

Inspection and Approval Requirements

for

Federation Architecture for Composed Infrastructure Services (FACIS) Zero Trust Demonstrator

FACIS.ZTD

Purpose

The inspection and approval process follows a twofold approach: verification during the software development process and validation through software testing.

Verification is an ongoing, community-driven quality assurance process that focuses on architectural and code design and ensures that the software is built according to the specified requirements. The verification process includes reviews, walkthroughs, and inspections. Validation is a dynamic process that tests and confirms whether the resulting product meets the specified requirements. The validation process includes unit testing, integration testing, system testing, and user acceptance testing

In summary, verification and testing shall follow behavior-driven design principles for the core functionality. For the visualization component of the FACIS Zero Trust Demonstrator, established UX testing principles shall be applied, and the user interface shall be approved by the client.

Project Plan

The contractor must submit a project plan for approval within the first week after project's start. The project plan must include:

- Plan as GANTT Chart with at least 4 milestones:
 - Plan approval
 - Submission of BDD documentation (no later than one month after project plan approval)
 - Code ready for QA
 - Final validation
- Project team
- DevOps management and tools
- Related open-source packages to be included as runtime components (pre-checked according to license requirements)
- A final list of acceptance criteria and BDD test cases, derived from the related SRS document and the implementation strategy
- Wireframe designs or similar for the UX layout and Demonstrator's flow

Inspection and Approval Gates

After submission, the plan will be reviewed within one week with the client's team for approval.

The following gates must be reflected in the project plan:

- Presentation of visualization concept
- Infrastructure setup with Opa Gatekeeper, ORCE, Istio and other related environment components
- Deployment for all other components
- Development milestones for deployment
- UX-orchestration by ORCE
- Demonstration of product's functionality.

Validation & Acceptance

Validation will be performed against the acceptance criteria defined in the SRS document of the FACIS Zero Trust Demonstrator. The client will carry out the final assessment and approve the software based on these acceptance criteria.

The contractor shall inform the client at least two weeks before the software is expected to be ready for QA planning. Upon notification, the client shall coordinate the approval procedure. The behavior-riven development scenarios used for validation are defined in the SRS feature definitions and their associated acceptance criteria.

Assumptions & Dependencies

Main assumptions are the following:

- the OCM W-Stack and PCM Cloud and all their components are provided by the client
- IONOS Cloud and T-Systems OSC environments are provided by the client
- Harbor Docker repository is provided.

A final report referencing:

- the SRS document
- the Technical Development Requirements document
- the approved project plan
- the agreed acceptance criteria
- the evidence bundle per gate (hashes, reports, PDFs, logs, JSON outputs, trace matrix, BDD run logs)

will be prepared jointly by the client and the contractor.