CONFIDENTIAL COMPUTING CONSORTIUM
Governance Risk
& Compliance
Special Interest Group

Confidential Workload Upgrade Governance

August 2025

Context

Distributed applications, both in the cloud and IoT, are frequently deployed as a large number of nearly-identical instances. Furthermore, such applications are likely to be less tolerant of downtime. When such applications get updated, the update is usually rolled out gradually, and in some cases when a problem is found with the upgrade, a rollback may be required. During the upgrade, both old and new versions of the application are likely to coexist. For the successful continuous operation of the overall system, it needs to properly handle intermediate states where a subset of the application instances is upgraded, while the complementary subset of application instances is still awaiting upgrades.

Problem

Ensuring that the overall system — starting with Verifier and ending with Relying Parties — continues to operate without incurring undue downtime during the upgrade/rollback period requires careful orchestration.

Forces

Critical distributed applications often have high availability requirements. In addition, Control Specifications or Control Objectives may dictate that for certain classes of problems (e.g., high-impact vulnerabilities), all systems must be updated within a given time interval, sometimes an aggressive one.

Solution

The terms MUST/SHOULD/MAY etc. below are used in accordance with **[2]**. Every SHOULD recommendation is explained separately in the "SHOULD vs. MUST Clarifications" section towards the end of this document.

Integrate the upgrade with the software deployment stack (e.g., the CI/CD pipeline).

Once a new Confidential Workload* version becomes available, the Verifier policies** SHOULD **[a]** allow both old and new versions of the Workload to be treated as valid. If the rollout of the new Workload version is successful, the old Workload version is then removed from the Verifier policies. Conversely, if the rollout experiences difficulties, a rollback is initiated and the new Workload version is removed from the Verifier policies leaving only the old Workload version as valid. This is illustrated in the diagram below.

Workload Update Solution Diagram Missing [404 Error on Site]

* By "Confidential Workload", or "Workload" for short, this document means the combination of code and configuration loaded, measured and attested by a TEE instance.

** *Verifier policies* as used in this document is a shorthand for Endorsements, Reference Values and Appraisal Policy for Evidence in RATS **[1]** parlance.

Governance Expectations Summary

The numbers in the left column below refer to **[3]**. Rows listed as N/A indicate that corresponding expectations are listed under different Patterns documents.

#	DESCRIPTION
1–6, 8–15	N/A
7	Update Verifier policies with new expected Reference Values before deployment begins. Roll back this update if the Workload deployment fails for any reason. Remove Verifier policies related to older versions(s) of the Workload measurements after the deployment of updated Workload is successful.

“SHOULD” vs. “MUST” Clarifications

a. Failure to handle intermediate states where only a subset of Workload instances are upgraded could result in downtime or intermittent failures related to the upgrade, i.e., where only upgraded Workloads can successfully attest and existing Workloads will fail verification against the upgraded policies.

References

1. Remote Attestation Procedures (RATS) Architecture RFC:
   https://datatracker.ietf.org/doc/rfc9334/

2. Key Words for Use in RFCs to Indicate Requirement Levels:
   https://datatracker.ietf.org/doc/rfc2119/

3. Expectations of Ecosystem Participants
   ./Expectations of Ecosystem Participants

4. Confidential Computing Glossary:
   https://github.com/confidential-computing/glossary/