Free and Open Source Software Auditing (FOSSA) Pilot Project

DISSEMINATION MATERIALS

WP3 EXECUTIVE SUMMARY

The FOSSA Pilot project aims at a systematic approach for the EU institutions to contribute to free and open source software (FOSS), namely to ensure that widely used critical software can be trusted. It will help reinforcing the contribution of EU institutions to ensure and maintain integrity and security of key FOSS.

FOSSA Work Package 3 (WP3) has defined an inventory methodology, to obtain a complete inventory of free and open source software and standards used within the European Parliament and the European Commission and to identify the critical software for its submission to code review.

Interviews have been conducted with stakeholders from both the EC and the EP to collect evidence on the current software databases and the information available on software and standards.

The main deliverables of WP3 are:

A. a **replicable methodology to build and maintain an inventory of free and open source software and open standards**

The proposed inventory process aims at integrating the existing inventory databases, managed by different Units in the European Institutions and containing heterogeneous information, into a comprehensive software inventory, through the following steps:

- Partially automated collection and integration of software inventory data from existing databases; filtering of Open Source Software (OSS);
- Ranking of OSS components by criticality;
- Detailed analysis of critical software to add metadata on dependencies;
- Inventory of standards, obtained by cross-checking the data on standards applicable to the inventoried OSS software with external libraries and analysing dependencies.

B. the **Inventory architecture**

It is made up of four layers:

1. Raw data from existing databases;
2. ETL (Extract/Transform/Load), where inventory data are extracted from the raw data and normalized;
3. Database engine, hosting the inventory data and used to filter the OSS;
4. Presentation layer, i.e. the dashboard where the software ranking and analysis is performed to identify the most critical software components, candidate for a code review.

For each layer, WP3 has analysed and recommended specific tools, based on criteria evaluating their reliability. Consistently with the nature of the FOSSA project, only open source tools have been considered.

Once DIGIT has validated the recommended tools, the project team has proceeded with their **installation and configuration** on a shared repository.

Finally, WP3 has identified several **longer-term improvement areas** that will lead to a more efficient and streamlined inventory process, more automatized and substantially real-time.