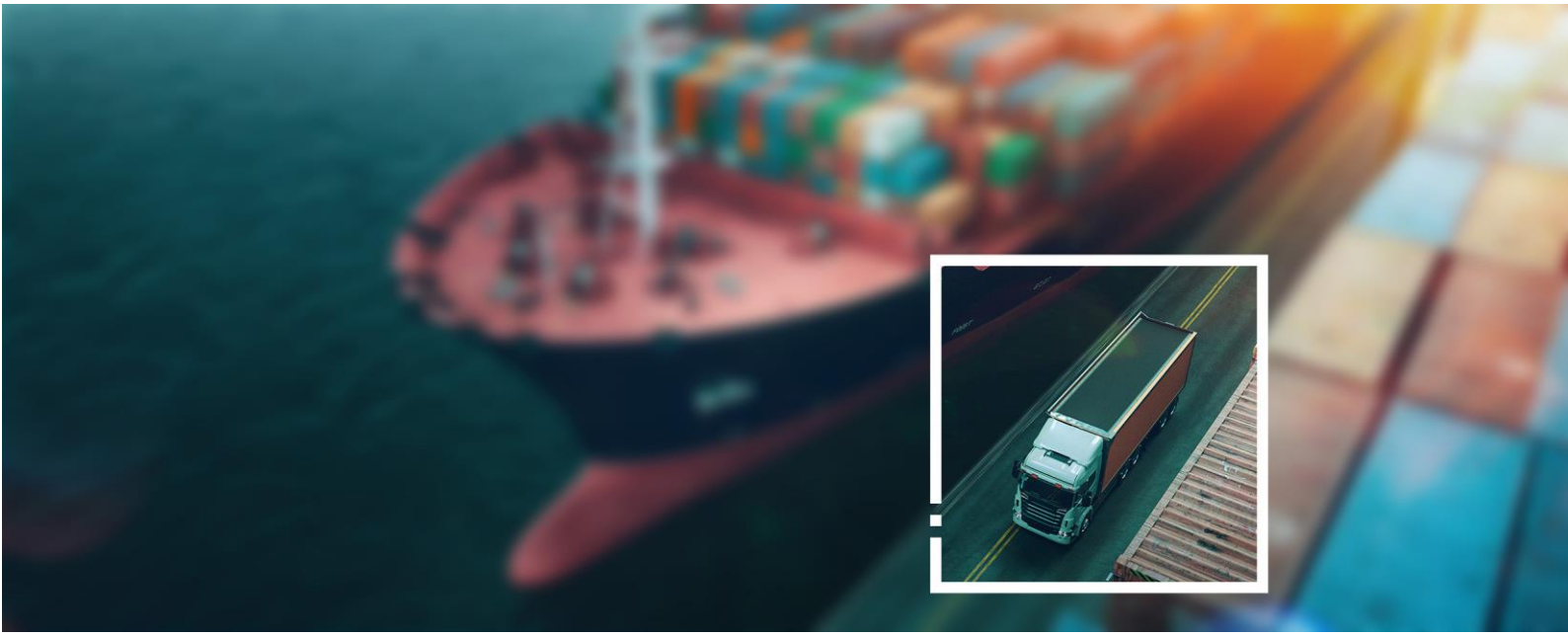
STIBO SYSTEMS
MASTER DATA MANAGEMENT



Certificate Update

Root Cause Analysis – Feb 2024

Version 1.0, Feb 29th 2024
AUTHOR: Jens Ulrik Østergaard

CONFIDENTIALITY LEVEL:

Public

Summary of impact

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.

Root Cause

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

Two problems 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. A function in the STEP code has the unwanted side effect of caching configuration for the TLS certificate. As a result, STEP systems were unable to locate a valid TLS certificate when the current certificate was updated with the new one which eventually led to the message ‘Service Unavailable’ being presented to the user.

Mitigation

At 08:37 CET, our monitoring systems identified services being unavailable, and the Stibo Systems operations team started to receive notifications from customers facing problems.

Investigation was conducted to determine the underlying cause, which took additional time, and at 11:00 CET the decision was made to roll back 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

A fix for problem A has been created in the form of an updated TLS certificate that includes a cross-sign certificate provided by GlobalSign for the purpose of closing the gap and make the updated TLS certificate valid from the oldest (R1) to the newest (R6) root CA certificate.

The updated TLS certificate has been tested and validated both on workstations having only the older R1 root CA certificate as well as workstations fully updated with the new R6 root CA certificate.

A fix for problem B has been created, tested and validated and will be included in any future patch versions and updates that a customer applies via the Selfservice UI.

A new TLS certificate rollout is planned to take place in the near future. More communication about this will follow.