SIEMENS
Ingenuity for life

FOSSology License Compliance and Automation

Michael C. Jaeger & Thomas Graf, Siemens AG

Inhalt

SIEMENS
Ingenuity for life

Was ist FOSSology?

SIEMENS
Ingenuity for life

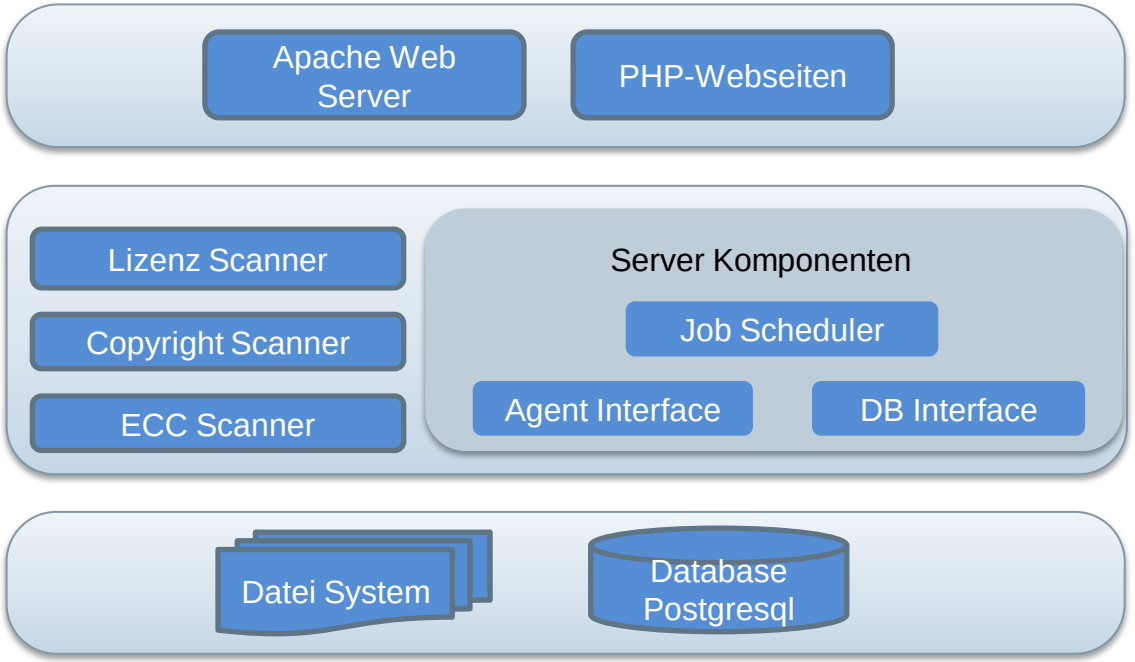
FOSSology Projekt

https://www.fossology.org/

- Veröffentlicht in 2008, GPL-2.0
- 2015: Linux Foundation Collaboration Projekt
- Toolkit für License Compliance
- Scanning Agenten für relevante Informationen, UI für Analyse
- Server-Anwendung für eine Multi-User / Multi-Tenant Benutzung durch Web Browser

FOSSology Entwicklung

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



FOSSology – Automatisierung und Analyse

SIEMENS
Ingenuity for life

Building Blocks Automatisierung

Kommandozeilentools um FOSSology server “fernzusteuern”: Cp2foss, fo-licenselist, etc.

Kommandozeilentools um einzelne Funktionen separat aufzurufen

- Lizenz Scanner
- Copyright Scanner
- ECC Scanner

XML-Datenformate (SPDX) für Export und Import von Compliance Informationen

Latest: FOSSology REST Interface #1198

Analyse und Begutachtung

- Ermittlung Lizenz-relevanter Aussagen
- Hervorhebung von Textstellen
- Erfassen von Textstellen
- Erzeugen vielfältiger Dokumentionen
  - Zur Auslieferung: Textdatei oder SPDX
  - Oder Org-intern: SPDX

Wonach scannen wir eigentlich? – unter anderem:

SIEMENS
Ingenuity for life

Lizenz Texte	Lizenz Header	Lizenz Metadaten	Prosaische Lizensierung	Urheberrechts vermerke
• GPL Text • MIT Text • Etc. • Meist auf Top Ebene auf einer Distribution	• Standard Header von Lizenzen • Oder Spezielle Header	• SPDX-License Identifier • Package Metadaten	• Prosaischer Verweis auf eine bekannte Lizenz • Prosaische Lizensierunstexte	• “Copyright 2018 Software Bauer”

Scanning oder Analyse? – Begutachtung ist Sinnvoll II

SIEMENS
Ingenuity for life

Es gibt angepasste Lizenztexte:

- Varianten der BSD Lizenzen: z.B. BSD-3-Clause Text mit einem Abschnitt ersetzt
- Varianten beim Hauftungsausschlüssen, Nennungen der Urheber bei Texten von
  - z.B. X11: andere organisation statt “X Consortium”
  - NTP: Anpassungen des Urhebers
  - Weitere Texte
    - Inbesondere in denen die Nennung der Urheber naheliegt
    - Insbesondere in den Hauftungsausschlüssen

Scanning oder Analyse? – Begutachtung ist Sinnvoll I

SIEMENS
Ingenuity for life

Es gibt viel mehr Lizenzen als in der SPDX License List … Beispiele:

- Jabber Open Source License Version 1.0 “This Jabber Open Source License (the "License") applies to Jabber Server and related software products as well as any updates…”
- Arphic Public License: “Copyright (C) 1999 Arphic Technology Co., Ltd. 11Fl. No.168, Yung Chi Rd., Taipei, 110 Taiwan All rights reserved except as specified below…”
- The Catharon Open Source LICENSE: “2000-Jul-04 Copyright (C) 2000 by Catharon Productions, Inc. Introduction This license applies to source files distributed by Catharon:”
- Espressif General Public License: “PREAMBLE The Espressif General Public License is a free, copyleft license for software and other kinds of works …”

Scanning oder Analyse? – Begutachtung ist Sinnvoll III

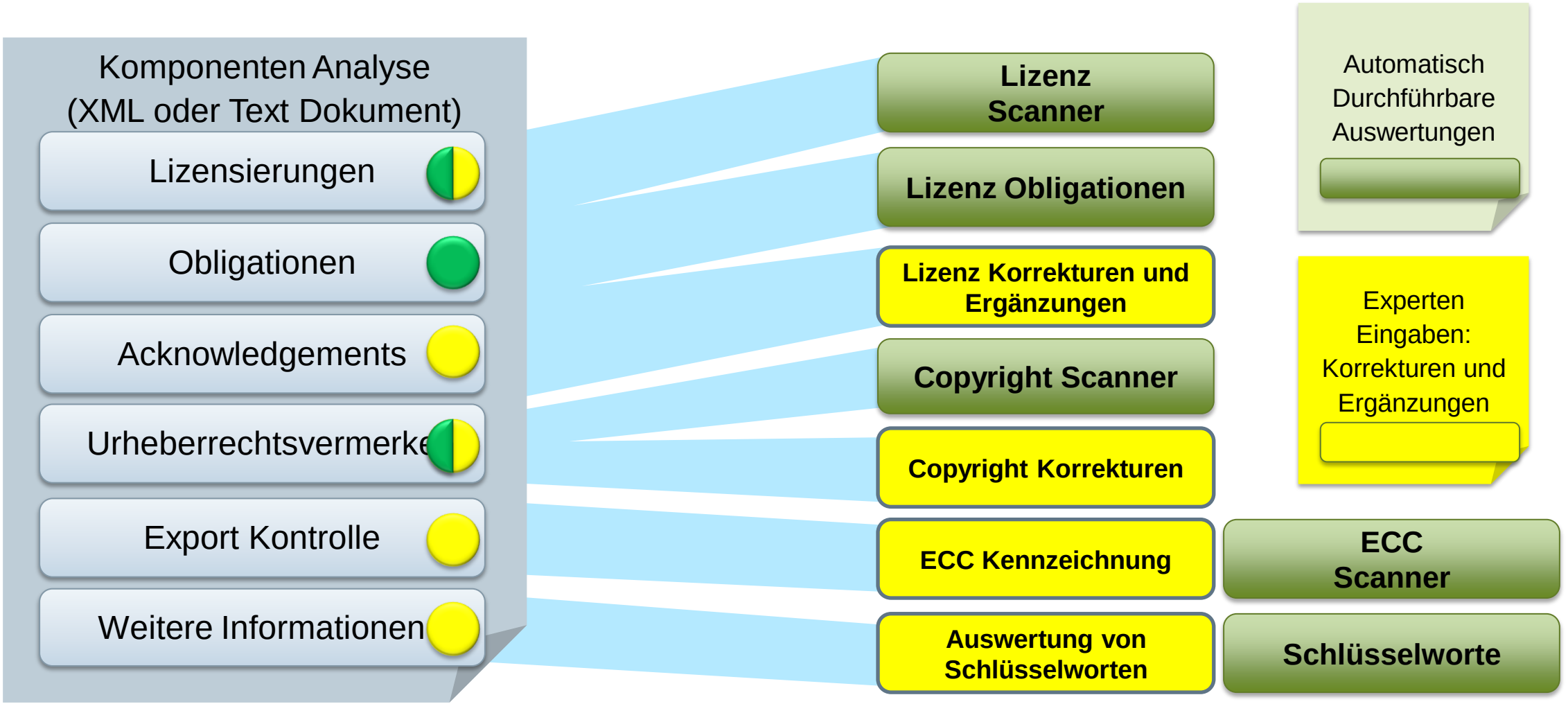
SIEMENS
Ingenuity for life

Auch in “vermeindlicher” OSS existieren proprietäre Lizensierungen

This software is the confidential and proprietary information of *** ***, Inc. ("Confidential Information"). You shall not disclose such Confidential Information and shall use it only in accordance with the terms of the license.

FOSSology – Was automatisiert werden kann

SIEMENS
Ingenuity for life



FOSSology bei Siemens Building Technologies

SIEMENS
Ingenuity for life

Siemens

380.000

20.000

20.000

Building Technologies

28.000

1.000

16

OSS

250

1.000

➔ Jede Fremdsoftware muss bei uns einen Freigabeprozess durchlaufen, bei dem geprüft wird, unter welchen Bedingungen wir die Software verwenden können.

Was brauchen wir?

SIEMENS
Ingenuity for life

Wir benötigen

- Lizenzinformationen
- Urheber-Informationen (Copyrights)
- Falls vorhanden: Informationen über Patente, Exportkontrollinformationen, etc.

Man könnte einfach die Informationen nehmen die auf GitHub, OpenHub, etc. verfügbar sind, aber …

- … Lizenzinformationen sind unvollständig
- … Copyrights sind nur bruchstückhaft aufgelistet
- … Informationen über Patente, Exportkontrolle, etc. sind in einzelnen Dateien im gesamten Quellcode verteilt

Wir brauchen aber fundierte Information, die auch vor Gericht verwendbar wären …
OLG Hamburg: man darf sich nicht auf die Zusicherung von Lieferanten verlassen, sondern muss eine Überprüfung in geeigneter Weise durchführen.

*) Urteil LG Hamburg, Az. 308 = 10/13

Warum FOSSology?

SIEMENS
Ingenuity for life

FOSSology bietet uns genau das was wir brauchen:

- Suche nach Lizenzen **und** Copyrights **und** weiteren Stichwörtern
  ➔ wir brauchen keine weiteren Werkzeuge

- Hohe Treffsicherheit und **niedrige Anzahl an False-Positives**

- **Delta-Überprüfung**, d.h. FOSSology merkt sich die Informationen über einzelne Dateien. Bei einer neuen Version einer Komponente müssen also nur noch neue bzw. geänderte Dateien überprüft werden. Insbesondere mit Hinblick auf Sicherheitsschwachstellen und damit verbundene Updates auf neuere Versionen ist das ein großer Vorteil

- Export der Ergebnisse in vielen verschiedenen Formaten, darunter SPDX aber auch als Word-Dokument

Warum FOSSology?

SIEMENS
Ingenuity for life

- Aber vor allem deshalb, weil wir alle Scan-Ergebnisse **sichten und editieren** können, so dass in unseren Berichten zu den Software-Komponenten auch nur das steht, was wirklich lizenzrechtlich relevant ist

- Diese editierten Ergebnisse können wir dann ausgeben in **einem Report** der
- … alle vollständigen Lizenztexte enthält
- … alle Copyright-Statements
- … alle Acknowledgements
- … und eine Liste der Obligationen die erfüllt werden müssen

Vergleich von Scan-Ergebnissen: Bootstrap 3.3.6

SIEMENS
Ingenuity for life

	Homepage	GitHub	OpenHub	ScanCode	FOSSology Scan	FOSSology (bearbeitet*)
Lizenz	Code: **MIT** Docs: CC-BY-3.0	Code: **MIT** Docs: CC-BY-3.0	**MIT**	**MIT** BSD **GPL-1.0** Apache-2.0 CC-BY-3.0 Public Domain Unlicense	**MIT** **GPL-3.0** Apache-2.0 Public Domain CC-BY-3.0 Dual-licensed X11	**MIT** Public Domain CC-BY-3.0
Copyright	(Twitter, Inc.)	2011-2016 Twitter, Inc.	---	19 Copyrights, davon 4 False-Positives	62 Copyrights, davon 25 False-Positives	19 Copyrights

Bearbeitet bedeutet

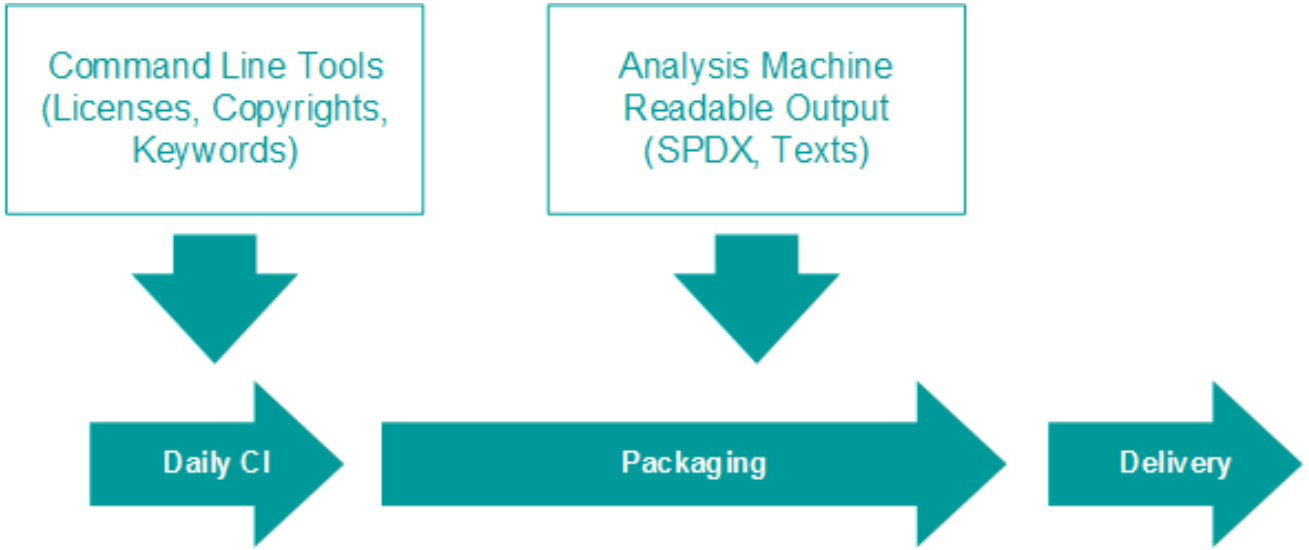
- Das Dual-License Statement bezieht sich auf MIT oder GPL-3.0. Sonst gibt es keinen Hinweis auf GPL-3.0. Alle diese Dateien sind im `docs` Ordner und werden normalerweise nicht ausgeliefert.
- Auch die Apache-2.0 bzw. X11-lizensierten Dateien sind nur Dokumentation.
- CC-BY-3.0 kommt auch in den ausgeliefertes Stylesheets vor, muss also angegeben werden.

FOSSology – Bereit für Automatisierung

SIEMENS
Ingenuity for life

FOSSology ist ein Baukasten:

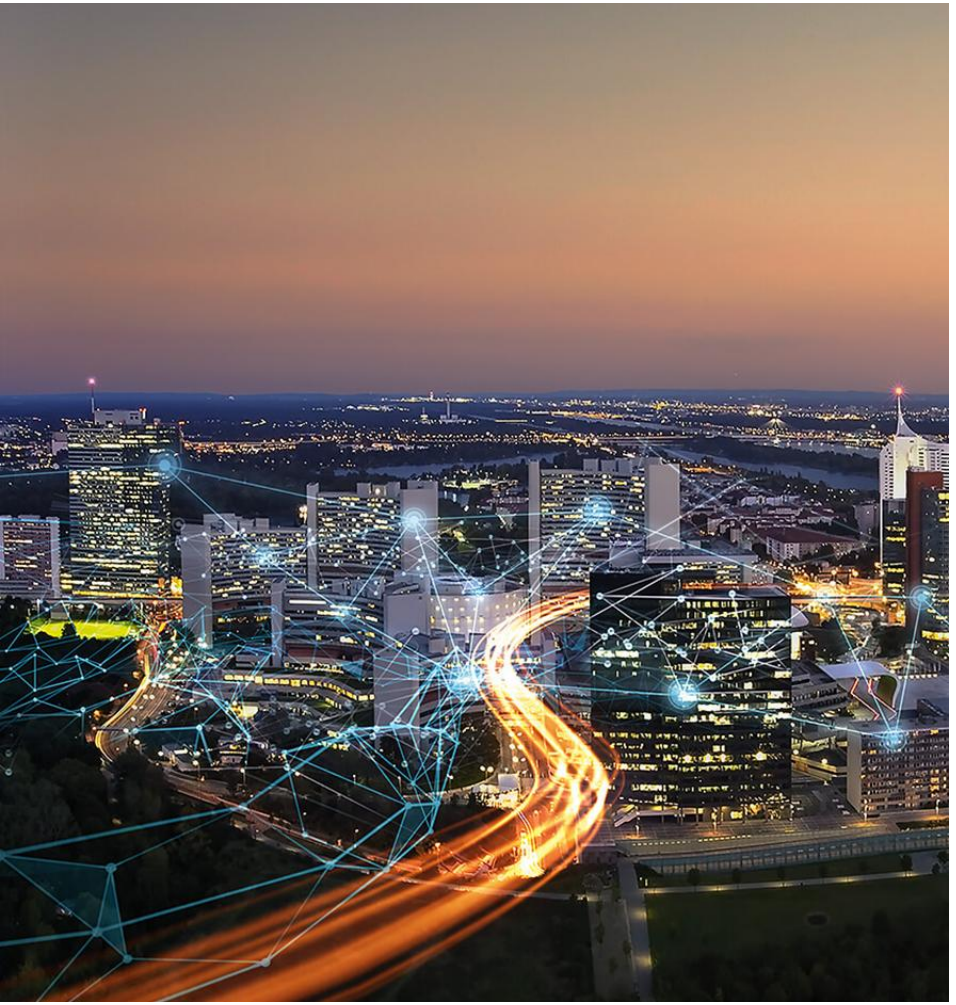
- Scanner, Command Line Tools, Server, Repository und User Interface
- Einzelne Elemente sind unabhängig verwendbar
- XML/Text Formate für die Weiterverarbeitung
- Ein Teil der Lizenzanalyse kann automatisiert werden
- Experten müssen bei Regelabweichungen eingreifen



Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

SIEMENS
Ingenuity for life



Thomas Graf
Senior Software Clearing Expert
BT SSP R&D

E-mail:
thomas.graf@siemens.com

Dr. Michael C. Jaeger
FOSSology Maintainer
CT RDA SSI

E-mail:
michael.c.jaeger@siemens.com

siemens.com

SIEMENS
Ingenuity for life

Backup

SIEMENS
Ingenuity for life

Key Message:

Die Umsetzung von License Compliance ist ein Customizing Projekt –
Organisationen und Entwicklungsprojekte sind zu unterschiedlich
für eine One-Size-Fits-All Lösung.
FOSSology ist ein Baukasten mit unterschiedlichen Elementen,
die in eine License Compliance Lösung integriert werden können.