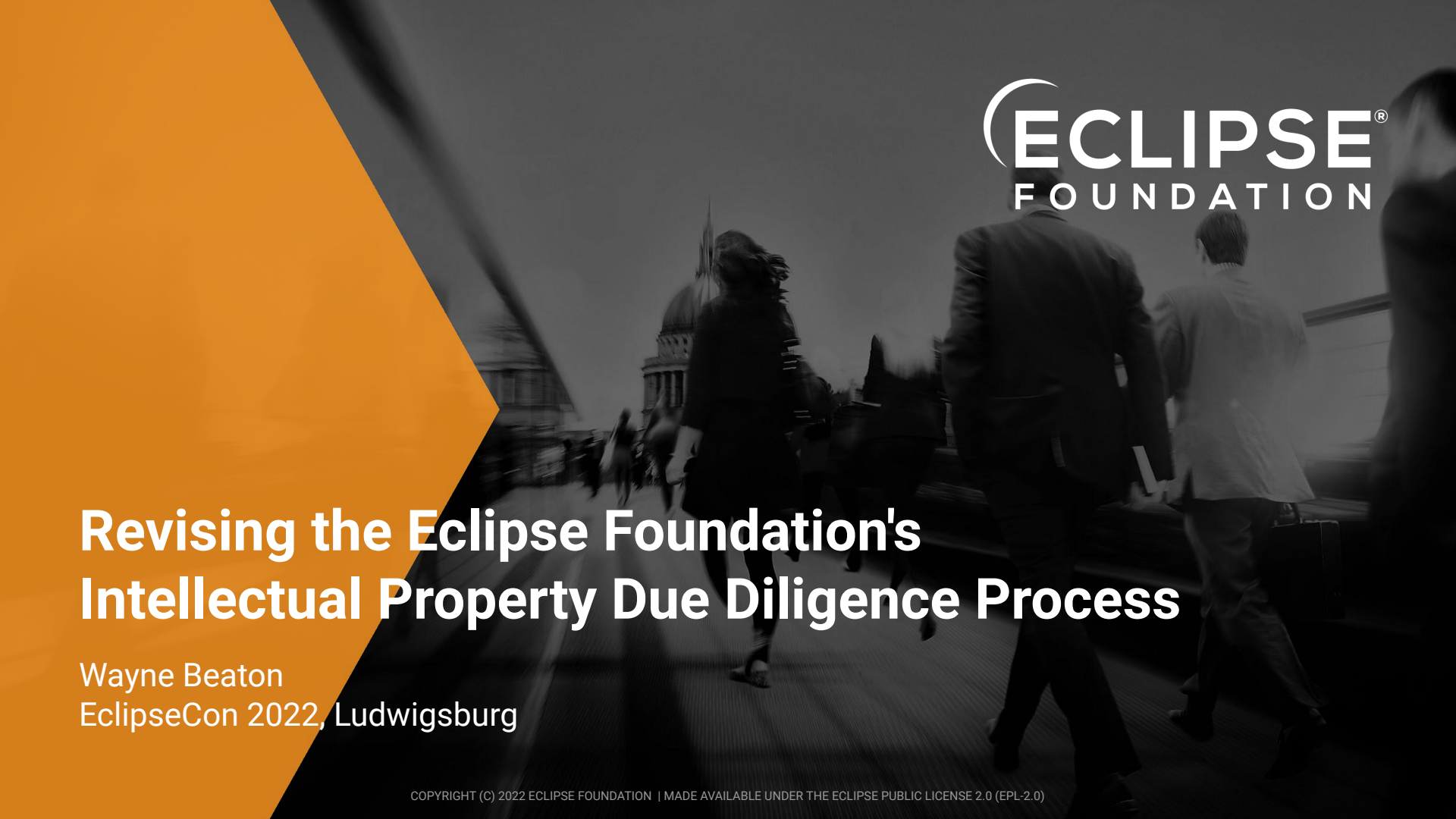


Revising the Eclipse Foundation's Intellectual Property Due Diligence Process

Wayne Beaton
EclipseCon 2022, Ludwigsburg

Trademark Disclaimer

Eclipse and Eclipse Foundation Logos are registered trademarks of Eclipse Foundation.

Background

History

- Copyright provenance was the initial deep focus of our IP processes
- Our existing tools and infrastructure are ancient and must be replaced
- Eclipse Foundation was conceived as a single-license foundation

Industry Expectations Have Changed

Industry best practices are now focused on:

- License compliance
  - And security, but that is a different topic
  - License compatibility is a key part of this
- Software bill of materials (SBOM) to ensure downstream consumers understand what they are getting
- Automation - OSS is now happening at an enormous scale, and relying on manual processes is no longer tenable

IP Policy Update

Changes…

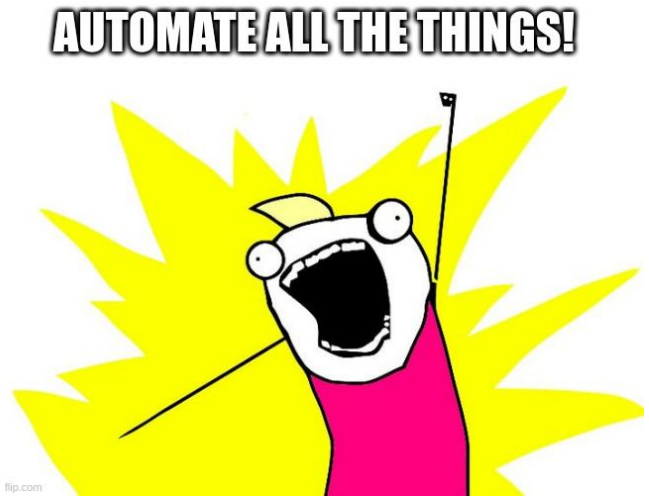
- The EPL is no longer special in the IP Policy or elsewhere
  - But we still love and highly recommend the EPL-2.0
- Focus our energies on license compliance
- License approval processes managed by the EMO without requirement for Board approvals
  - Focus on project-level license compatibility
- We can no longer assume that Eclipse Foundation projects can just use other EF projects without license compatibility checks

… Changes

- Eliminate manual record keeping requirements
- Revoke the existing policy on third party dependencies
- Deprecate IPzilla and CQs (contribution questionnaires)
- Eliminate the requirement for IP Logs
  - Rely entirely on SBOMs and git logs
- Implement build-time license compliance tools such as ORT
  - Automate license compliance checking of all third party dependencies
  - Automate creation of machine-readable SBOMs

Benefits

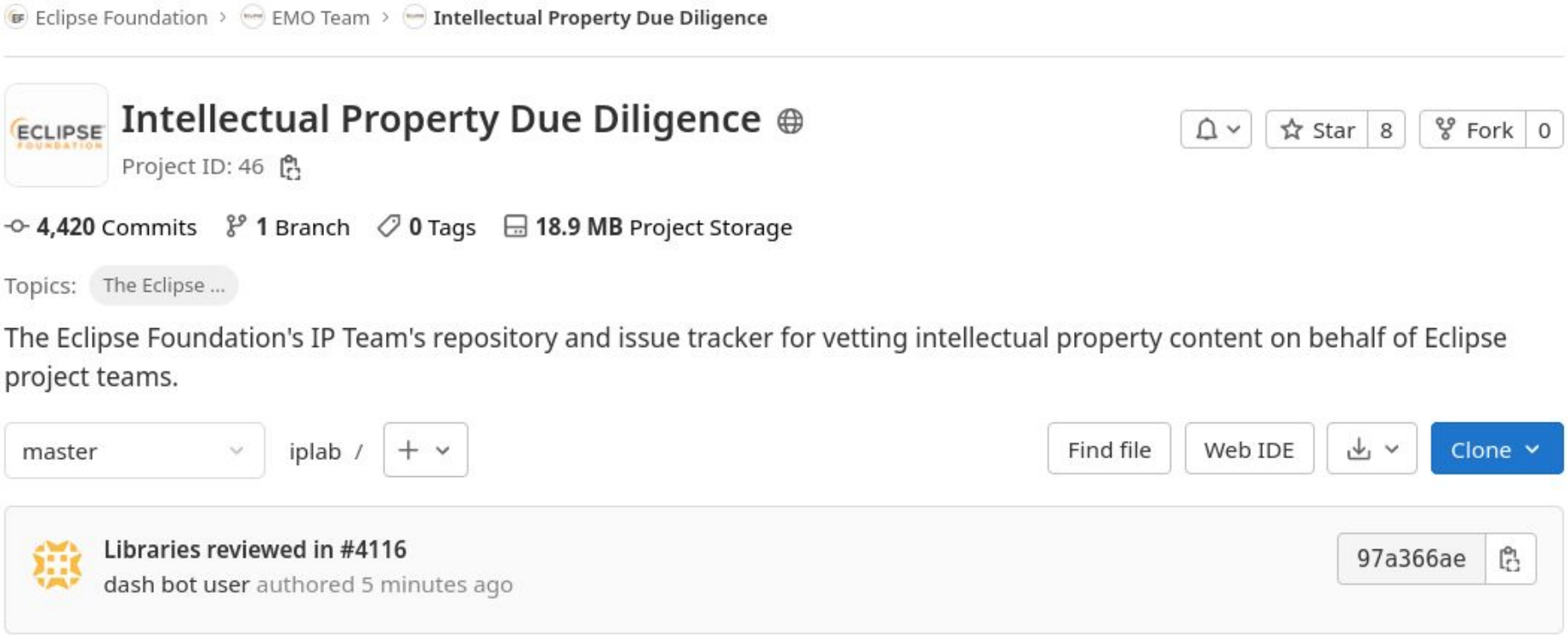
- Brings EF processes in line with current industry best practices
- Improves our ability to scale
- Reduces the IP due diligence burden on our projects, committers, and staff
- Deprecates old infrastructure
- New mantra: automate all the things (as much as possible)



So What Does This Mean?

Practical Impact

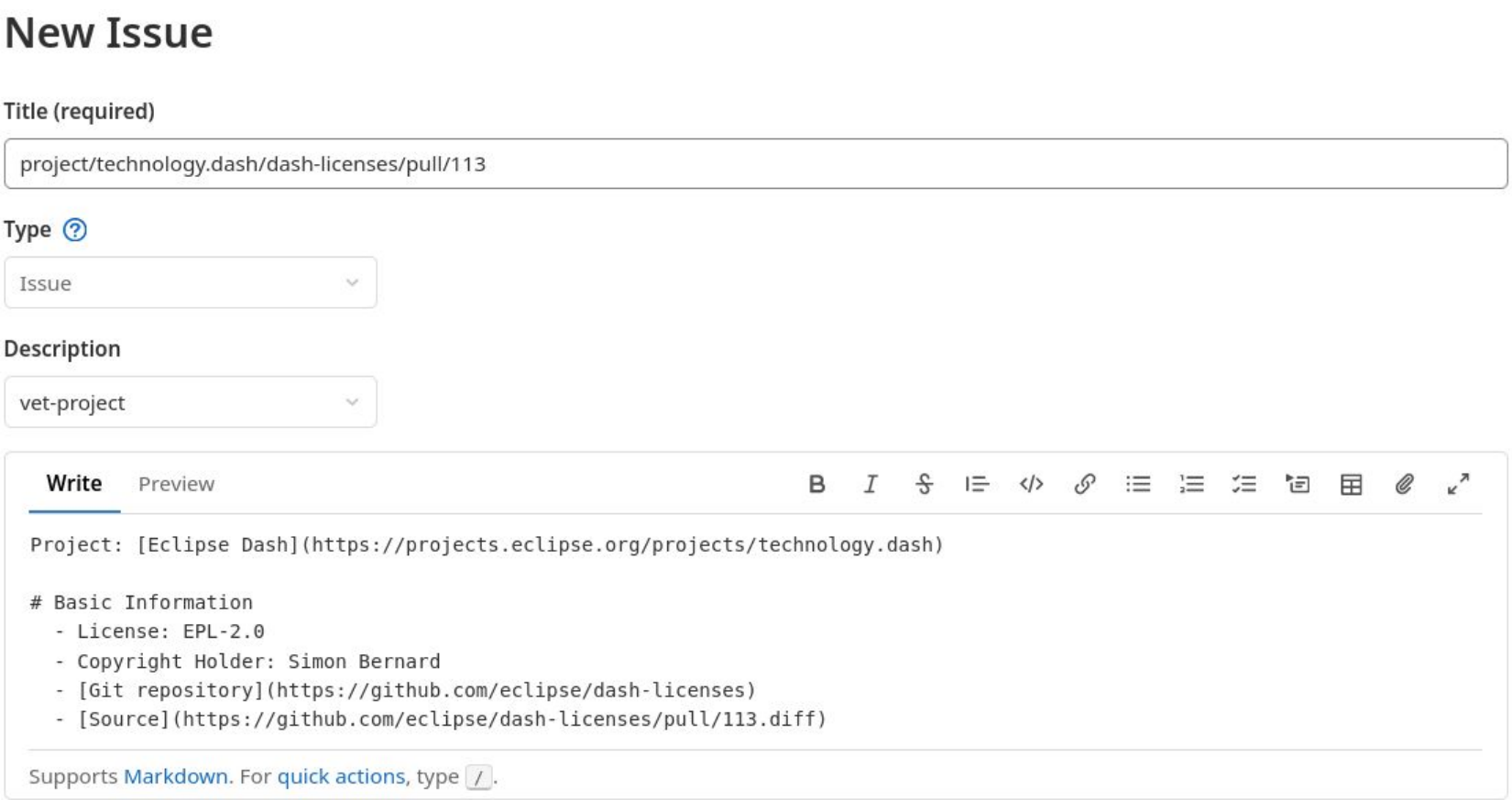
IPZilla is Deprecated; Long Live IPLab!



Initial Contributions/Repository Move

Before	Now
• Create CQ • Cursory IP Check • “checkin” • Move repository • Full IP review • Approval	• Move repository • Full IP review • Approval
Release	

Project Code Contributions



Bye-bye IP Logs

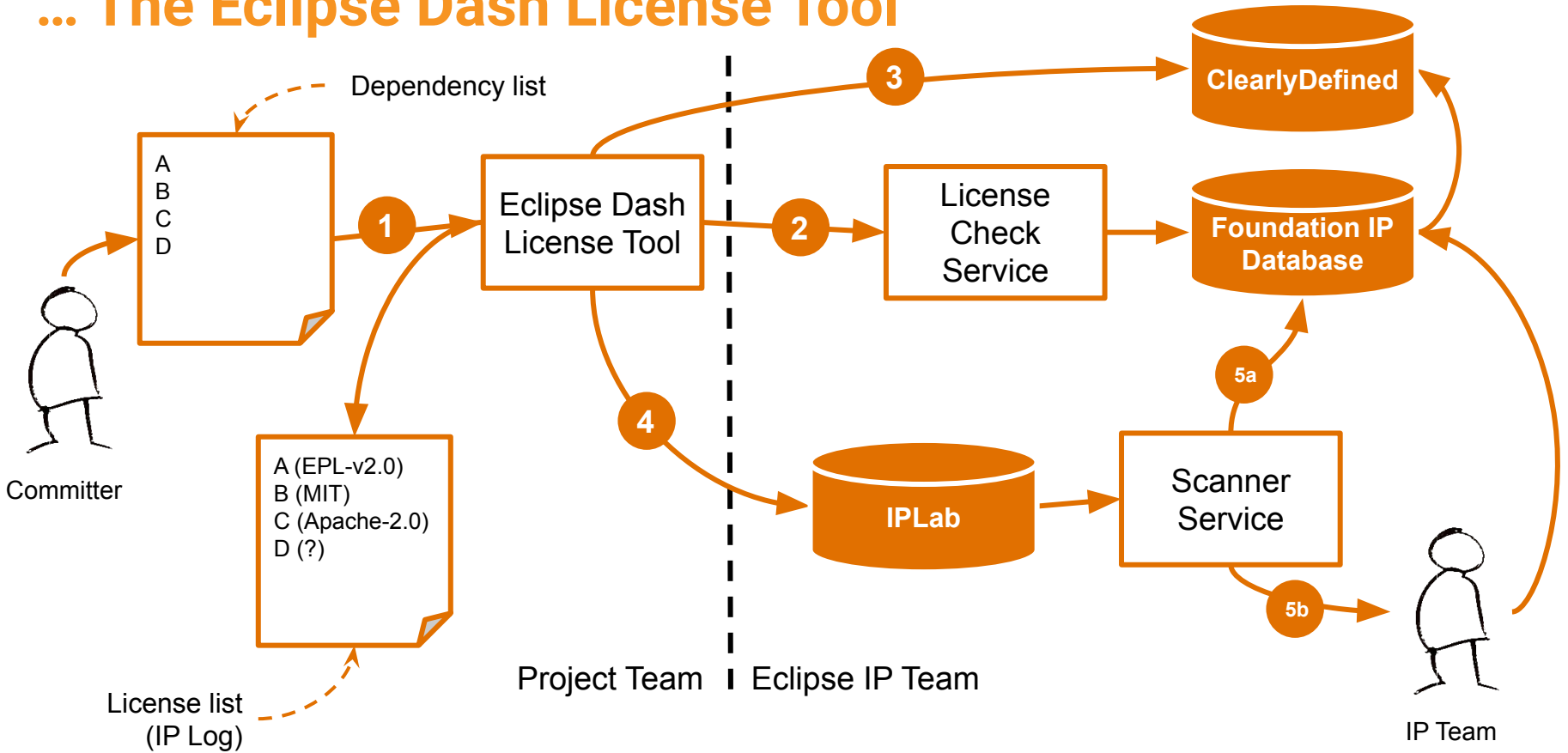
- IP Logs replaced by…
  - Git commit record (git log)
  - NOTICE file in repository root
  - SBOMs
- IP Log review
  - We (try to) build your code

The Eclipse Dash License Tool…

```
$ mvn org.eclipse.dash:license-tool-plugin:license-check \
-DexcludeGroupIds=org.eclipse \
-Ddash.summary=THIRDPARTY
...
[INFO] --- license-tool-plugin:0.0.1:license-check (default-cli) @ leshan ---
[INFO] Querying Eclipse Foundation for license data for 20 items.
[INFO] Found 14 items.
[INFO] Querying ClearlyDefined for license data for 6 items.
[INFO] Found 6 items.
[INFO] Vetted license information was found for all content.
[INFO] No further investigation is required.
[INFO] Summary file was written to: /home/gitroot/temp/leshan/THIRDPARTY
...
$ _
```

https://github.com/eclipse/dash-licenses

… The Eclipse Dash License Tool



OSS Review Toolkit (ORT)

- Analyzer - identify dependencies
- Downloader - fetches all source code
- Scanner - detect license / copyright
- Advisor - retrieves security advisories
- Evaluator - evaluates license / copyright
- Reporter - identify dependencies, licenses, copyrights, policy violations

OSS
Review Toolkit

SBOMs

- OSS Review Toolkit Generates SPDX and Cyclone DX SBOMs out of the box
- Initial investigation is promising
- Currently: we've started accumulating SBOMs
- The dream: to automatically feed these SBOMs back to the project via merge/pull requests against their repositories

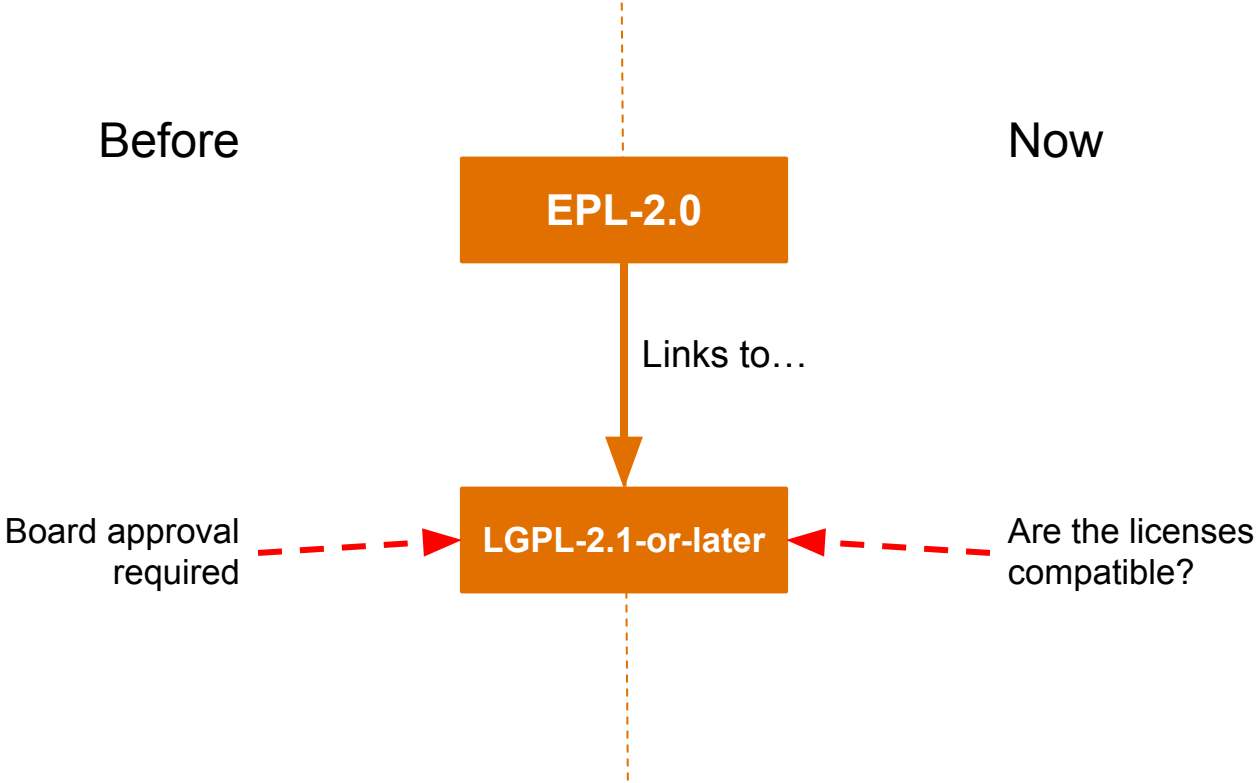
SBOMs generated by ORT are a reflection of the repository contents, not any particular product or artifact

Automation

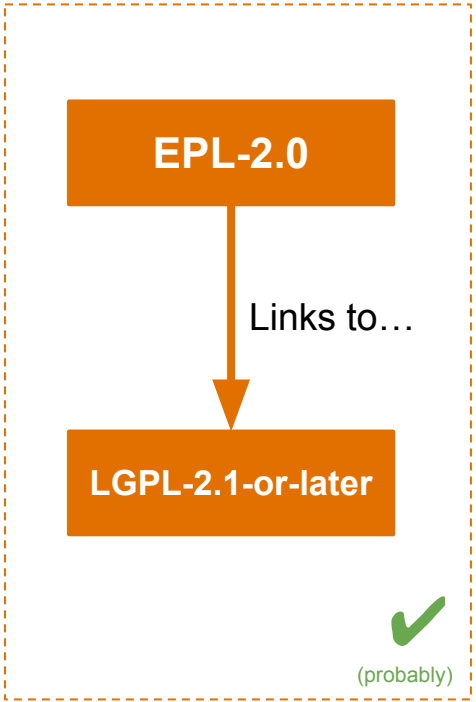
- Easy things are easy
- Easy things are (relatively) easily automated
- Hard things are still hard
- Hard things are still time consuming

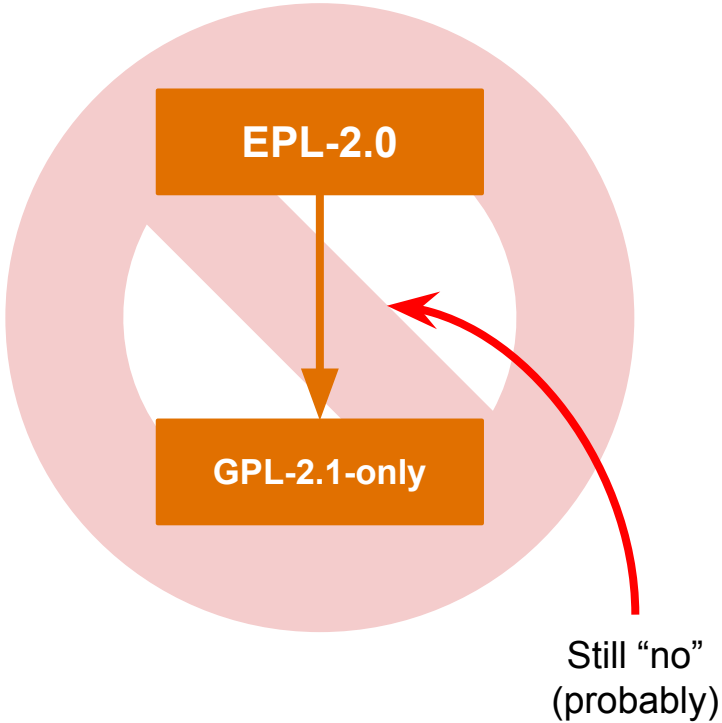
License Compatibility

Approved Licenses



License Compatibility





Not Always Easy

- Permissive licenses: relatively easy
  - Lean on our “approved licenses” list
- Compatible or not?
  - EPL-2.0 or GPL-2.0-only with Classpath-Exception-2.0
  - MPL-2.0-no-copyleft-exception
- Some very popular software is a “dog’s breakfast” of licenses

Automation

- Opens Source Automation Development Lab (OSADL)
  - License checklists
  - License compatibility matrix

Other Things to Think About

While I have your attention…

SPDX Identifiers


```
/*******************************************************************************
 * Copyright (c) {date} {owner}[ and others]
 *
 * This program and the accompanying materials are made available
 * under the terms of the Eclipse Public License v. 2.0 which is
 * available at https://www.eclipse.org/legal/epl-2.0, or the Apache
 * License, Version 2.0 which is available at
 * https://www.apache.org/licenses/LICENSE-2.0.
 *
 * SPDX-License-Identifier: EPL-2.0 OR Apache-2.0
 *******************************************************************************/
```

Relatively hard to parse

Super easy to parse

ECLIPSE FOUNDATION

Evolution of File Headers?


```
// SPDX-License-Identifier: EPL-2.0 OR Apache-2.0
// SPDX-FileCopyrightText: 2020 The Eclipse Foundation
// SPDX-FileCopyrightText: 2021 SAP SE
```

REUSE

- License and Copyright
  - Information must be provided for every file
  - Either embedded or in *.license files
- Alternative: .reuse/dep5 file in repository
- License files in LICENSES directory


```
SPDX-FileCopyrightText: 2015 Contributors to the Eclipse Foundation
SPDX-FileCopyrightText: 2015 Eclipse Foundation

SPDX-License-Identifier: EPL-2.0
```

REUSE dep5

```
Format: https://www.debian.org/doc/packaging-manuals/copyright-format/1.0/
Upstream-Name: Eclipse Dash
Upstream-Contact: Wayne Beaton <wayne.beaton@eclipse-foundation.org>
Source: https://github.com/eclipse/dash-licenses

Files: .project
Copyright: 2019 The Eclipse Foundation
License: EPL-2.0

Files: yarn/yarn.lock
Copyright: 2020 Kichwa Coders Canada Inc.
License: EPL-2.0

Files: core/src/test/java/licenses.json
Copyright: 2017 The Eclipse Foundation
License: EPL-2.0
```

GitBOM

- Consistently construct verifiable Artifact Dependency Graph (ADG)s across languages, environments, and packaging formats, with zero developer effort, involvement, or awareness
- Enable automatic, verifiable artifact resolution across today's diverse software supply chains
- Complement SBOMs, such as SPDX, CycloneDX, or SWID
- Co-exist with, but not require, version control systems

End

Did we even manage to get this far?