Automating OSS Compliance with Fossology, SW360 and SPDX

Anupam Ghosh (anupam.ghosh@siemens.com), Siemens Technology and Services Private Limited

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

Overview: Contents

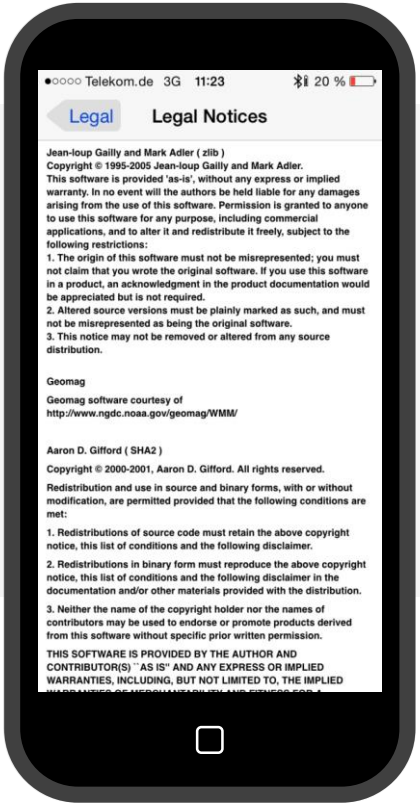
© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

The Problem Actually

You know these examples

Distributing open source software requires to

- Provide licenses of involved software
- Provide copyright statements of involved authors
- Provide disclaimers
- … and much more



© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

It is about finding licenses

fossology

Finding Licenses

- License texts
- References to licenses
- Written texts explaining licensing
- License relevant statements

ProjectRepository.java

ProjectRepository.java 〉 No Selection

```java
/*
 * Copyright Siemens AG, 2013-2015. Part of the SW360 Portal Project.
 *
 * This program is free software; you can redistribute it and/or modify it under
 * the terms of the GNU General Public License Version 2.0 as published by the
 * Free Software Foundation with classpath exception.
 *
 * This program is distributed in the hope that it will be useful, but WITHOUT
 * ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS
 * FOR A PARTICULAR PURPOSE. See the GNU General Public License version 2.0 for
 * more details.
 *
 * You should have received a copy of the GNU General Public License along with
 * this program (please see the COPYING file); if not, write to the Free
 * Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA
 * 02110-1301, USA.

package com.siemens.sw360.datahandler.db;

import com.google.common.collect.Sets;
import com.siemens.sw360.components.summary.ProjectSummary;
import com.siemens.sw360.components.summary.SummaryType;
import com.siemens.sw360.datahandler.couchdb.DatabaseConnector;
import com.siemens.sw360.datahandler.couchdb.SummaryAwareRepository;
import com.siemens.sw360.datahandler.thrift.projects.Project;
import com.siemens.sw360.datahandler.thrift.users.User;
import org.ektorp.support.View;
import org.jetbrains.annotations.NotNull;

import java.util.HashSet;
import java.util.List;
import java.util.Set;

import static com.siemens.sw360.datahandler.common.SW360Utils.getBUFromOrganisation;

/**
 * CRUD access for the Project class
 *
 * @author cedric.bodet@tngtech.com
 * @author Johannes.Najjar@tngtech.com
 */
@View(name = "all", map = "function(doc) { if (doc.type == 'project') emit(null, doc._id) }")
public class ProjectRepository extends SummaryAwareRepository<Project> {
```


© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

What is FOSSology?

A Web server application for license and copyright compliance of software components.

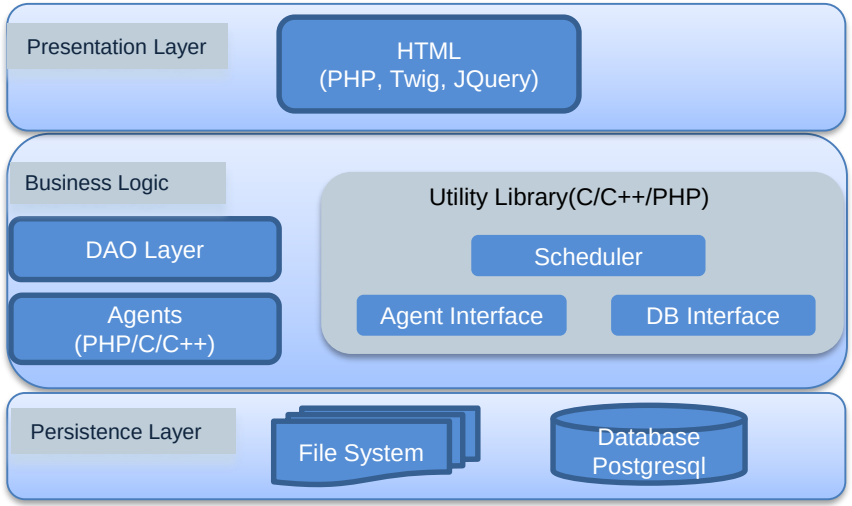
FOSSology Project

https://www.fossology.org/

- Published first in 2008, GPL-2.0
- 2015: Linux Foundation collaboration project
- Web server based and command line interfaces
- Scanning agents searching for license and copyright relevant hits (and more …)
- A multi-user / multi-tenant Web UI for review organizing clearing job

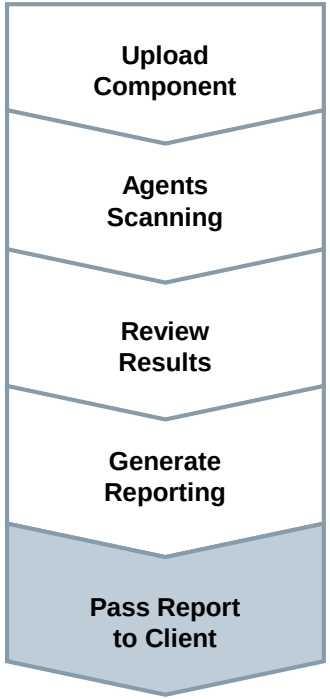
FOSSology Development

https://www.github.com/fossology/fossology



© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

How does FOSSology work? – Overview



- Uploading source code archive (*.zip, *.tar.gz, etc)

- Agents scan for license relevant text (Nomos, Monk, Ojo)
- Copyrights, Export Control (ECC), your keywords to look for etc.

- Review scanner results for wrong license classification
- Review other scanner findings (copyrights, ECC)

- Result of the “clearing”
  - SPDX reporting
  - Generated notice or readme file
  - debian-copyright

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

Fossology REST API

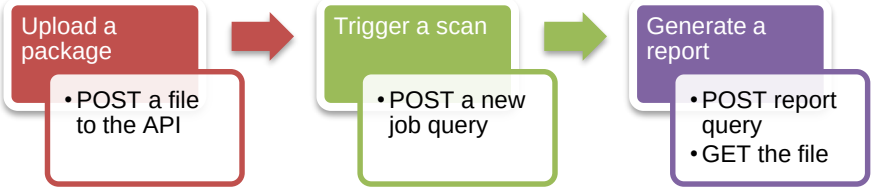
© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

Feature: REST API – Basic functionality

After the release of version 3.4.0, the project has added a REST API to FOSSology

Current Endpoints :

- Uploads
- Folders
- Search
- Users
- Jobs
- Reports
- Tokens



https://www.fossology.org/get-started/basic-rest-api-calls/

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

SW360 Introduction

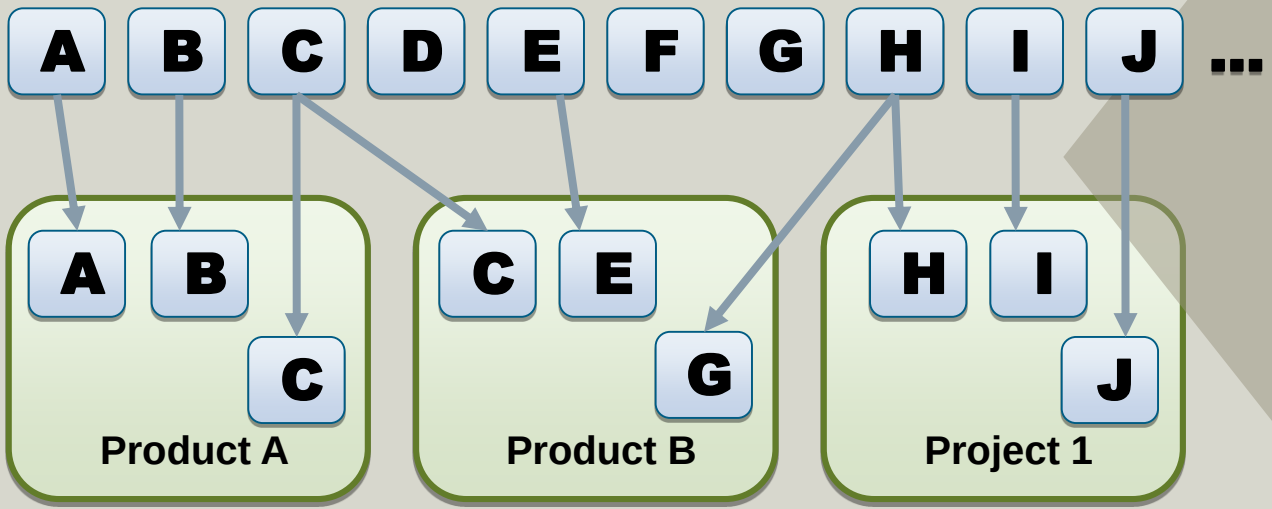
Eclipse SW360 – An Open Source Component Hub

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

Introduction

SW360 is a 3rd party software component catalogue

Assigns 3rd party components to products or projects



Goals and Benefits

- Reuse information about components
- Coordinate product documentation process
- Support software clearing

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

SW360 and Liferay Portal Community Edition

SW360 is an application based on Liferay Portal Community Edition

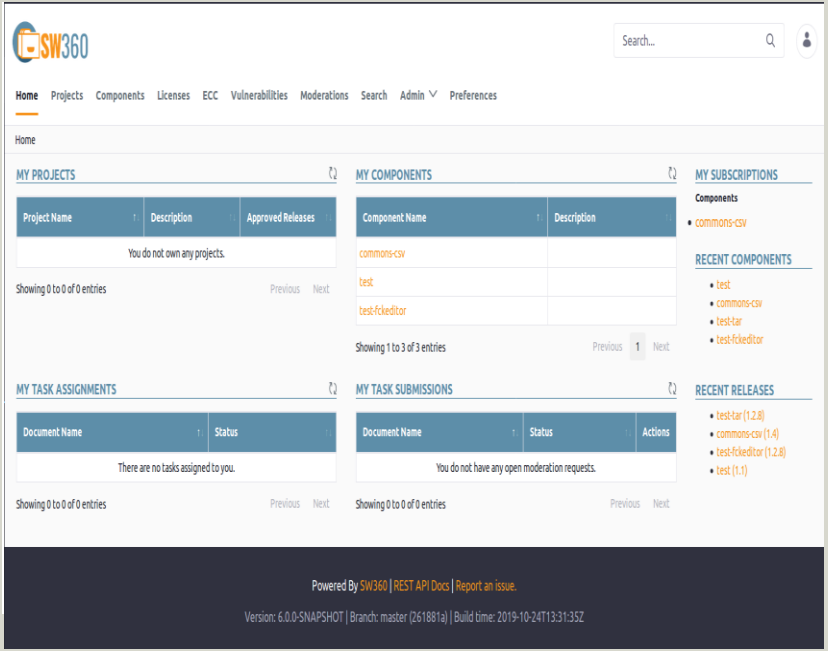
- SW360 uses Liferay Portal CE as portal server
  - updated to 7.2.x
- Liferay Portal community edition, LGPL-2.1.-or later

Advantages

- Many Liferay-based solutions exist
- Proven user, session and data management
- Further technologies ready for future adoption:
  - Mobile device support
  - Marketplace of add-ons
  - Collaboration and Social tools

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

Main Use Case 1: Component Inventory Database

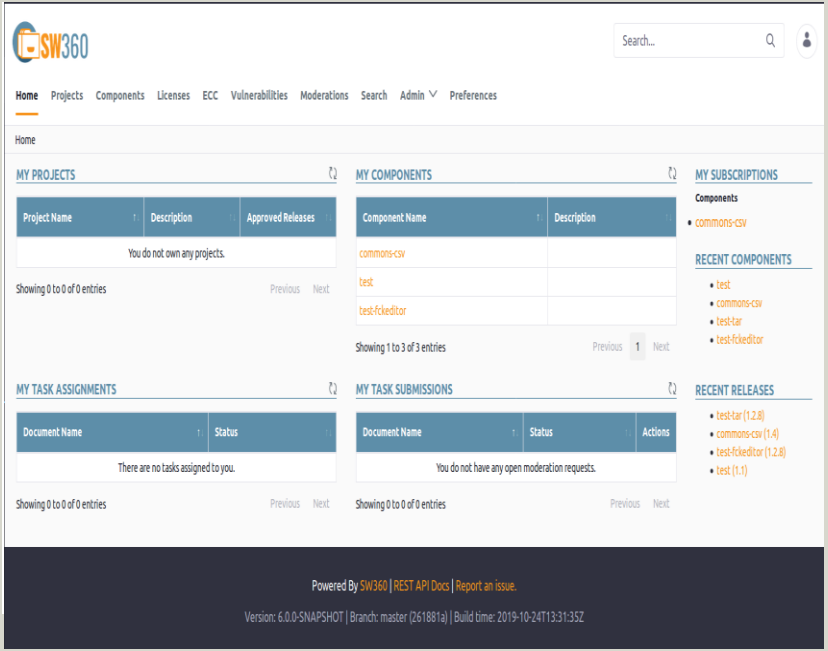


Collect Information about Components

- **It is about Components in use:** for all others, Internet can do better
- **OSS Licensing:** collect analysed licensing information (and reuse analyses)
- **Not OSS only:** internal components, commercial, freeware
- **More information:** ECC, vulnerabilities, statistics, static code analyses, etc.

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

Main Use Case 2: Bill-of-Material Management

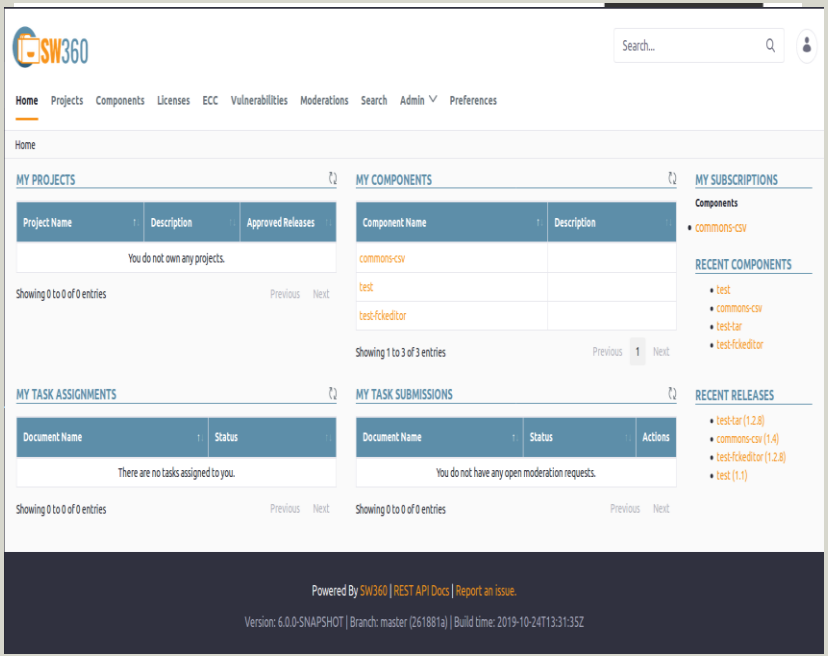


BOM. Inventory Management

- **Understand which software component is used in which products**
- **Product / Project:** holds relation to releases of components
- **Component Catalogue:** captures organisation information of components and releases

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

Main Use Case 3: Product Documentation



Readme OSS / NOTICE Generation

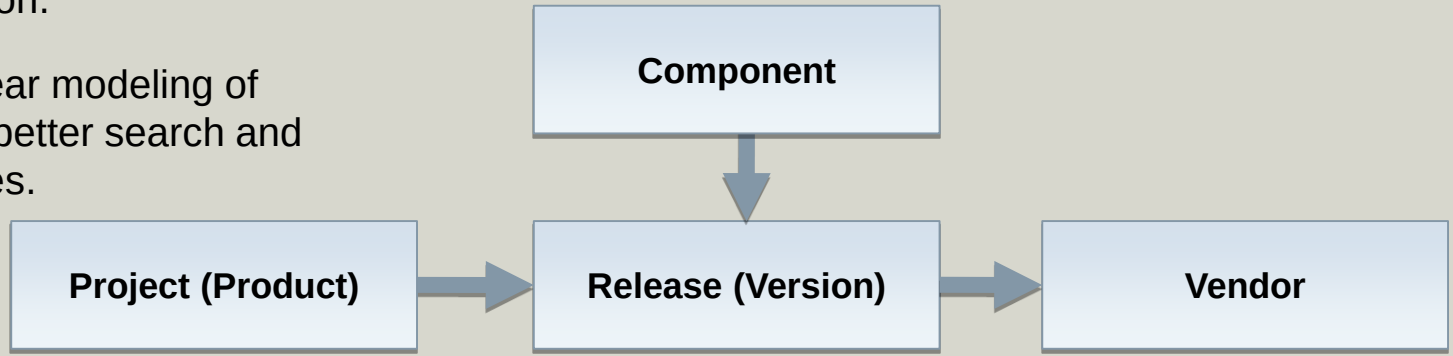
- **Create Component Releases**
- **Upload SPDX file:** exchange file for Licenses, Copyrights and Acknowledgements
- **Create Project:** and add the component releases
- **Generate documentation:** For all linked releases, license information is collected for generation

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

Basic Data Model

Goals and Motivation

- Clean Component Catalogue: Reduction of duplicate entries.
- Separating vendor and version from the name of the components brings clarity to component identification.
- Interoperation with other systems: support the CPE standard which also implement this 3-parts separation.
- Having the clear modeling of data enables better search and filtering abilities.



© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

Demo

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

Summary

1. **FOSSology for precise license analysis**
2. FOSSology is a mature framework and Web application for license analysis
3. **SPDX Report**
4. review of SPDX documents and … reuse of licensing info at new versions
5. **Sw360 software component catalogue**
6. Beyond exchange of license information: Complete documentation of analysis
7. **Obligations / Policies handling**
8. Organise obligations with the found licenses.
9. **Rest API**
10. Integrate Fossology and Sw360

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0

Thank you very much - … some links:

© 2016-2019 Siemens AG, The Linux Foundation

Internet

https://www.fossology.org/
https://www.eclipse.org/sw360/

Github

https://github.com/fossology/fossology
https://github.com/eclipse/sw360

Further Links

https://www.spdx.org
https://www.openchainproject.org

© 2016-2019 Siemens AG, Linux Foundation - CC-BY-SA 4.0