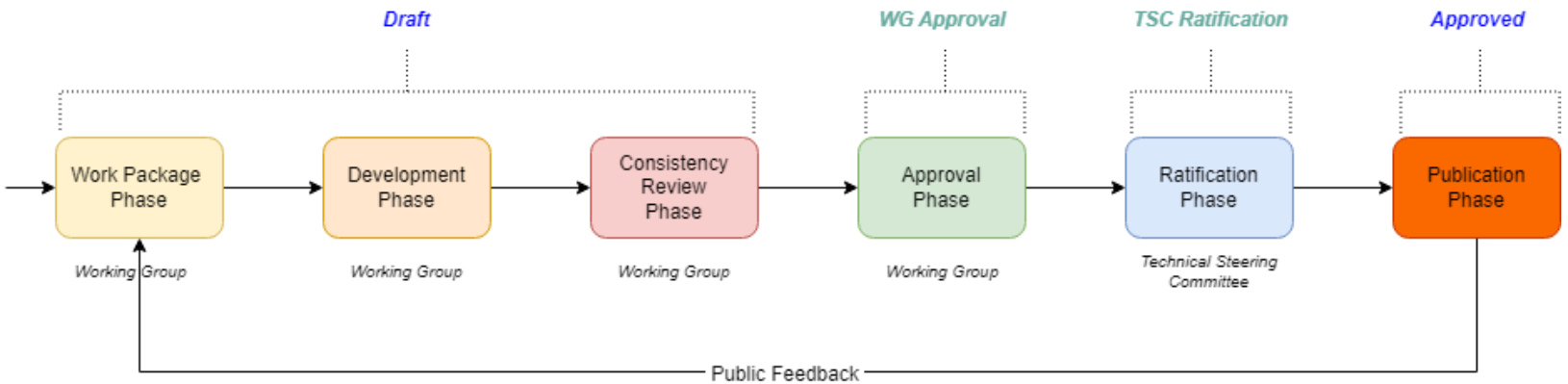
UXLF Security as a Work Package (WP)

Presented by: Roman Zhukov, Intel

open-source WG call, February 27th, 2024



Security WP: Rationale

As a responsible open-source maintainer UXLF would like to ensure that for all its repos:

- Security is properly coordinated focusing on “developer-first approach”
- Security best practices and tools are adopted and executed for project releases
- Vulnerabilities are handled properly, including transparent disclosures

Following greatest practices for open-source
OpenSSF, k8s, **envoy, django**, llvm, glibc, OpenSSL, curl etc.

Don’t our open-source projects do the good job already?
Yes, 100%. But following inhouse corporate policies and tools.

Security WP: Scope (Epics)

UXLF Security Team (cross-project)

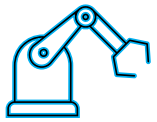
- Members & nomination criteria (*1-2 persons per project*)
- Security work coordination and step-by-step implementations
- Onboarding/assessment of the new projects joining

Vulnerability Response

- Public Policy and acceptance criteria (see oneDNN Security.md example)
- Reporting channels & mailing lists
- Coordinated review and fixing process
- Disclosure process

Secure Development (SDL)

- OpenSSF Best Practices (e.g., Scorecards)
- [advanced] Security coding practices and standards



DevSecOps - open and free scan tools are in the pipelines

- SAST (e.g., CodeQL, Scan.Coverity)
- SCA-CVEs (e.g., Dependabot, Trivy)
- Secrets (e.g., trufflehog, gitleaks)
- [advanced] (e.g., oss-fuzz, signing, SLSA)

Nearest ARs

- Nominate 1-2 persons from each project to join Security Slack channel and Security Mailing list. Should be committed for and engaged to actual work like tools evaluation and implementation, etc.
  - Sent this over to Roman Zhukov via DM in Slack or by email: roman.zhukov@intel.com
- Start looking into Public Policy and adopt it (see oneDNN Security.md example)
- Start looking into OpenSSF Security Best Practices (understand your score, example https://securityscorecards.dev/viewer/?uri=github.com/oneapi-src/oneDNN). 7 is a good target for now.
- Start looking at Scan.Coverity (more suitable for C/C++) and at CodeQL (more suitable for all other langs like Python, Go, Java, etc.)
- Make sure Dependabot is enabled