TLS Certificate Migration – FAQ

What is happening?

TIS is migrating to AWS-issued TLS certificates. This was previously announced, and TIS had intended to postpone it by renewing the existing certificate to provide additional transition time until September 2026.

Why is the timeline changing now?

Following discussions with TIS's certificate authorities, TIS learned that renewing the existing certificate would require a new root and intermediate certificate chain. Due to evolving global security standards, the certificate authorities involved can no longer issue certificates from the previous root and intermediate CAs, as modern operating systems, browsers, and security platforms may no longer trust these legacy certificate chains.

As a result, customers would need to update their trust configuration even if TIS remained with its current certificate authority. Because the same type of trust-store changes would also be required later for the planned migration to AWS certificates, proceeding with a temporary renewal would mean customers performing essentially the same change twice.

Why not just do the temporary renewal as originally planned?

Even with a renewal through the current certificate authority, customers would still need to update their trust configuration, because the root and intermediate certificates have changed. Delaying the migration would not eliminate the required customer action — it would only postpone it and likely require a second change later. To avoid unnecessary effort, operational risk, and repeated testing activities, TIS has therefore decided to move directly to the AWS certificate chain as originally planned.

What do customers need to do, and by when?

All customers must complete migration to the AWS certificate chain before July 10, 2026, when the current certificate expires. TIS will switch the certificate on July 9, 11:59am Central European Summer Time (CEST).

What are the recommended steps?

- Trust the AWS root certificates, rather than installing specific server or intermediate certificates.
- Avoid pinning individual server (leaf) or intermediate certificates whenever possible.
- Configure your systems to trust the appropriate root certificate authorities, enabling future certificate renewals without manual intervention.

What happens if the changes aren't made in time?

Integration with the TIS platform would cease to function, which would have a significant impact on customers' payment processes.

Who should this be forwarded to?

Customers are asked to forward this communication to their technical/IT department if they are unable to understand the technical details themselves.

Why is TIS making this change at all?

TLS certificates are a fundamental building block of secure communication on the public internet. Across the industry, increasingly stringent requirements for certificate authorities and service providers are driving shorter certificate lifetimes and more frequent certificate renewals.

As a service provider, TIS relies on certificate authorities for certificate issuance and lifecycle management and cannot influence industry-mandated renewal processes or trust-chain requirements. Modern security practices require client implementations to be flexible enough to accommodate regularly renewed certificates, by trusting the appropriate root certificate authorities rather than individual server certificates. TIS's migration to AWS-managed certificates is aligned with these industry best practices and provides a more secure, scalable, and operationally resilient approach to certificate lifecycle management.

Why do we have to import 5 certificates and not just one or two, similar to what was done before?
Amazon Web Services (AWS) does not guarantee that our future server certificates will be generated under Amazon Root CA 1, which makes it a necessity for our customers to install all 5 root CAs in total (highlighted in the list below). 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

How do we determine if we are successful with this change?

Please have your IT/technical team answer these questions:
"Did you install the Amazon CA certificates into all relevant systems?"
"Did your team upload all 5 certificate files into these systems?"
"Did you make sure that no certificate pinning is implemented and if pinning is required is it limited to the root CA?"

If the team can answer these questions with **YES**, then your connections to TIS should be fine.

What is Plan B for systems that cannot be switched over in time?

If systems cannot be switched to the new TLS server certificates on time, manually exporting and importing payment files and account statement files can serve as a temporary, short-term alternative. For security reasons, however, this should be used only to a very limited extent and as a last resort.

Who can customers contact for help?

If customers require support validating their configuration or have questions regarding the migration, they are asked to contact TIS as soon as possible. The TIS team is available to help ensure a smooth transition before the July 9th deadline.