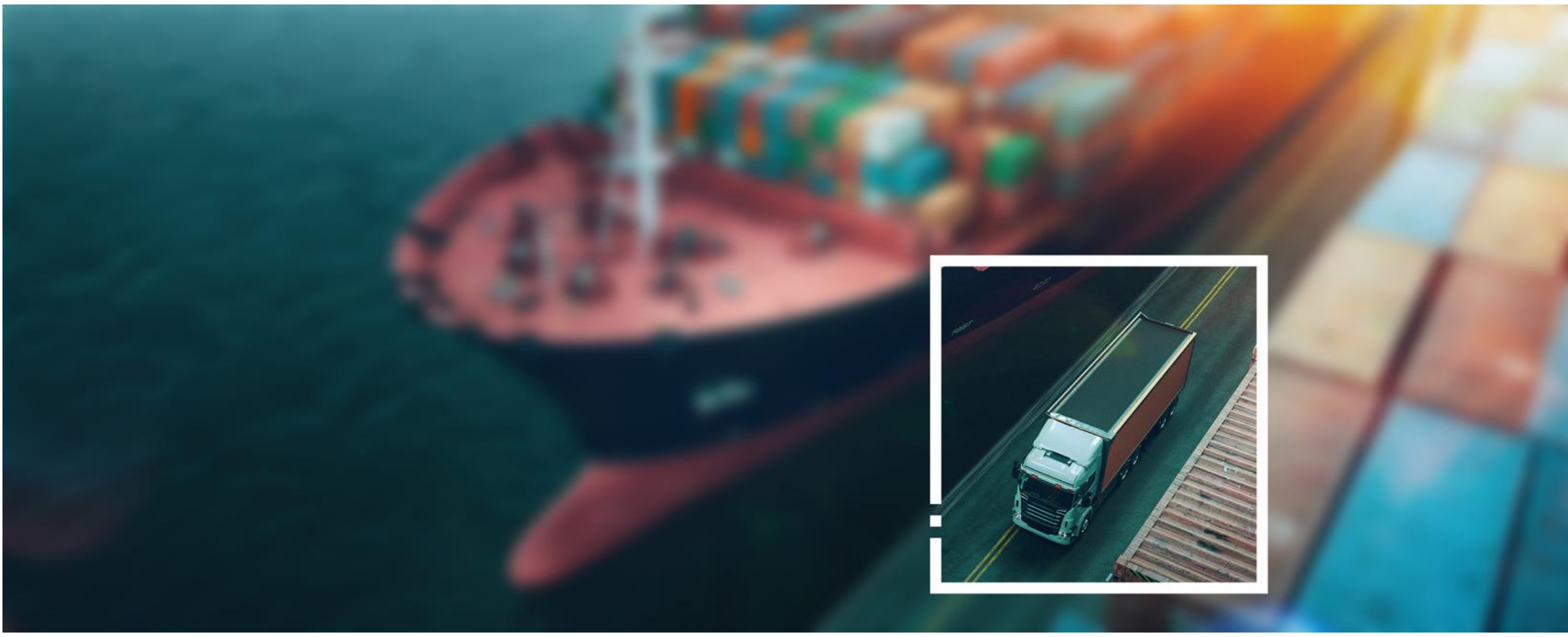

Certificate Update

Preliminary Incident Response – Feb 2024

Version 1.0, Feb 21st 2024
AUTHOR: Jens Ulrik Østergaard

CONFIDENTIALITY LEVEL:

Public

What happened

Between 07:00 and 11:57 CET on 15 February 2024, customers attempting to access the STEP SaaS platform may have experienced issues launching the STEP Workbench client or accessing the STEP application in general.

What we know so far

The problems are linked to the rollout, of an updated TLS certificate for the STEP SaaS platform, starting 07:00 CET on 15 February.

We have knowledge of two problems that can have impacted customers access to the STEP SaaS platform in a negative way.

A. The updated TLS certificate, signed by GlobalSign, is based on a newer root CA certificate (R6) that GlobalSign issued 2014. Where web-based applications to STEP will use the frequently updated truststore that comes with the web browser in use by the customer, the STEP Workbench will use a truststore on the local workstation that is maintained by the operating system – MacOS or Windows.

   The newer root CA certificate (R6) from GlobalSign is pushed with updates to the workstations operating system, and we see that workstations that are not receiving OS updates will have older root CA certificates and not the newer R6 from GlobalSign. As a result, the chain of trust between the client and the server cannot be established and the connection from STEP Workbench to the STEP environment fails.

B. What appears to be a race condition in STEP has led to a portion of the customers STEP environments to refuse connection and present the message of ‘Service Unavailable’ when the updated TLS certificate was rolled out. This problem is still being investigated.

How did we respond

At 08:37 CET, we started to receive notifications from customers facing problem A, and at 11:00 CET the decision was made to rollback the change to the original TLS certificate that is based on the older root CA certificate from GlobalSign.

At 11:57 CET, the rollback was completed, and all customer impact was fully mitigated.

Next Steps

Problem A:

We have worked with GlobalSign to get a crosssign certificate bundled together with the updated TLS certificate and its intermediate certificate. The crosssign certificate will help establish the full chain of trust - both to older root CA certificates and up to the newest. Tests have been executed to reproduce the problem internally on workstations without the newer R6 root CA certificate, and it has been validated to solve the problem of launching STEP Workbench when the crosssign certificate *is* included in the bundle.

Problem B:

> Investigation centers around what leads the system to refuse connection and prevent seamless update of the new TLS certificate in STEP.

Both problem A and problem B will need to be solved and carefully tested before a new rollout of the updated TLS certificate is planned.

A root cause analysis will follow when all information is present and include corrective actions.