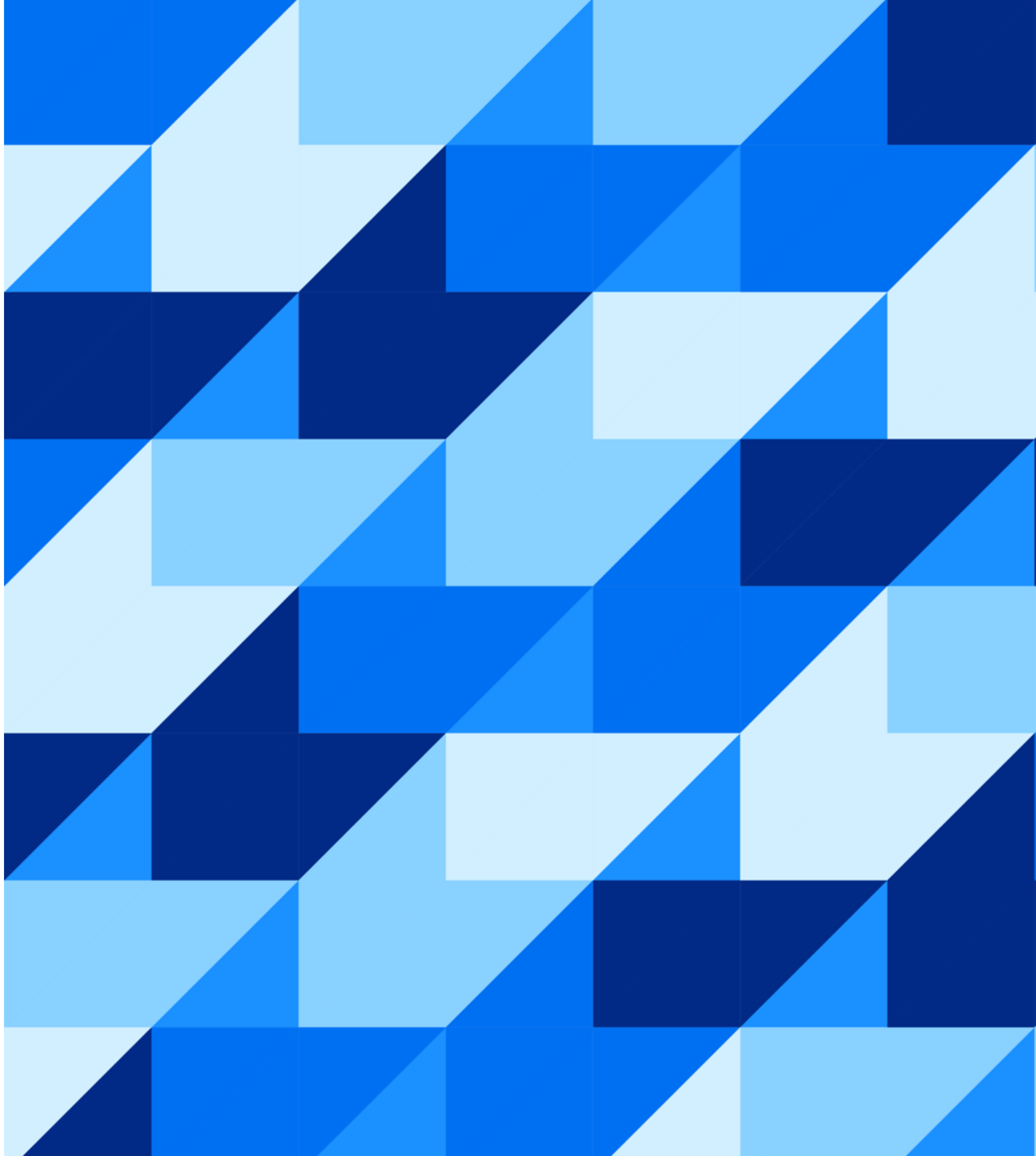
SAP Ariba Website Certificate Renewal

Ankita Gupta
Fernanda Boldrin
Prem Biradar

February 20, 2025

Public



Agenda

Introduction to Certificates

Why Does SAP Ariba Renew Certificates?

How and Where to Download Certificates

How to Identify Old vs. New Certificates

Impact of Missing Certificate Updates

Resources

Q&A

Public

Digital certificates

Definition: A digital certificate is a message format, signed by a Certificate Authority. A digital certificate contains information that can allow verification of the user of that certificate.

Purpose: Digital certificates and SSL are widely accepted for security authorization and authentication of two parties without knowing pre-existing information about the other party, acting as a Public Key Encryption system.

Common Formats:

- X.509
  - The most common format for a digital certificate
  - ITU standard X.509
  - Usually described as 'server certificates'
  - Generally, are split into two files:
    - a public key which is signed by the CA
    - a private key file, which is in RSA format

How is a certificate obtained?

A certificate is obtained through a Certificate Authority (CA).

- SAP Ariba uses DigiCert Inc as CA

All the certificates obtained share three common characteristics:

- All are listed under its Common Name (CN)
- All include a .cert and .key file
- All have a symbolic link to a file, which is the Base64 encoded representation

How do a client application and SAP Ariba server work?

1. A client application connects to the SSL port on SAP Ariba servers.
2. The client application and server attempt to start an SSL session.
3. Then, both agree on a protocol version and select cryptographic algorithms.
4. Finally, they authenticate each other.

Why SAP Ariba renews or updates the certificates

Security & Compliance – Certificates ensure encrypted communication and secure connections. Regular updates help maintain compliance with security standards (e.g., **TLS protocols**).

Prevent Service Disruptions – Expired or outdated certificates can cause connection failures, preventing users from accessing SAP Ariba services. Renewal ensures uninterrupted service.

Trust & Authentication – Certificates validate the identity of SAP Ariba's servers and services, ensuring that users interact with legitimate systems. Updating them maintains trust.

Industry Best Practices – Certificate authorities (**CAs**) and security protocols evolve. Regular updates align SAP Ariba with the latest security measures and industry standards.

Regulatory Requirements – Certain industries or regions mandate periodic certificate updates to comply with cybersecurity laws and regulations.

By renewing and updating certificates proactively, SAP Ariba ensures security, reliability, and seamless operations for its customers.

Understanding certificate authorities & encryption algorithms

Certificate Authority (CA)

Definition: A trusted organization that issues digital certificates to secure online communication.

Purpose

- Establish trust in internet transactions
- Authenticate web servers and encrypt data

Hierarchy

- **Leaf Certificates**: Issued by intermediate CAs
- **Intermediate Certificates**: Signed by root CAs for global trust

Encryption & hashing algorithms

Hashing Algorithms

- **SHA1**: An older, less secure algorithm
- **SHA2 (including SHA256)**: The latest, used by SAP Ariba for stronger security

Encryption Algorithms

RSA (Rivest-Shamir-Adleman):

- Based on factoring large numbers
- Requires longer key lengths for security

ECC (Elliptic Curve Cryptography):

- A newer, more efficient algorithm
- Provides equal security as RSA with shorter key lengths

Understanding the "Issued by" field in certificates

SHA256 and SHA384

- Represent the type of **Secure Hash Algorithm (SHA)** used
- Numbers (256, 384) indicate the hash output length in bits

Key Details

- If "Issued by" states **RSA** or **SHA256**:
    - The certificate uses **RSA encryption** and the **SHA-256** hash function.
- If "Issued by" states **ECC** or **SHA384**:
    - The certificate uses **ECC encryption** and the **SHA-384** hash function.

Takeaway

- The "Issued by" field helps identify the encryption and hashing methods securing the certificate.

Who will receive the notification?

Buyer side

The registered Designated Support Contact (DSC) will receive the notifications.

Supplier Side

The SAP Business Network Account Administrator will receive the notifications.

Timeline for notification

First Notification

It will be sent 60 days in advance, serving as an initial heads up about the upcoming certificate updates. This gives customers ample time to plan and prepare for the changes.

Second Notification

This will be sent 30 days in advance, informing customers that the new certificates are available for download. Customers should download the new certificates.

Third Notification

This will be sent 5 days in advance, serving as a reminder for those who may have delayed or forgotten to update their certificates before the scheduled update date.

Action to take

Buyer (Customer and Designated Support Contact)

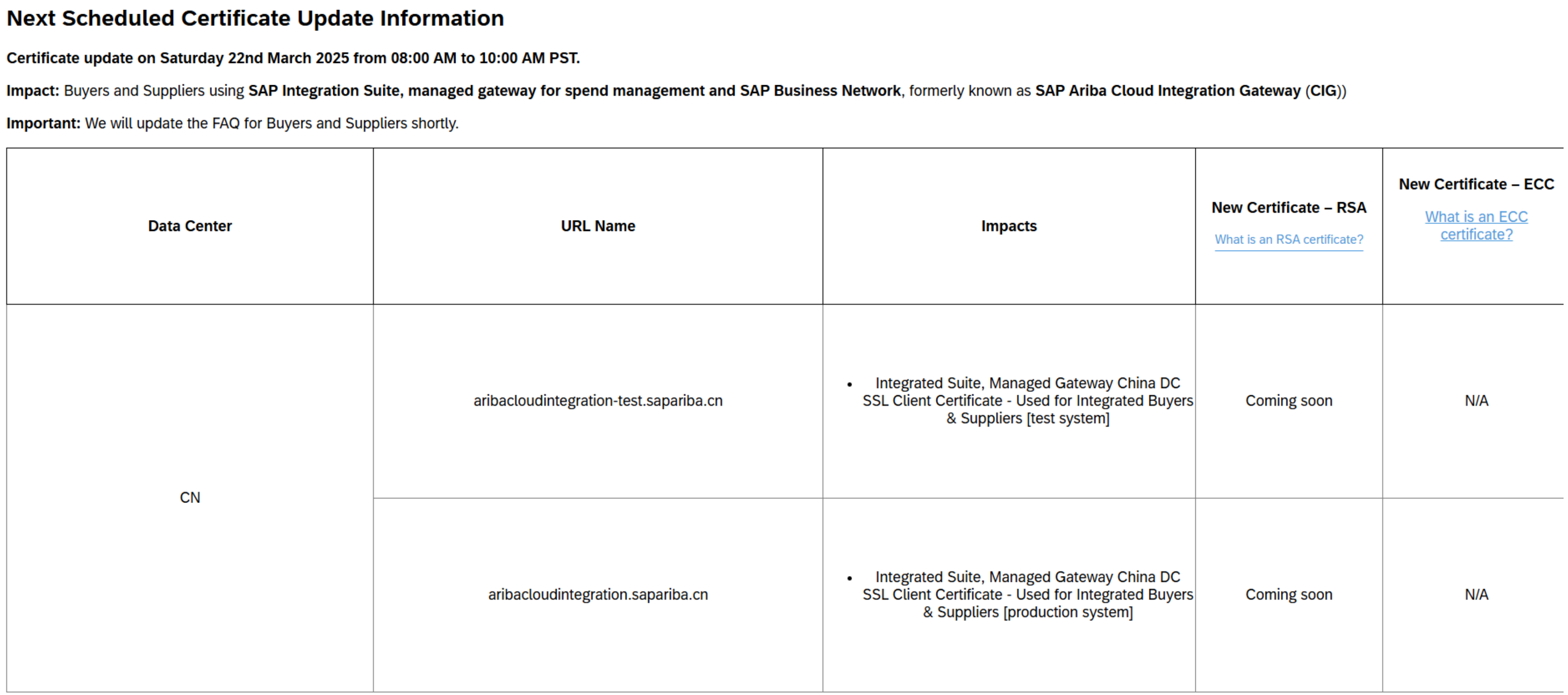
Ensure you are subscribed to the Maintenance subscription option

Supplier Customer

Ensure you have a Network Service Subscription

Where to download the certificates

To download the certificate, please use the link from the notification and navigate to the certificate repository for the old certificates. For new certificates, it should be under **Next Scheduled Certificate Update Information**



Next Scheduled Certificate Update Information

Certificate update on Saturday 22nd March 2025 from 08:00 AM to 10:00 AM PST.

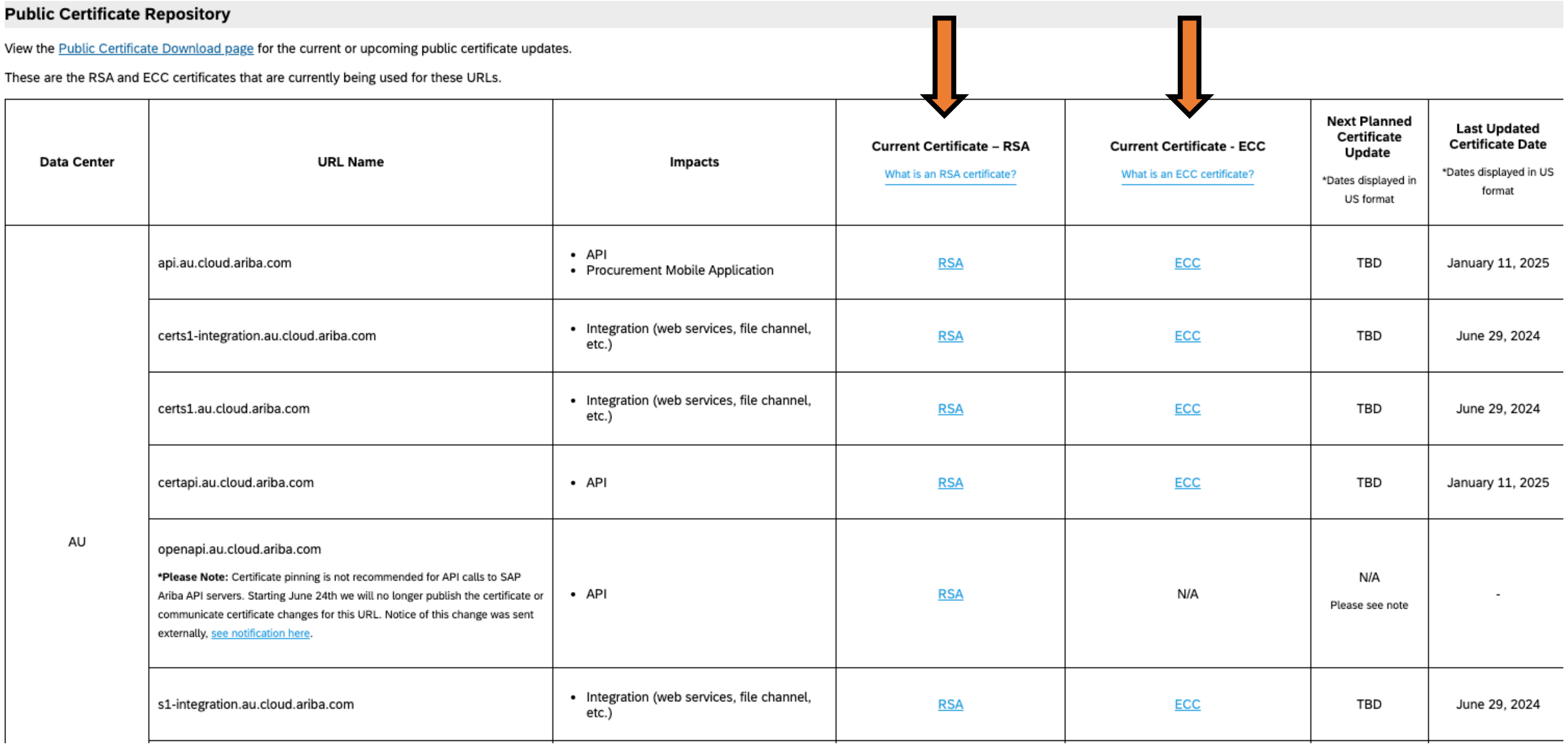
Impact: Buyers and Suppliers using **SAP Integration Suite, managed gateway for spend management and SAP Business Network**, formerly known as **SAP Ariba Cloud Integration Gateway (CIG)**)

Important: We will update the FAQ for Buyers and Suppliers shortly.

Data Center	URL Name	Impacts	New Certificate – RSA What is an RSA certificate?	New Certificate – ECC What is an ECC certificate?
CN	aribacloudintegration-test.sapariba.cn	• Integrated Suite, Managed Gateway China DC SSL Client Certificate - Used for Integrated Buyers & Suppliers [test system]	Coming soon	N/A
	aribacloudintegration.sapariba.cn	• Integrated Suite, Managed Gateway China DC SSL Client Certificate - Used for Integrated Buyers & Suppliers [production system]	Coming soon	N/A

Finding and downloading SAP Ariba certificates (Old)

- **Old certificates** are available for download in RSA and ECC formats on the **Public Certificate Repository** page. This repository contains all active certificates currently used by SAP Ariba.



Public Certificate Repository

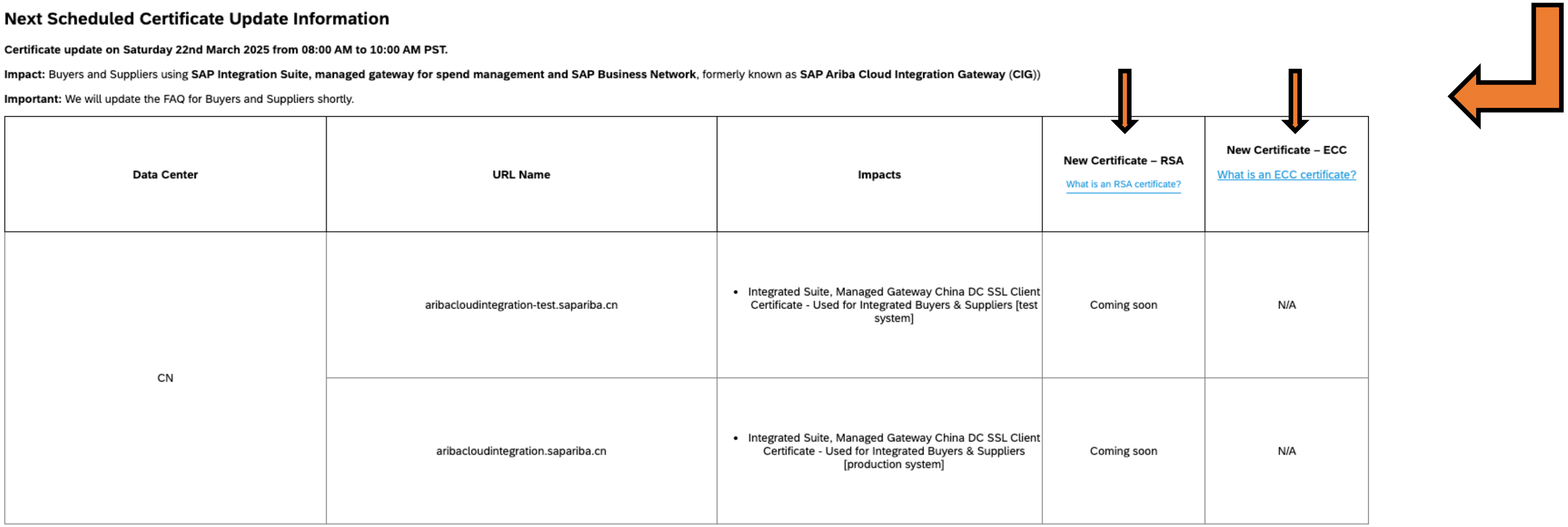
View the Public Certificate Download page for the current or upcoming public certificate updates.

These are the RSA and ECC certificates that are currently being used for these URLs.

Data Center	URL Name	Impacts	Current Certificate – RSA What is an RSA certificate?	Current Certificate - ECC What is an ECC certificate?	Next Planned Certificate Update *Dates displayed in US format	Last Updated Certificate Date *Dates displayed in US format
AU	api.au.cloud.ariba.com	• API • Procurement Mobile Application	RSA	ECC	TBD	January 11, 2025
	certs1-integration.au.cloud.ariba.com	• Integration (web services, file channel, etc.)	RSA	ECC	TBD	June 29, 2024
	certs1.au.cloud.ariba.com	• Integration (web services, file channel, etc.)	RSA	ECC	TBD	June 29, 2024
	certapi.au.cloud.ariba.com	• API	RSA	ECC	TBD	January 11, 2025
	openapi.au.cloud.ariba.com ***Please Note:** Certificate pinning is not recommended for API calls to SAP Ariba API servers. Starting June 24th we will no longer publish the certificate or communicate certificate changes for this URL. Notice of this change was sent externally, see notification here.	• API	RSA	N/A	N/A Please see note	-
	s1-integration.au.cloud.ariba.com	• Integration (web services, file channel, etc.)	RSA	ECC	TBD	June 29, 2024

Finding and downloading SAP Ariba certificates (New)

- Upcoming SAP Ariba certificate updates are announced on the **Public Certificate Download** page. **New certificates** are available for download 30 days prior to the scheduled update.



Next Scheduled Certificate Update Information

Certificate update on Saturday 22nd March 2025 from 08:00 AM to 10:00 AM PST.

Impact: Buyers and Suppliers using **SAP Integration Suite, managed gateway for spend management and SAP Business Network**, formerly known as **SAP Ariba Cloud Integration Gateway** (CIG))

Important: We will update the FAQ for Buyers and Suppliers shortly.

Data Center	URL Name	Impacts	New Certificate – RSA What is an RSA certificate?	New Certificate – ECC What is an ECC certificate?
CN	aribacloudintegration-test.sapariba.cn	• Integrated Suite, Managed Gateway China DC SSL Client Certificate - Used for Integrated Buyers & Suppliers [test system]	Coming soon	N/A
	aribacloudintegration.sapariba.cn	• Integrated Suite, Managed Gateway China DC SSL Client Certificate - Used for Integrated Buyers & Suppliers [production system]	Coming soon	N/A

- After a certificate update, the updated certificates are moved from the **Public Certificate Download** page to the **Public Certificate Repository**. The next planned update is then added to the **Download** page.

How do you determine if you are impacted by this change?

Sixty (60) days prior to a certificate update, SAP Ariba sends a notification listing the impacted URLs. Since not all customers use every SAP Ariba service, not all are impacted by every update. Check your integrations, APIs, and SSO configurations with your IT department to see if any of the listed URLs are relevant to your setup. If none of the URLs are used in your configurations, you are not affected by the update.

How do I determine if my integration scenarios are impacted by this change?

The following should be checked to determine if your integrations are impacted by a certificate update.

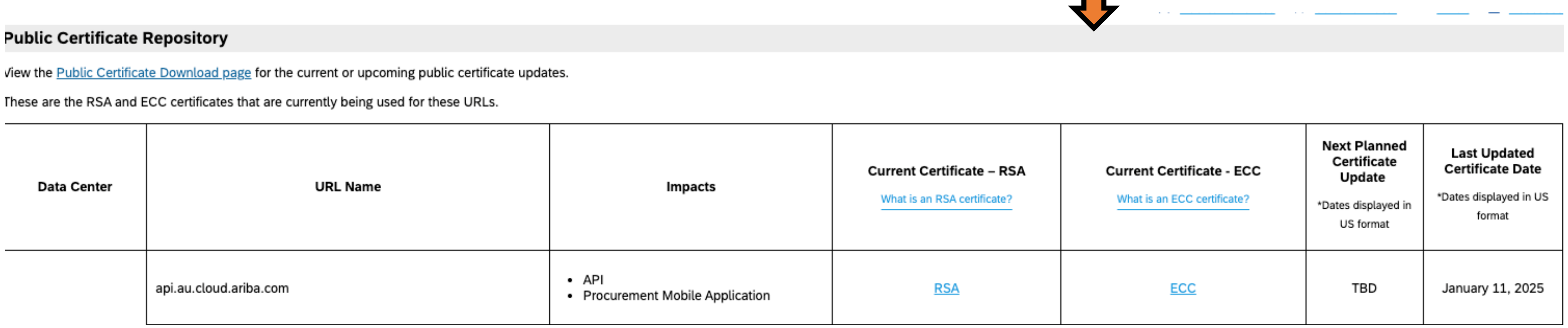
1. Check to see if URLs specified in the notification are used in any integration configurations (webservices, integration toolkit, etc.).

2. Check your configurations in the following areas.
    1. **Inbound Webservices** - Customers who have enabled an inbound web service are impacted regardless of their authentication mode (shared secret or certificate).
    2. **Outbound Webservices** - Customers who have enabled “**Sign with Ariba Private Key**” in the web services security of their SAP Ariba outbound end point are impacted.
    3. **Integration Toolkit** - All customers who are using ITK are impacted regardless of their authentication mode (shared secret or certificate). Please note: If you do not use SSL handshake in ITK then you do not need to update the certificate if you are using shared secret authentication. SAP Ariba does not have logs of a customer's use of SSL handshake, so this will need to be determined by your internal IT team.
    4. **ERP Integration to S4** via mediated connectivity (not through the SAP Business Network) are impacted.

Certificate Repository and Schedule

The **Public Certificate Repository** can be accessed in the following link.

https://support.ariba.com/item/view/192337



Public Certificate Repository

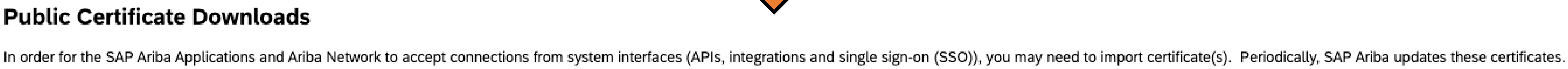
View the Public Certificate Download page for the current or upcoming public certificate updates.

These are the RSA and ECC certificates that are currently being used for these URLs.

Data Center	URL Name	Impacts	Current Certificate – RSA What is an RSA certificate?	Current Certificate - ECC What is an ECC certificate?	Next Planned Certificate Update *Dates displayed in US format	Last Updated Certificate Date *Dates displayed in US format
	api.au.cloud.ariba.com	• API • Procurement Mobile Application	RSA	ECC	TBD	January 11, 2025

Information about next scheduled certificate update can be accessed in the following link.

https://support.ariba.com/item/view/178876



Public Certificate Downloads

In order for the SAP Ariba Applications and Ariba Network to accept connections from system interfaces (APIs, integrations and single sign-on (SSO)), you may need to import certificate(s). Periodically, SAP Ariba updates these certificates.

Resources

The knowledge base for DigiCert CA updates can be found at:

https://knowledge.digicert.com/general-information/digicert-root-and-intermediate-ca-certificate-updates-2023

Additionally, you can contact DigiCert via the following link:

https://www.digicert.com/contact-us?utm_medium=organic&utm_source=support-ariba&referrer=https://support.ariba.com/

Thank you.

Contact information:

Ankita Gupta
ankita.gupta05@sap.com

Fernanda Boldrin
fernanda.boldrin@sap.com

Prem Biradar
prem.biradar@sap.com

Bring out your best.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. See Legal Notice on www.sap.com/legal-notice for use terms, disclaimers, disclosures, or restrictions related to this material.