02 07 2026

TIS Certificate Updates

ERP & Integrations

Introduction

Dear TIS Customer,

We are planning to update the **Certificate Authority (CA)** for the **(m)TLS API Endpoints** in both Europe and the United States. This change is required due to the upcoming expiration of the current certificates and industry-wide changes in terms of certificate lifecycle management. This change is necessary to ensure continued secure connectivity.

More information can be found on https://www.digicert.com/blog/tls-certificate-lifetimes-will-officially-reduce-to-47-days

--

Our endpoints will be changing according to the following timeline:

- **UAT environments (available from July 6th 12pm CEST, 2026)**
    - api-mtls.eu-test.tispayments.com
    - api-mtls.us-test.tispayments.com
- **Production environments (cutover on July 9th 12pm CEST, 2026)**
    - api-mtls.eu.tispayments.com
    - api-mtls.us.tispayments.com

All systems (SAP or non-SAP) that connect to TIS Payments mTLS APIs must update their trust stores by importing the new Amazon root certificates before July 9th, 2026, to avoid integration failures.

The new TIS certificates will be issued by Amazon Root CAs. For details check Repository | Amazon Trust Services.

Distinguished name	SHA-256 hash of subject public key information	Self-signed certificate	Test URLs
CN=Amazon Root CA 1,O=Amazon,C=US	fbe3018031f9586bcbf41727e417b7d1c45c2f47f93be372a17b96b50757d5a2	DER PEM	Valid Revoked Expired
CN=Amazon Root CA 2,O=Amazon,C=US	7f4296fc5b6a4e3b35d3c369623e364ab1af381d8fa7121533c9d6c633ea2461	DER PEM	Valid Revoked Expired
CN=Amazon Root CA 3,O=Amazon,C=US	36abc32656acfc645c61b71613c4bf21c787f5cabbee48348d58597803d7abc9	DER PEM	Valid Revoked Expired
CN=Amazon Root CA 4,O=Amazon,C=US	f7ecded5c66047d28ed6466b543c40e0743abe81d109254dcf845d4c2c7853c5	DER PEM	Valid Revoked Expired
CN=Starfield Services Root Certificate Authority - G2,O=Starfield Technologies, Inc.,C=US,S=Arizona,L=Scottsdale	2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92	DER PEM	Valid Revoked Expired
* CN=Amazon RSA 2048 Root EU M1,O=Amazon,C=DE	8d935558e6a3c896330148ffdf6a1ac0a5bfba1ab44545135a3b376c9a1a308d	DER PEM	Valid Revoked Expired
* CN=Amazon ECDSA 256 Root EU M1,O=Amazon,C=DE	9565907725464be0bff44b1232f85ee862a9a0d99db971ba20344aaf41431d58	DER PEM	Valid Revoked Expired
* CN=Amazon ECDSA 384 Root EU M1,O=Amazon,C=DE	798fe10957e8c5a0874201caf09d5ef4b2e2412c47bf991949566cb542d3af3f	DER PEM	Valid Revoked Expired

* Root certificate is pending inclusion in browser trust stores.

PLEASE NOTE: TIS and Amazon do not recommend and support certificate pinning. Intermediate certificates may change when renewing certificates. If you require pinning, then we recommend that you pin the public key of the root.

Scope & Action Required

What is changing?

- TIS exchanges ZeroSSL/Sectigo CA by Amazon Trust Services CAs
- New Amazon root certificates must be imported and trusted by your systems

What is NOT changing

- No API endpoint URLs will change
- The mTLS authentication method remains the same
- All client certificates (published by TIS Customer CA remain) unchanged
- User logins, single sign-on or SFTP connections to TIS platform are not impacted

Immediate Actions

1. Download the new Amazon root certificates from here **Repository | Amazon Trust Services**
2. Import new certificates into your integration system(s)
3. Validate that connectivity to UAT and/or Production endpoints is still working

Do not remove the old root certificates provided by TIS before July 13th

Change Instructions

SAP ByDesign

Requirement

Customers **must import the new Amazon root certificates** into SAP ByDesign's Certificate Trust List.

Why

- SAP ByD performs **outbound TLS validation** against TIS endpoints.
- It does **not rely on OS-level trust** → certificates must be explicitly trusted.

Step-by-Step Instructions

1. Log in to SAP ByDesign
2. Navigate to: "Edit Certificate Trust List"
3. Click "Upload"
4. Browse and select the certificate files
5. Select "Add"

(Note: possibly the certificates already exist. In this case, the exercise is completed.)

--

SAP S/4HANA On-Prem/Private Edition

Requirement

Customers must import the new root certificates. This is done in **SAP STRUST** under the SSL client PSE.

Why

1. SAP validates TIS endpoints during outbound HTTPS calls.
2. Java trust store inside SAP is **isolated** from OS trust.

Step-by-Step Instructions

- In STRUST, switch to Change view
- Select the existing PSE SSL-Identity dedicated to TIS (that's the PSE/bundle the add-on uses)
- Import the new Amazon root certificates into that specific Client PSE:
    - Use the menu Certificate → Import
    - Provide the file path of the CA chain file and choose Base64 as the file format
    - Verify the certificate content and click "Add to Certificate List"
- Click Save

--

SAP S/4HANA Cloud / Public Cloud

SAP Public Cloud already trusts the Amazon Certificate Authority (CA) by default. No action is required.

--

SAP ECC

Requirement

Customers must import the new root certificates. This is done in **SAP STRUST** under the SSL client PSE.

Why

3. SAP validates TIS endpoints during outbound HTTPS calls
4. Java trust store inside SAP is **isolated** from OS trust

Step-by-Step Instructions

- In STRUST, switch to Change vie
- Select the existing PSE SSL-Identity dedicated to TIS.
- Import the new Amazon root certificates into that specific Client PSE:
    - Use the menu Certificate → Import
    - Provide the file path of the CA chain file and choose Base64 as the file format
    - Verify the certificate content and click "Add to Certificate List"
- Click Save

Recommendation

Restart ICM via SMICM during your maintenance window(s) in case the ICM is not informed automatically.

--

TIS Agent

Step-by-Step Instructions

Update to the latest version **TIS Agent 4.2.3 (https://support.tispayments.com/downloads/files/tis-agent-423)**.

You can accomplish this by

- Turning on automatic updates for your current installation or,
- Performing a manual update of TIS Agent or
- Downloading it from TIS Customer Support Portal.

The latest TIS Agent already trusts the TIS Platform endpoints by default.

Restart your TIS Agent service for changes to take effect.

Note: The built-in update functionality only works for Agent version >4.x, otherwise you must update following this guidance: https://support.tispayments.com/downloads/files/tis-agent-update-2

--

Non-SAP / Custom Integrations (Also Impacted)

Even if not SAP, any system calling TIS APIs over mTLS is impacted, including:

- Middleware / Integration Platforms
    - SAP CPI (Cloud Integration)
    - MuleSoft
    - Boomi
- Other ESB/iPaaS platforms
- Custom Applications
- Java applications (using trust stores / key stores)
- .NET services
- Python / Node.js integrations
- Any backend service connecting via HTTPS with certificate validation

The system must be updated if it

✓ Connects to:

api-mtls.eu.tispayments.com

api-mtls.eu-test.tispayments.com

api-mtls.us.tispayments.com

api-mtls.us-test.tispayments.com

✓ Uses:

HTTPS with certificate validation

mTLS (mutual TLS authentication)

✓ Maintains:

A trust store / certificate store

What Must Be Updated

All impacted systems must:

- ☑ Import Amazon root certificates
- ☑ Ensure new certificates are trusted / active

Support

For support, contact support@tispayments.com, your Professional Services Consultant or Customer Success Manager with the subject: **"TIS Certificate Update – mTLS APIs"**

Please include:

- System type (SAP ByDesign / S/4HANA / ECC / other)
- Environment (UAT/Production)
- Error details and timestamp (if applicable)

--

Thank you for your cooperation in ensuring a smooth and secure transition.

Kind regards,
TIS Support Team