



## Automating OSS Compliance with Fossology, SW360 and SPDX

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

# Overview: Contents



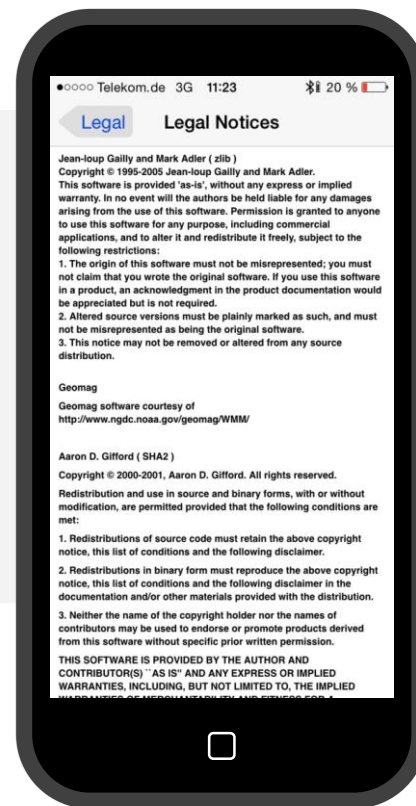
- 1. Introduction to FOSSology**
2. What is FOSSology
- 3. Introduction to Sw360**
4. What is Sw360
- 5. FOSSology REST Interface**
6. Demo
- 7. FOSSology and sw360 Integration**
- 8. Conclusion**

# The Problem Actually

## You know these examples

Distributing open source software requires to

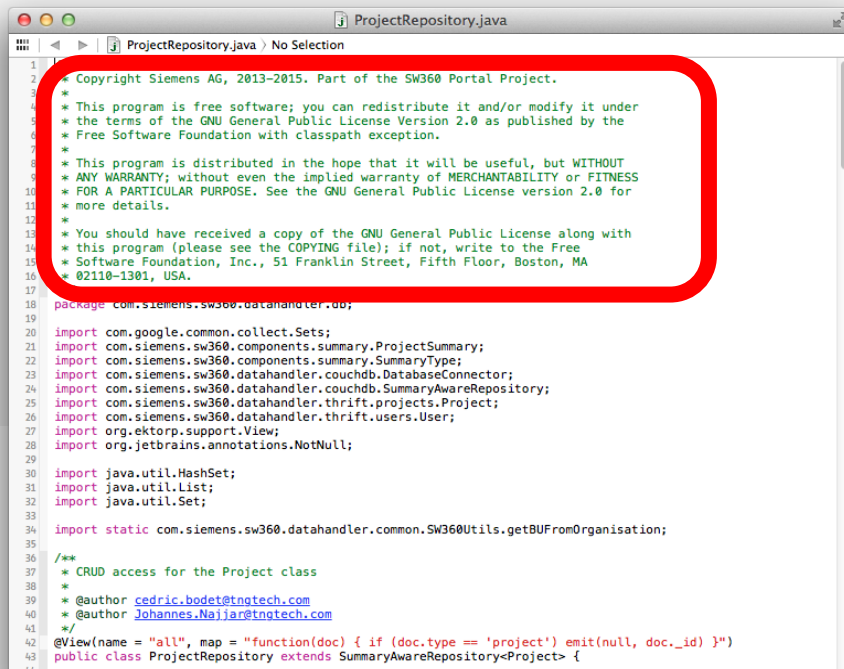
- Provide licenses of involved software
- Provide copyright statements of involved authors
- Provide disclaimers
- ... and much more



# It is about finding licenses

## Finding Licenses

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



```
1  * Copyright Siemens AG, 2013-2015. Part of the SW360 Portal Project.
2  *
3  * This program is free software; you can redistribute it and/or modify it under
4  * the terms of the GNU General Public License Version 2.0 as published by the
5  * Free Software Foundation with classpath exception.
6  *
7  * This program is distributed in the hope that it will be useful, but WITHOUT
8  * ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS
9  * FOR A PARTICULAR PURPOSE. See the GNU General Public License version 2.0 for
10 * more details.
11 *
12 * You should have received a copy of the GNU General Public License along with
13 * this program (please see the COPYING file); if not, write to the Free
14 * Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA
15 * 02110-1301, USA.
16
17 package com.siemens.sw360.datahandler.db;
18
19
20 import com.google.common.collect.Sets;
21 import com.siemens.sw360.components.summary.ProjectSummary;
22 import com.siemens.sw360.components.summary.SummaryType;
23 import com.siemens.sw360.datahandler.couchdb.DatabaseConnector;
24 import com.siemens.sw360.datahandler.couchdb.SummaryAwareRepository;
25 import com.siemens.sw360.datahandler.thrift.projects.Project;
26 import com.siemens.sw360.datahandler.thrift.users.User;
27 import org.ektorp.support.View;
28 import org.jetbrains.annotations.NotNull;
29
30 import java.util.HashSet;
31 import java.util.List;
32 import java.util.Set;
33
34 import static com.siemens.sw360.datahandler.common.SW360Utils.getBUFFromOrganisation;
35
36 /**
37  * CRUD access for the Project class
38  *
39  * @author cedric.bodet@tngtech.com
40  * @author Johannes.Najjar@tngtech.com
41  */
42 @View(name = "all", map = "function(doc) { if (doc.type == 'project') emit(null, doc._id) }")
43 public class ProjectRepository extends SummaryAwareRepository<Project> {
44
45 }
```

# What is FOSSology?



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

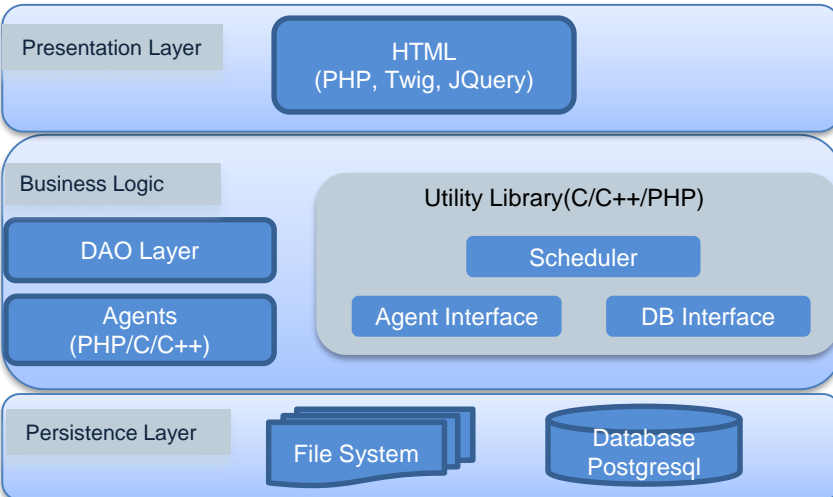
## FOSSology Project

<https://www.fossology.org/>

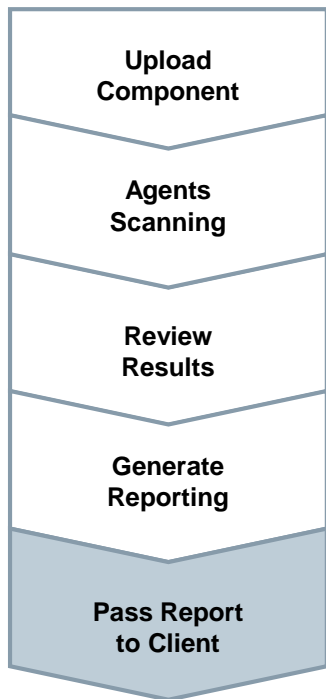
- Published first in 2008, GPL-2.0
- 2015: Linux Foundation collaboration project
- Web server based and command line interfaces
- Scanning agents searching for license and copyright relevant hits (and more ...)
- A multi-user / multi-tenant Web UI for review organizing clearing job

## FOSSology Development

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



# 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

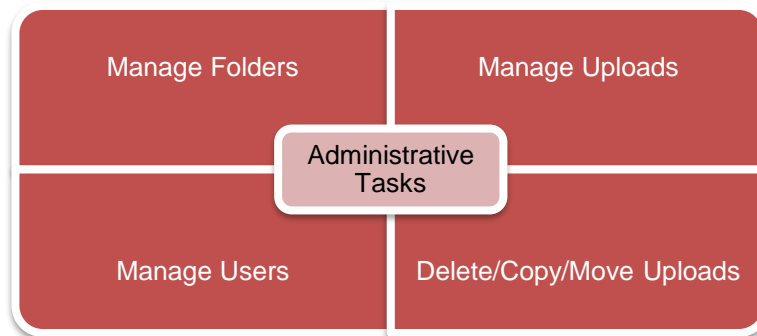
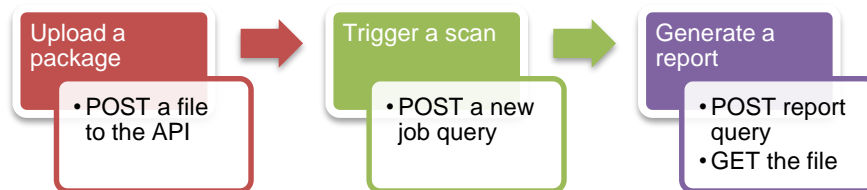
# Fossology REST API

# 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/>





Open Source License  
Compliance by Open  
Source Software

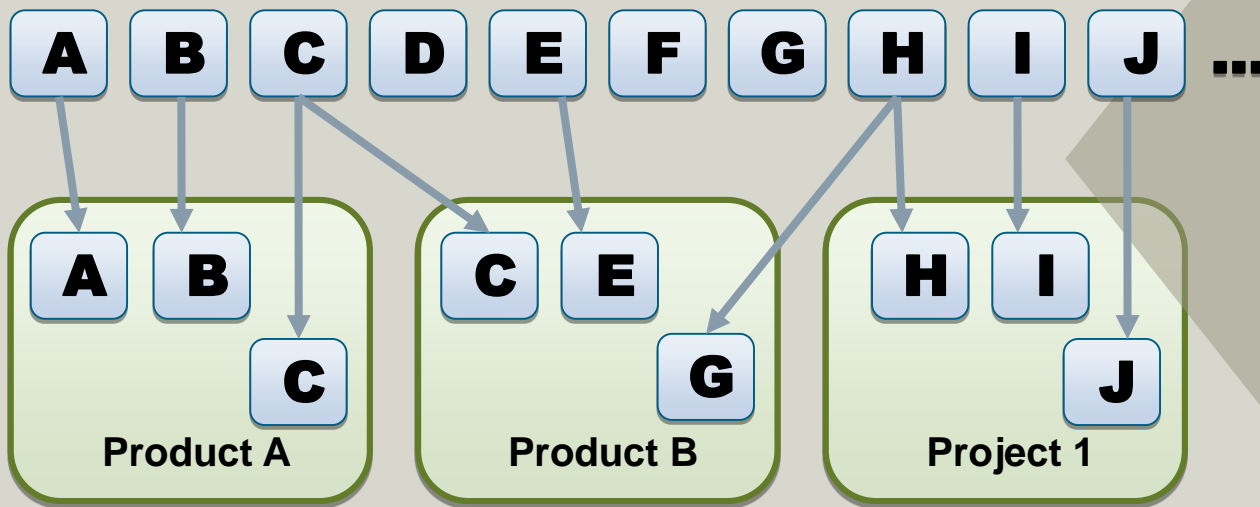
# SW360 Introduction

Eclipse SW360 – An Open Source Component Hub

# Introduction

SW360 is a 3<sup>rd</sup> party software component catalogue

Assigns 3<sup>rd</sup> party components to products or projects



## Goals and Benefits

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

# 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

# Main Use Case 1: Component Inventory Database



The screenshot displays the SW360 web application interface. At the top, there is a navigation bar with links for Home, Projects, Components, Licenses, ECC, Vulnerabilities, Moderations, Search, Admin, and Preferences. A search bar and a user profile icon are also present. The main content area is divided into several sections:

- MY PROJECTS:** A table with columns for Project Name, Description, and Approved Releases. It shows a message: "You do not own any projects." Below the table, it says "Showing 0 to 0 of 0 entries" with Previous and Next navigation links.
- MY TASK ASSIGNMENTS:** A table with columns for Document Name and Status. It shows a message: "There are no tasks assigned to you." Below the table, it says "Showing 0 to 0 of 0 entries" with Previous and Next navigation links.
- MY COMPONENTS:** A table with columns for Component Name and Description. It lists components: commons-csv, test, and test-fckeditor. Below the table, it says "Showing 1 to 3 of 3 entries" with Previous and Next navigation links.
- MY TASK SUBMISSIONS:** A table with columns for Document Name, Status, and Actions. It shows a message: "You do not have any open moderation requests." Below the table, it says "Showing 0 to 0 of 0 entries" with Previous and Next navigation links.
- MY SUBSCRIPTIONS:** A section titled "Components" showing a list of components: commons-csv, test, commons-csv, test-tar, and test-fckeditor.
- RECENT COMPONENTS:** A section showing a list of components: test, commons-csv, test-tar, and test-fckeditor.
- RECENT RELEASES:** A section showing a list of releases: test-tar (1.2.8), commons-csv (1.4), test-fckeditor (1.2.8), and test (1.1).

At the bottom of the page, there is a footer with the text: "Powered By SW360 | REST API Docs | Report an issue." and "Version: 6.0.0-SNAPSHOT | Branch: master (261881a) | Build time: 2019-10-24T13:31:35Z".

## 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.

# Main Use Case 2: Bill-of-Material Management



The screenshot displays the SW360 web application interface. At the top, there is a navigation bar with links to Home, Projects, Components, Licenses, ECC, Vulnerabilities, Moderations, Search, Admin, and Preferences. Below the navigation bar, the main content area is divided into several sections:

- MY PROJECTS:** A table with columns for Project Name, Description, and Approved Releases. It shows a message: "You do not own any projects." and "Showing 0 to 0 of 0 entries".
- MY COMPONENTS:** A table with columns for Component Name and Description. It lists components: commons-csv, test, and test-fckeditor. It shows "Showing 1 to 3 of 3 entries".
- MY SUBSCRIPTIONS:** A section titled "Components" listing commons-csv. Below it, "RECENT COMPONENTS" lists test, commons-csv, test-tar, and test-fckeditor.
- MY TASK ASSIGNMENTS:** A table with columns for Document Name and Status. It shows a message: "There are no tasks assigned to you." and "Showing 0 to 0 of 0 entries".
- MY TASK SUBMISSIONS:** A table with columns for Document Name, Status, and Actions. It shows a message: "You do not have any open moderation requests." and "Showing 0 to 0 of 0 entries".
- RECENT RELEASES:** A section listing recent releases: test-tar (1.2.8), commons-csv (1.4), test-fckeditor (1.2.8), and test (1.1).

At the bottom of the page, there is a footer with the text: "Powered By SW360 | REST API Docs | Report an issue." and "Version: 6.0.0-SNAPSHOT | Branch: master (261881a) | Build time: 2019-10-24T13:31:35Z".

## 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

# Main Use Case 3: Product Documentation



The screenshot displays the SW360 web application interface. At the top, there is a navigation bar with links for Home, Projects, Components, Licenses, ECC, Vulnerabilities, Moderations, Search, Admin, and Preferences. A search bar and a user profile icon are also present. The main content area is divided into several sections:

- MY PROJECTS:** A table with columns 'Project Name', 'Description', and 'Approved Releases'. It shows a message: "You do not own any projects." Below the table, it says "Showing 0 to 0 of 0 entries" with 'Previous' and 'Next' buttons.
- MY COMPONENTS:** A table with columns 'Component Name' and 'Description'. It lists components: 'commons-csv', 'test', and 'test-fckeditor'. Below the table, it says "Showing 1 to 3 of 3 entries" with 'Previous', '1', and 'Next' buttons.
- MY TASK ASSIGNMENTS:** A table with columns 'Document Name' and 'Status'. It shows a message: "There are no tasks assigned to you." Below the table, it says "Showing 0 to 0 of 0 entries" with 'Previous' and 'Next' buttons.
- MY TASK SUBMISSIONS:** A table with columns 'Document Name', 'Status', and 'Actions'. It shows a message: "You do not have any open moderation requests." Below the table, it says "Showing 0 to 0 of 0 entries" with 'Previous' and 'Next' buttons.
- MY SUBSCRIPTIONS:** A section titled 'Components' showing a list of components: 'commons-csv', 'test', 'commons-csv', 'test-tar', and 'test-fckeditor'.
- RECENT COMPONENTS:** A list of components: 'test', 'commons-csv', 'test-tar', and 'test-fckeditor'.
- RECENT RELEASES:** A list of releases: 'test-tar (1.2.8)', 'commons-csv (1.4)', 'test-fckeditor (1.2.8)', and 'test (1.1)'.

At the bottom of the page, there is a footer with the text: "Powered By SW360 | REST API Docs | Report an issue." and "Version: 6.0.0-SNAPSHOT | Branch: master (261881a) | Build time: 2019-10-24T13:31:35Z".

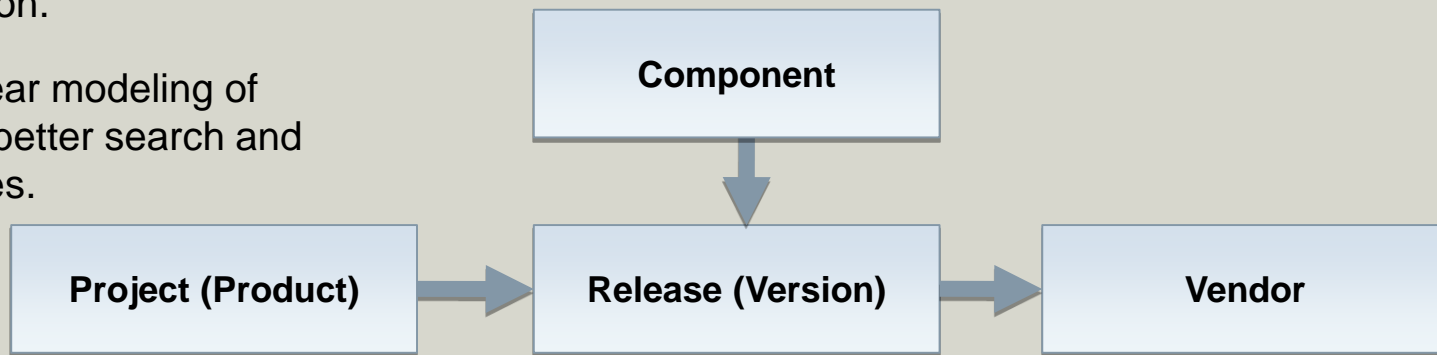
## Readme OSS / NOTICE Generation

- **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

# 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.



# Demo



# 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

# 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>