Mojaloop
Platform Quality & Security

PI-26 product council update, 25th February 2025

Sam Kummary MLF

Mojaloop PQS: Fixing quality issues

1. Hardening of Mojaloop releases
    - Licensing issues
    - Codeowners
    - Dependabot alerts
    - Protected primary branches
    - License headers in source files
    - Clear obsolete PRs
    - Clear obsolete issues on repos
2. Merged into mojaloop main branches and tested as dev release - Mojaloop v17 RC

PQS Workstream Mojaloop slack channel: https://mojaloop.slack.com/archives/C06UW0E2KBN

Mojaloop PQS: Open SSF badge

1. OpenSSF checklist
    - Created individual issues for various aspects
    - Completed a single pass filling out the forms
    - Review needed by community members outside of the team to provide an objective view
    - Starting with passing level
    - Addressing gaps, fixing broken links, documentation updates

PQS Workstream Mojaloop slack channel: https://mojaloop.slack.com/archives/C06UW0E2KBN

Mojaloop PQS: artefacts provenance

Provenance for helm charts

1. Helm charts commands tested and verified
2. Options to include in scripts / CI tested
3. To be tested on a dev release along with the v17 RC testing
4. Helm charts can be signed during publishing
5. Signed charts can be verified during install or pre-install steps
6. Available for both standard releases and dev releases

PQS Workstream Mojaloop slack channel: https://mojaloop.slack.com/archives/C06UW0E2KBN

Mojaloop PQS: SBOM updates

1. SBOM for components and Mojaloop platform
2. Led to identification of issues
3. Lots of packages updated, fixed
4. Included in CI tools (CI orb)

PQS Workstream Mojaloop slack channel: https://mojaloop.slack.com/archives/C06UW0E2KBN

Mojaloop PQS: Image scanning

1. Anchor-cli anchor-engine used so far
2. Grype
3. Trivy
4. Testing in progress
5. To be included in CI tools (CI orb) replacing anchor-engine

PQS Workstream Mojaloop slack channel: https://mojaloop.slack.com/archives/C06UW0E2KBN

Mojaloop PQS: PI-26 status

1. SBOM for components and Mojaloop platform
2. Hardening of Mojaloop releases - continuation
3. Auditing in Mojaloop - Requirements, design discussions in PI26
4. Address deprecated libraries / packages in core services
5. Improve tooling used in CI/CD
    1. CI tools
    2. License checkers
    3. SBOM inclusion for all repositories
6. Blog posts and guidance to implementers and improve documentation - in progress
7. Update license files in repos - completion
8. OpenSSF checklist and compliance - PI 26
9. Stress / Load testing of Mojaloop - PI 26
10. Candidate: Provenance of Mojaloop artifacts
11. Review and followup SonarCloud

PQS Workstream Mojaloop slack channel: https://mojaloop.slack.com/archives/C06UW0E2KBN

PI26: Workstream Update - Objectives & details

Workstream Name:	Mojaloop platform quality & security (PQS)
Roadmap Pillar:	Quality Product (Foundation)
Lead:	Sam Kummary
Workstream Objectives:	The focus for PI-26 will be on 1) Hardening Mojaloop releases and contents (ensure quality & security, for Mojaloop v17) 2) Include SBOM scripts for all release quality repos 3) Auditing in Mojaloop - review and address gaps (requirements & design) 4) Bonus: Another objective this PI is to look into achieving OpenSSF badge for Mojaloop and blog posts.
Slack channel:	*#ws-pqs-pi26*, link: https://mojaloop.slack.com/archives/C06UW0E2KBN
Acceptance criteria:	
Meeting schedule:	Weekly - Wednesdays 12:30pm UTC; Team check-ins 2-3 times weekly and slack updates
Support Needed:	1. Contributions welcome.

Mojaloop PQS: Objectives

1. Hardening of Mojaloop releases
2. Security testing of Mojaloop
   - Assess feedback from testing done by security experts, internally
   - Prioritize issues based on criticality and severity ✅
   - Update backlog with stories to address issues ✅
3. Review core and related repositories released with Mojaloop for
   - Ensure dependabot alerts are addressed
   - Ensure Snyk issues are addressed ✅
4. Review any tasks “to-do” in the codebase and related quality issues
5. Review PRs in critical repositories and address (close, approve / reject)
6. Update nodejs version for any services not yet upgraded ✅
7. Update maintenance tooling (license-scanner and such) ✅
8. GitHub maintenance of Mojaloop repositories (used in the platform) (continuation)
9. Hardening Mojaloop core and addressing any known and reported quality, security issues
10. SBOM of dependencies in Mojaloop to better manage situations ✅
11. Provenance of Mojaloop artefacts - PI26 candidate