

Innovationsverbund
Öffentliche Gesundheit

#WIRVSVIRUS

Björn Steiger Stiftung
WIR HELFEN LEBEN RETTEN

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

The CRA: A key to a more resilient FOSS ecosystem

Lessons to be learned from non-digital supply chains

13.10.2026 - Community over Code - Glasgow

https://inoeg.de gregor.bransky@inoeg.de https://mastodon.social/@dcsi https://codeberg.org/dcsi

What's the Cyber Resilience Act? - Goals of the CRA

- Reducing vulnerabilities in digital products
- Cyber Security maintenance throughout a product's life cycle
- Empower users to make informed decisions
- Goes into full effect by 11. December 2027

What do those three items have in common?



ECO-DIM.10 WiFi
LED dimmer module 250W

What do those three items have in common?



ECO-DIM.10 WiFi
LED dimmer module 250W



AK-SM 800A
System Control

What do those three items have in common?



ECO-DIM.10 WiFi
LED dimmer module 250W



AK-SM 800A
System Control



Parmesan
Cheese Wheel

What do those three items have in common? Subject to the CRA



ECO-DIM.10 WiFi
LED dimmer module 250W



AK-SM 800A
System Control



Parmesan
Cheese Wheel

What do those three items have in common? Subject to the CRA





AK-SM 800A
System Control



Parmesan
Cheese Wheel

formerly known as **RAPEX**

What do those three items have in common? Subject to the CRA





AK-SM 800A
System Control



Parmesan
Cheese Wheel

European Commission

Safety Gate: the EU rapid alert system for dangerous non-food products

Home | Safety Gate alerts | Reports and publications | Product safety in the EU | Buyi safe

Home > Safety Gate: the EU rapid alert system for dangerous non-food products

Alert number: SR/01437/26

Published on 22/05/2026 - Report-2026-20

Notifying country	The Netherlands
Product category	Lighting equipment
Product	Wi-Fi dimmer switch

The manufacturer's instructions suggest that the product can be installed with two wires under a screw terminal. This may cause sparking and lead to a fire.

formerly known as **RAPEX**

What do those three items have in common? Subject to the CRA







European Commission

Safety Gate: the EU rapid alert system for dangerous non-food products

Home | Safety Gate alerts | Reports and publications | Product safety in the EU | Buyi safe

Home > Safety Gate: the EU rapid alert system for dangerous non-food products

Alert number: SR/01437/26

Published on 22/05/2026 - Report-2026-20

Notifying country	The Netherlands
Product category	Lighting equipment
Product	Wi-Fi dimmer switch

The manufacturer's instructions
two wires under a screw termina

n | Sport | Culture | Lifestyle

The Guardian

Eur

s Asia Australia Middle East Africa Inequality Global development

Hackers force French supermarket fridges to heat up to 50C in 'unprecedented' cyber-attack

Hundreds of Intermarché shops and Coopérative U outlets in France hit, with fears Dutch chains also affected

Most viewed

Ilhan Omar says she v be silenced after fede agents raid her home

RJ Mitte, actor best k for Breaking Bad, die

m

heel

formerly known as **RAPEX**

What do those three items have in common? Subject to the CRA







European Commission

Safety Gate: the EU rapid alert system for dangerous non-food products

Home | Safety Gate alerts | Reports and publications | Product safety in the EU

Home > Safety Gate: the EU rapid alert system for dangerous non-food products

Alert number: SR/01437/26

Published on 22/05/2026 - Report-2026-20

Notifying country	The Netherlands
Product category	Lighting equipment
Product	Wi-Fi dimmer switch

formerly known as **RAPEX**

The Guardian

Sport | Culture | Lifestyle

Asia | Australia | Middle East | Africa | Inequality | Global development

Hackers force French supermarket fridges to heat up to 50C in 'unprecedented' cyber-attack

Hundreds of Intermarché shops and Coopérative U outlets in France hit, with fears Dutch chains also affected

The Guardian

Sport | Culture | Lifestyle

Asia | Australia | Middle East | Africa | Inequality | Global development

This article is more than 3 years old

Cheese and chips: parmesan producers fight fakes with microtransponders

Counterfeits are the bane of the Parmigiano Reggiano Consortium, which is now trialling tech in the rind

Most viewed

Ilhan Omar says she be silenced after fed agents raid her hom

RJ Mitte, actor best for Breaking Bad, di 34

Cheese is still save!

Hypothesis

“The CRA introduced the concept of product regulation and liability to all products with digital elements and their corresponding supply chains.

Hypothesis

“The CRA introduced the concept of product regulation and liability to all products with digital elements and their corresponding supply chains.

This will make technical debt and software supply chain risks a financially quantifiable risk and thus visible on balance sheets of publicly traded companies and in product insurance contracts.

Hypothesis

“The CRA introduced the concept of product regulation and liability to all products with digital elements and their corresponding supply chains.

This will make technical debt and software supply chain risks a financially quantifiable risk and thus visible on balance sheets of publicly traded companies and in product insurance contracts.

There are lessons to be learned from non-digtial supply chains with regards to technical documentation as well as finance flows to improve the technical quality of software.”

Hypothesis & Open Question

“The CRA introduced the concept of product regulation and liability to all products with digital elements and their corresponding supply chains.

This will make technical debt and software supply chain risks a financially quantifiable risk and thus visible on balance sheets of publicly traded companies and in product insurance contracts.

There are lessons to be learned from non-digital supply chains with regards to technical documentation as well as finance flows to improve the technical quality of software.”

What kind of tooling could be build to operationalize these learnings?

Hypothesis & Open Question & BoF?

“The CRA introduced the concept of product regulation and liability to all products with digital elements and their corresponding supply chains.

This will make technical debt and software supply chain risks a financially quantifiable risk and thus visible on balance sheets of publicly traded companies and in product insurance contracts.

There are lessons to be learned from non-digtial supply chains with regards to technical documentation as well as finance flows to improve the technical quality of software.”

What kind of tooling could be build to operationalize these learnings?

events.apache.org/events/2026/community-over-code/bof.html#foss-suite

Agenda

- Who’s talking, and why?
- Products with digital elements - a supply chain perspective
- Classical vs. digital supply chains - what´s the difference?
- Why public benefit stewards / 501 (c)3s for digital commons?
- rfc: supply chain centered communication

Who is talking? Gregor “Little Detritus” Bransky



- Theoretical Physicist - Complexity theory for QCs

Who is talking? Gregor “Little Detritus” Bransky



- Theoretical Physicist - Complexity theory for QCs
- Consultant for tech strategy in industrial production

Who is talking? Gregor “Little Detritus” Bransky



- Theoretical Physicist - Complexity theory for QCs
- Consultant for tech strategy in industrial production
- Involved in public digital infrastructures since 2016
  Freifunk (2016), Civic-Tech (2020)

Who is talking? Gregor “Little Detritus” Bransky



- Theoretical Physicist - Complexity theory for QCs
- Consultant for tech strategy in industrial production
- Involved in public digital infrastructures since 2016
  Freifunk (2016), Civic-Tech (2020)
- Works on software supply chains security & CRA (2022)

Who is talking? Gregor “Little Detritus” Bransky



- Theoretical Physicist - Complexity theory for QCs
- Consultant for tech strategy in industrial production
- Involved in public digital infrastructures since 2016
  Freifunk (2016), Civic-Tech (2020)
- Works on software supply chains security & CRA (2022)
  - Boardmember Policy & Press Innovation Council public health e.V.
  - Open Regulatory Compliance - ORC WG - Eclipse
  - Supplchain Integrity, Transparency & Trust - SCITT WG - IETF
  - Cyber Manual Movement contributor

5 steps toward Community over code



2023 - Isabel Drost-Fromm

“Volunteered Talk” Security.txt for gits FOSSBackstage23

5 steps toward Community over code





- 2023 - Isabel Drost-Fromm
  “Volunteered Talk” Security.txt for gits FOSSBackstage23
- 2024 - Shane Curcuru
  Gave a talk “Who funds FOSS Foundations?” FOSSBackstage24

5 steps toward Community over code







- 2023 - Isabel Drost-Fromm
  “Volunteered Talk” Security.txt for gits FOSSBackstage23
- 2024 - Shane Curcuru
  Gave a talk “Who funds FOSS Foundations?” FOSSBackstage24
- 2024 - Open Forum Europe incl. Dirk Wilhelm van Gulik
  Introduced Open Source Software Stewards into the CRA

5 steps toward Community over code



- 2023 - Isabel Drost-Fromm
  “Volunteered Talk” Security.txt for gits FOSSBackstage23
- 2024 - Shane Curcuru
  Gave a talk “Who funds FOSS Foundations?” FOSSBackstage24
- 2024 - Open Forum Europe incl. Dirk Wilhelm van Gulik
  Introduced Open Source Software Stewards into the CRA
- 2026 - Jarek Potiuk
  I like Fair Share Cost tokens, come to Community over Code!

5 steps toward Community over code



- 2023 - Isabel Drost-Fromm
  “Volunteered Talk” Security.txt for gits FOSSBackstage23
- 2024 - Shane Curcuru
  Gave a talk “Who funds FOSS Foundations?” FOSSBackstage24
- 2024 - Open Forum Europe incl. Dirk Wilhelm van Gulik
  Introduced Open Source Software Stewards into the CRA
- 2026 - Jarek Potiuk
  I like Fair Share Cost tokens, come to Community over Code!
- 2026 - Jan Lenhard
  We worked on supply chain tooling for a decade, let´s build!

What’s the Cyber Resilience Act? - It’s not alone

EXECUTIVE ORDER 14028, IMPROVING THE NATION'S CYBERSECURITY

Software Supply Chain Security Guidance +

Cybersecurity Labeling for Consumers +

Workshops & Call for

Improving the Nation's Cybersecurity: NIST’s Responsibilities Under the May 2021 Executive Order

Overview | Completed Assignments | Latest Updates

What's the Cyber Resilience Act? - It's not alone

EXECUTIVE ORDER 14028, IMPROVING THE NATION'S CYBERSECURITY

Secure Software Development Framework SSDF

So
Se

ponsibilities

Cy
fo

Overview

We

NIST has finalized SP 800-218A, *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile*. This publication augments SP 800-218 by adding practices,

What’s the Cyber Resilience Act? - It’s not alone

EXECUTIVE ORDER 14028, IMPROVING THE NATION'S CYBERSECURITY

Secure Software Development Framework SSDF



Open Source Security Foundation Raises $10 Million in New Commitments to Secure Software Supply Chains

October 13, 2021 | Press Release

Software Supply Chain Communication - for Compliance

EXECUTIVE ORDER 14028, IMPROVING THE NATION'S CYBERSECURITY

Secure Software Development Framework SSDF

Cyber Resilience Act enters into force to make Europe's cyberspace safer and more secure

PRESS RELEASE

Publication 10 December 2024

The Cyber Resilience Act, a landmark piece of legislation, entered into force. This marks a major leap forward in the EU's efforts to protect its citizens and businesses from cyber threats.

The Cyber Resilience Act (CRA) is the **first-ever EU legislation** placing mandatory cybersecurity requirements for products that include digital elements.

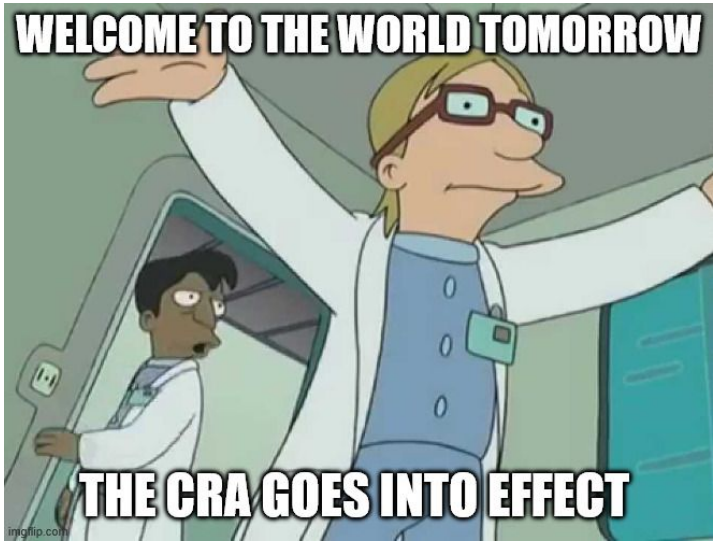
The Act introduces greater responsibilities on manufacturers to guarantee the security of hardware and software products. Central to the Act are new obligations for manufacturers to provide software updates that **fix security vulnerabilities and offer security support to consumers**. By enhancing transparency on cyber risks and product security, the Act empowers consumers to make more informed choices about products available on the EU market.



GettyImages © Peach_iStock

What are products with digital components?

- Starting 11. December 2027
- Manufacturers have to:
  - Meet essential security requirements
  - Patch vulnerabilities for at least 5 years - for free
  - Report security incidents to authorities
  - Share fixes with FOSS Projects
  - Create “information & instructions to the user”
  - Audit the FOSS Software they are using
- Or?
  - Penalty:
    max(15 Mio. € , 2,5 % total worldwide annual turnover)
  - Liability:
    Product Liability directive



Let´s talk about critical infrastructure



Products with digital elements - a supply chain perspective



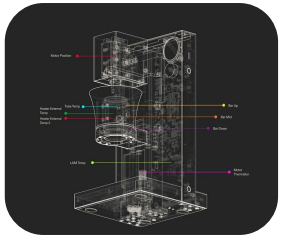
Products with digital elements - a supply chain perspective





Products with digital elements - a supply chain perspective

Manufacturer



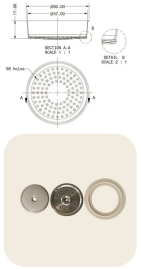


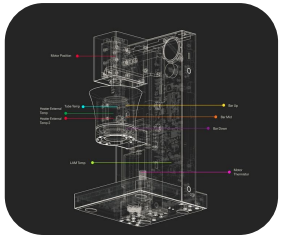


Products with digital elements - a supply chain perspective

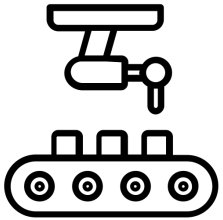
Regulation & Standards | Component | Manufacturer | Assembly | Product

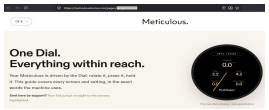






...





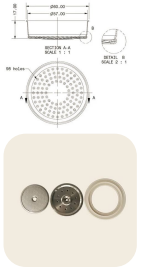




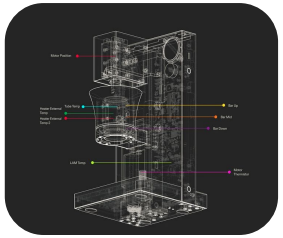
Products with digital elements - a supply chain perspective

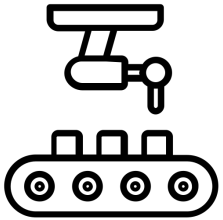
Regulation & Standards | Component | Manufacturer | Assembly | Product

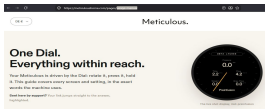


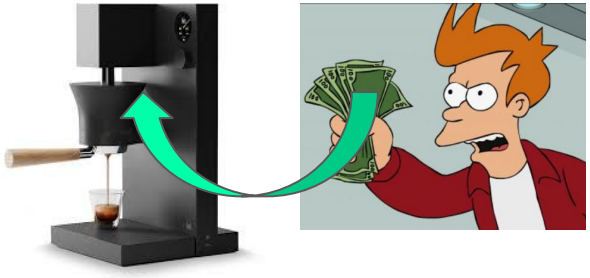


...





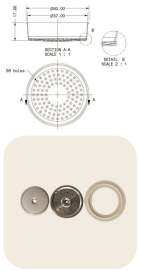




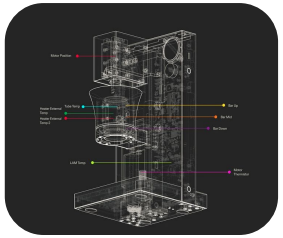
Products with digital elements - a supply chain perspective

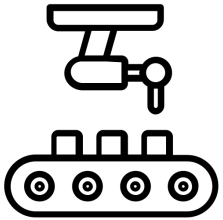
Regulation & Standards | Component | Manufacturer | Assembly | Product





...













Products with digital elements - a supply chain perspective

Regulation & Standards

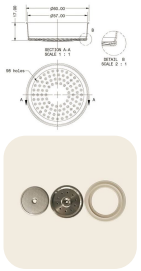
Component

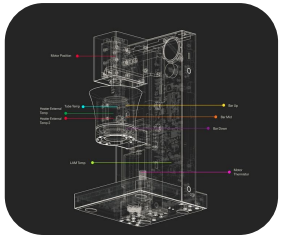
Manufacturer

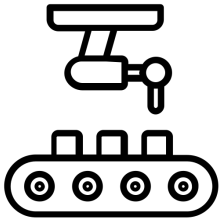
Assembly

Product









...



Products with digital elements - a supply chain perspective

Regulation & Standards

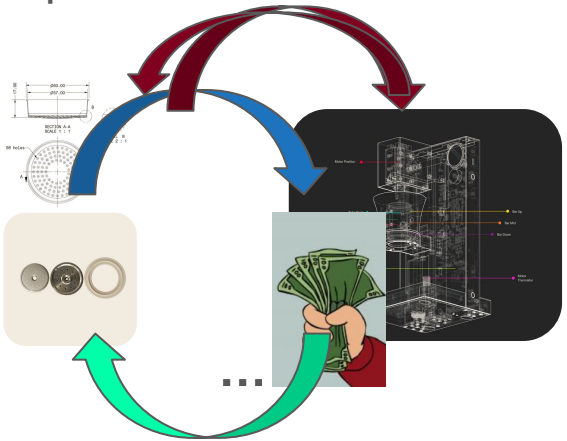
Component

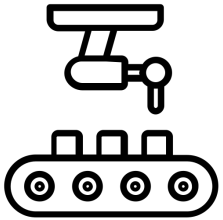
Manufacturer

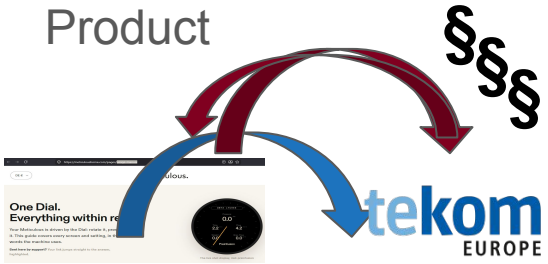
Assembly

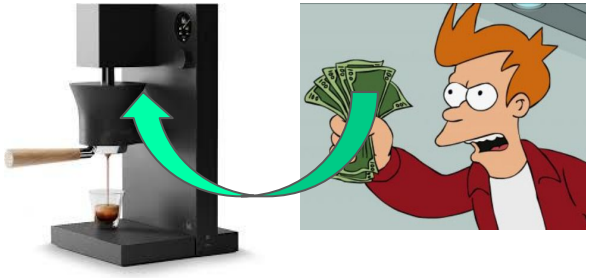
Product











Products with digital elements - a supply chain perspective



Products with digital elements - a supply chain perspective

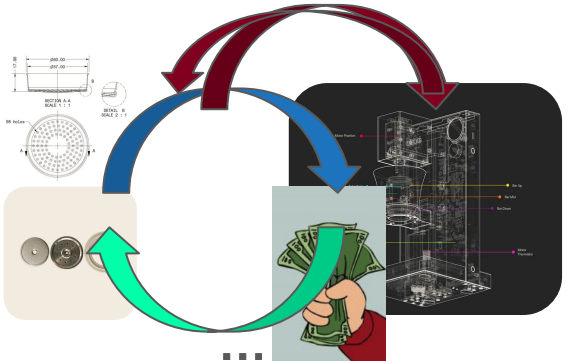
Regulation & Standards

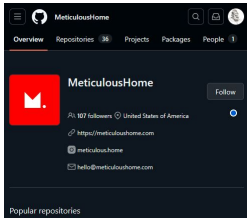
Component

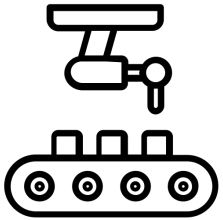
Manufacturer

Assembly

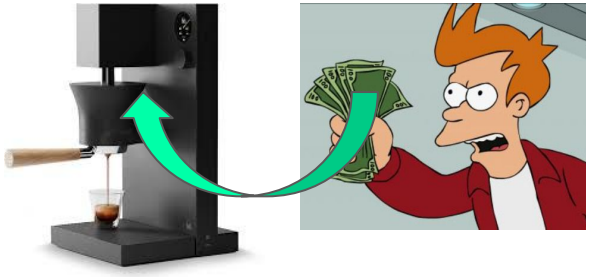
Product











Products with digital elements - a supply chain perspective

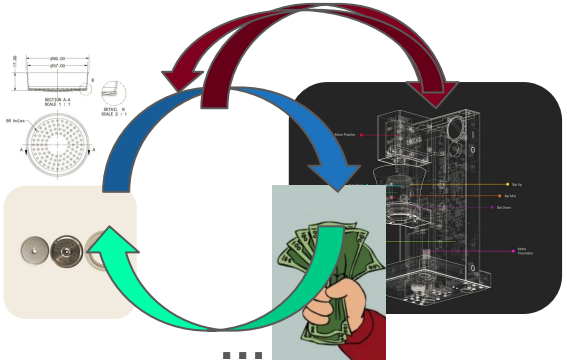
Regulation & Standards

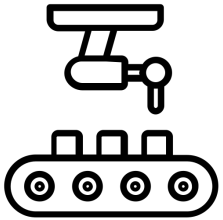
Component

Manufacturer

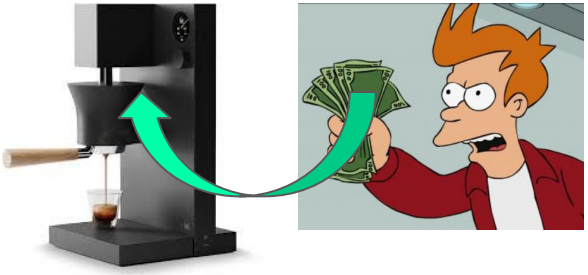
Assembly

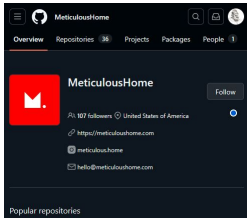
Product











Products with digital elements - a supply chain perspective

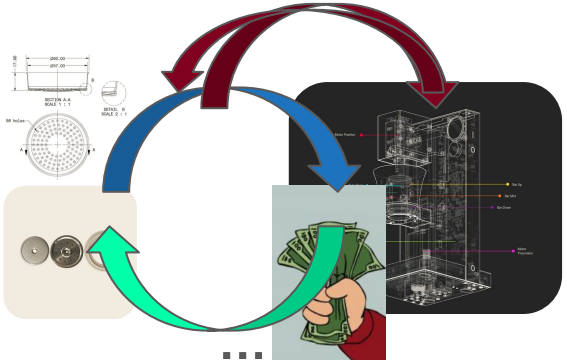
Regulation & Standards

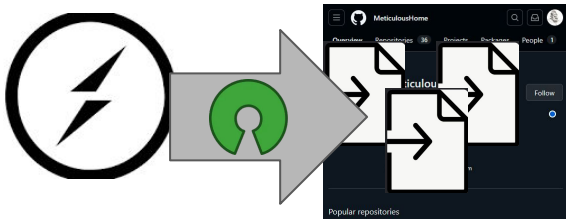
Component

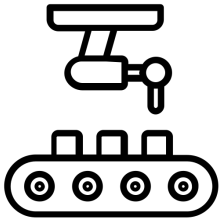
Manufacturer

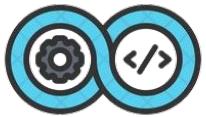
Assembly

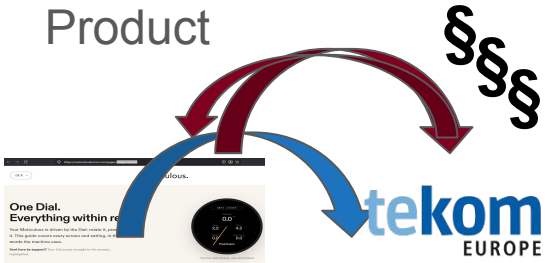
Product

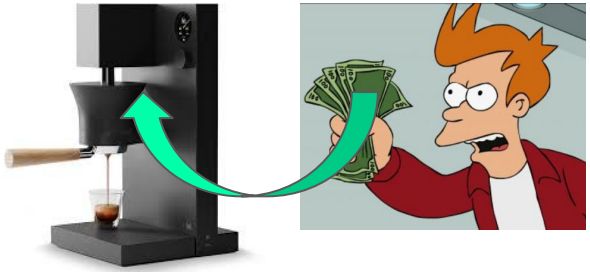












The five pillars of products with digital elements

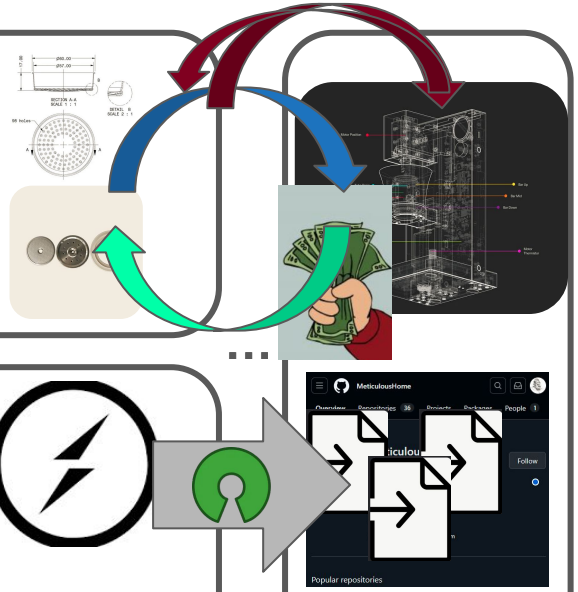
Regulation & Standards

Component

Manufacturer

Assembly

Product









The five pillars of products with digital elements

Regulation & Standards

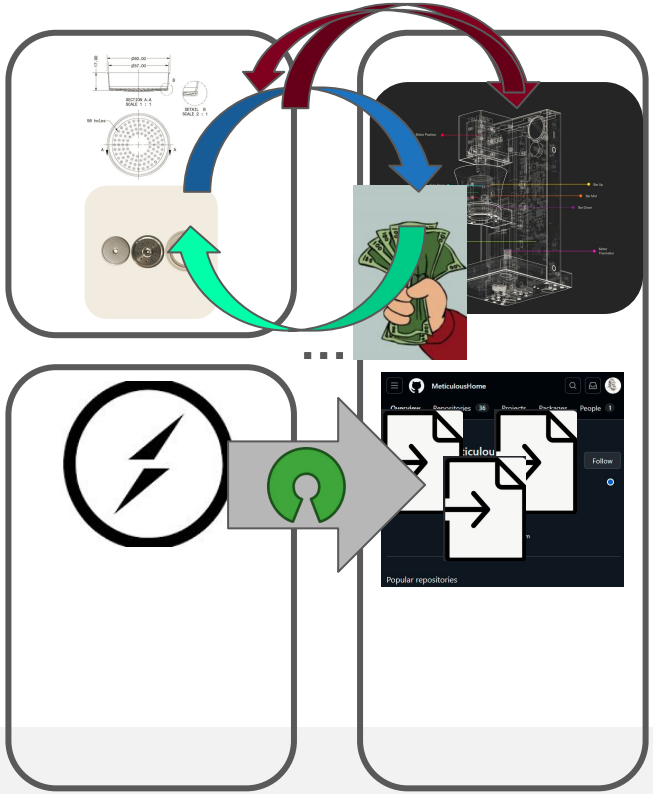
Component

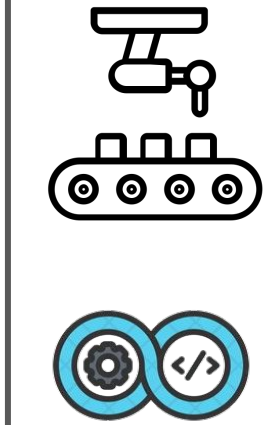
Manufacturer

Assembly

Product











Products with digital elements a supply chain perspective

- Starting 11. December 2027
- Manufacturers have to:
  - Meet essential security requirements
  - Patch vulnerabilities for at least 5 years - for fr
  - Report security incidents to authorities
  - Share fixes with FOSS Projects
  - Create **“information & instructions to the user”**
  - Audit the FOSS Software they are using
- Or?
  - Penalty:
    max(15 Mio. € , 2,5 % total worldwide annual turnover)
  - Liability:
    Product Liability directive



CYBER MANUAL MOVEMENT

Which future will we choose?

All products will have cyber manuals in 2028. The question is what they will look like.

Cybersecurity Manual

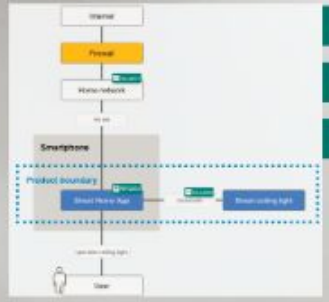
⚠ CAUTION

- **DO NOT line the oven walls, racks, bottom, aluminum foil or any other material.** Doi produce poor baking results and cause per (aluminum foil will melt to the interior surfac
- Never attempt to dry a pet in the oven.



Cybersecurity Manual

- This is how the product works
- Do this to use it securely



REQ 001

REQ 002

REQ 003

The five pillars of products with digital elements

Regulation & Standards

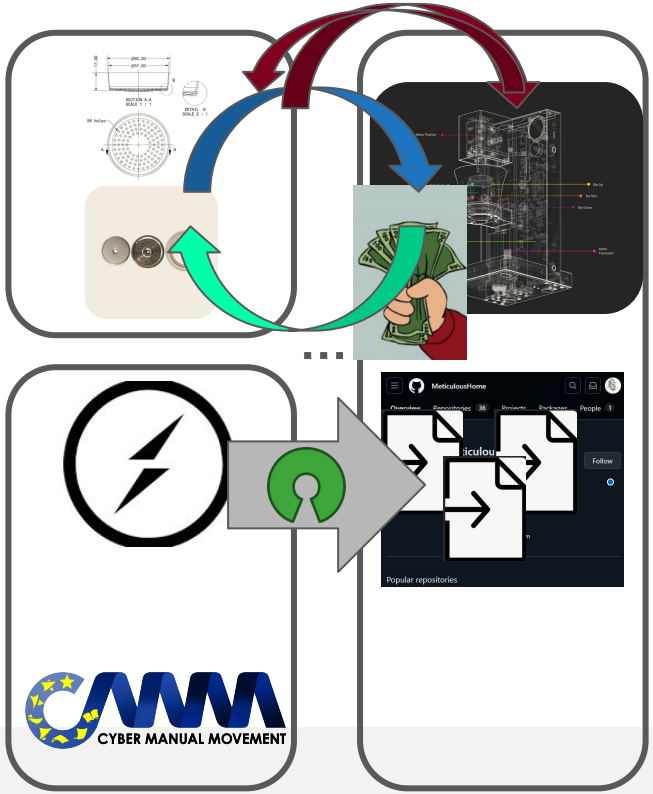
Component

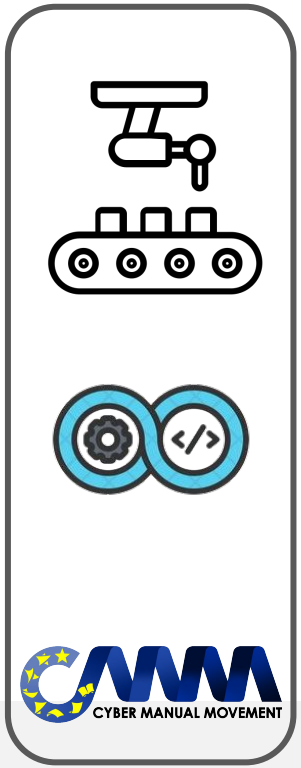
Manufacturer

Assembly

Product



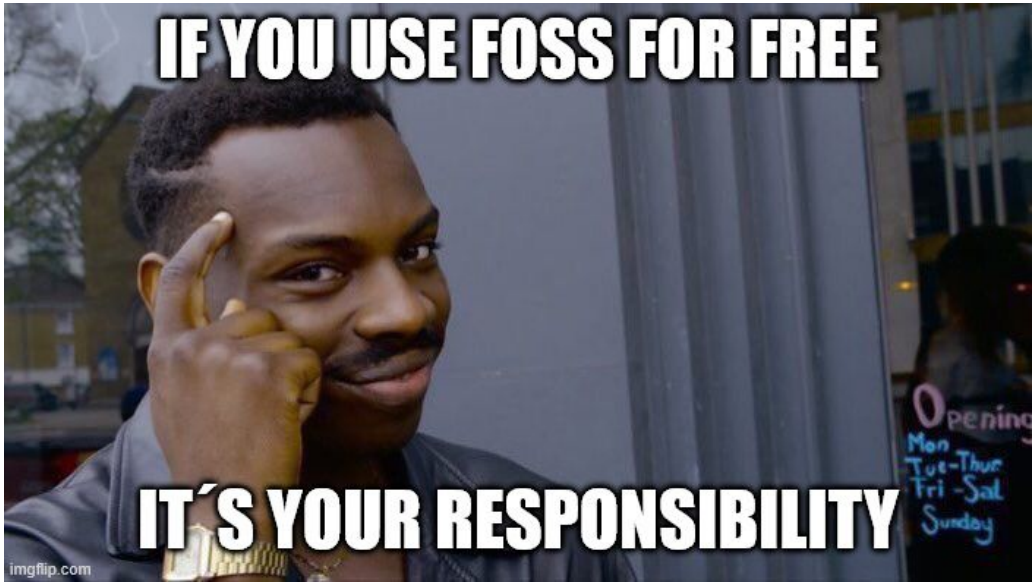




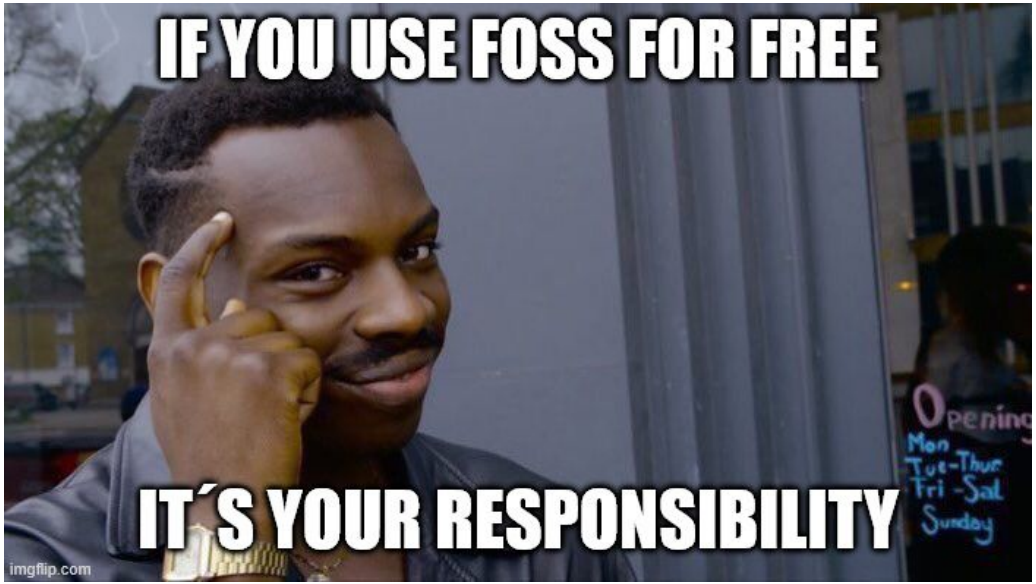




What are products with digital components? Art. 13(5)



What are products with digital components? Art. 13(5)



Art 13 (5)

manufacturers shall exercise due diligence when integrating components sourced from third parties [...], including when integrating components of free and open-source software

The five pillars of products with digital elements

Regulation & Standards

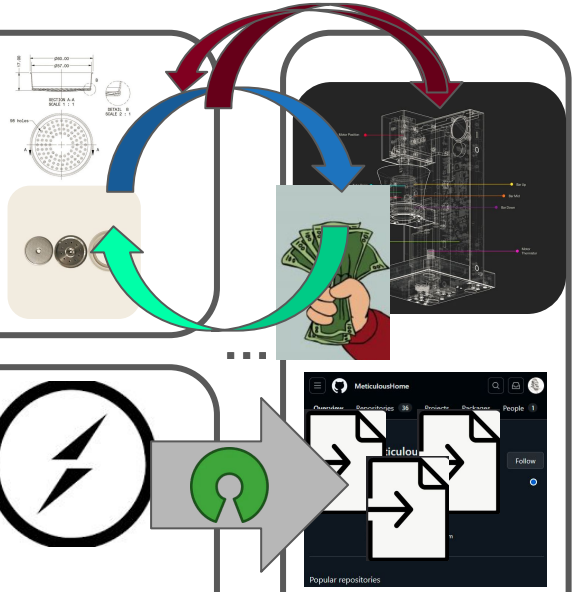
Component

Manufacturer

Assembly

Product

§§§







tekom EUROPE

CRA

CYBER MANUAL MOVEMENT

Art 13(5)

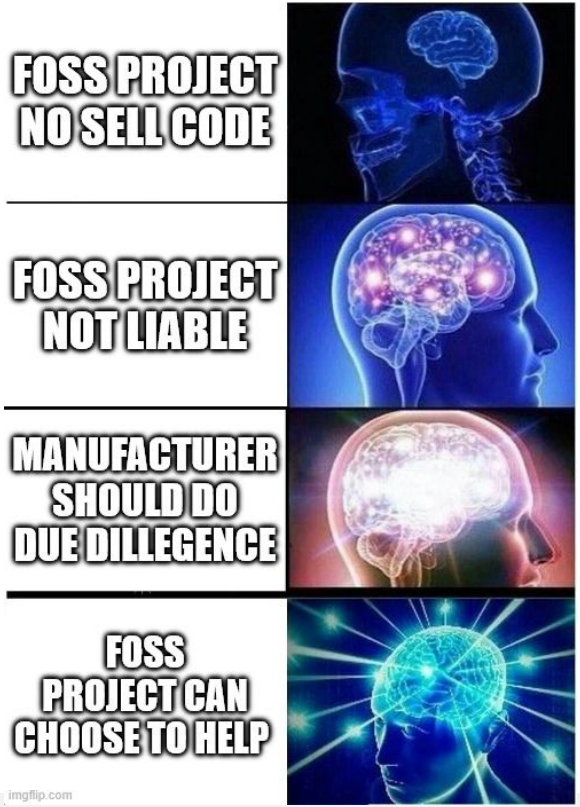
CYBER MANUAL MOVEMENT

CYBER MANUAL MOVEMENT

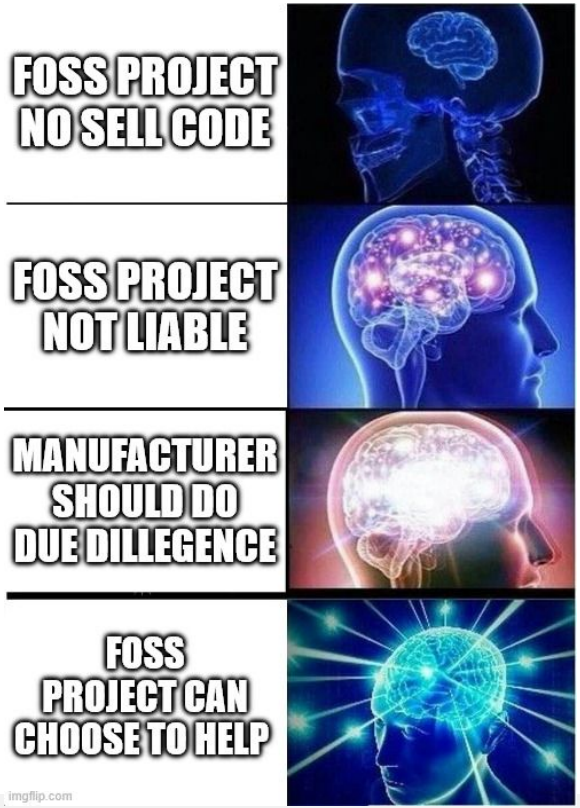
Manufactureres in 2027



What are products with digital components? Art.25



What are products with digital components? Art.25



Art 25

In order to facilitate the due diligence obligation set out in Article 13(5), in particular as regards manufacturers that integrate free and open-source software components in their products with digital elements, [...]

establishing voluntary security attestation programmes allowing the developers [...of ...] free and open-source software [...]

to assess the conformity [...] with all or certain essential cybersecurity requirements

The five pillars of products with digital elements

Regulation & Standards

Component

Manufacturer

Assembly

Product

§§§

tekom EUROPE

CE

IETF

WORLD WIDE WEB CONSORTIUM

CRA

Art 25

CYBER MANUAL MOVEMENT

Art 13(5)

CYBER MANUAL MOVEMENT

CYBER MANUAL MOVEMENT

The five pillars of products with digital elements

Regulation & Standards

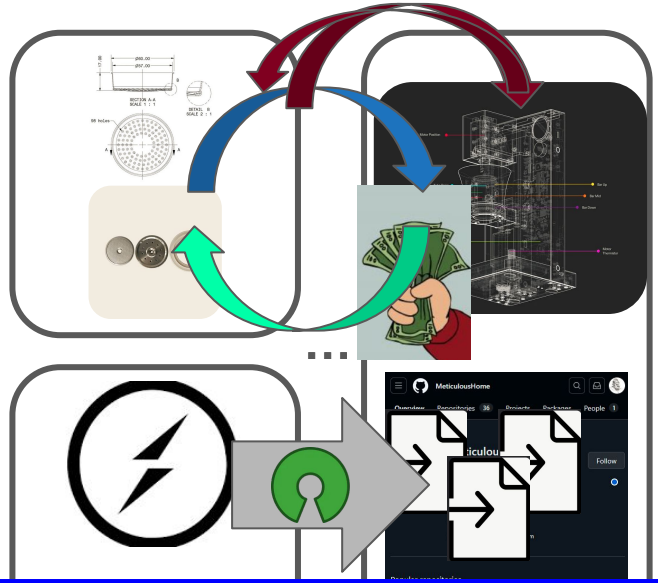
Component

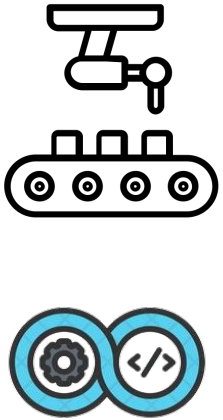
Manufacturer

Assembly

Product











§§§

tekom EUROPE

CRA

Art 25

CYBER MANUAL MOVEMENT

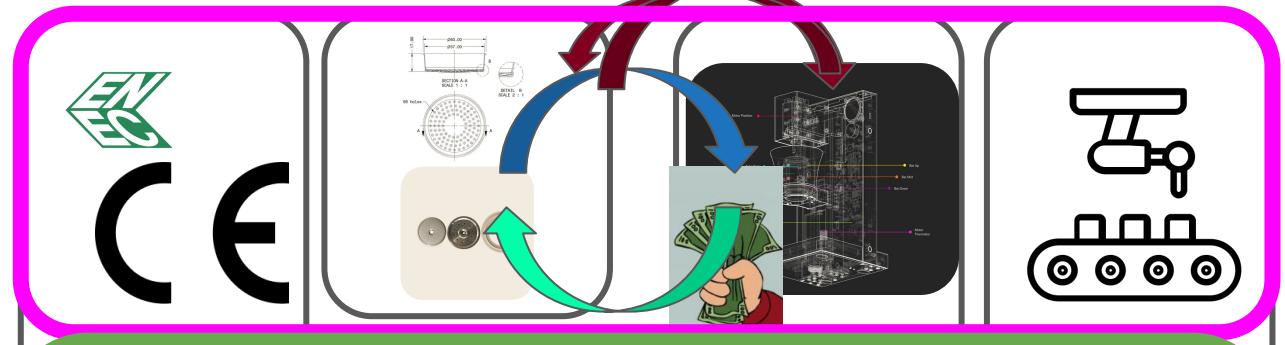
Art 13(5)

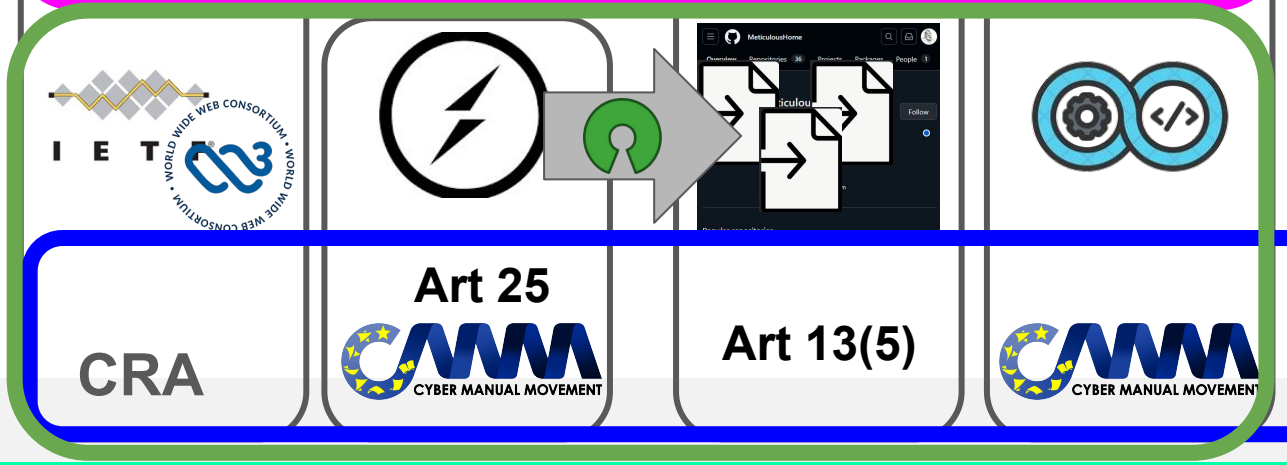
CYBER MANUAL MOVEMENT

CYBER MANUAL MOVEMENT

Classical vs. digital supply chains - what's the difference

Regulation & Standards | Component | Manufacturer | Assembly | Product







Classical vs. digital supply chains - what's the difference - technical

- **Distinguishability**
  Classical components are distinct physical objects, if one ist defect the other is not necessarily. This is not true for vulnerabilities in code.

Classical vs. digital supply chains - whats the difference - technical

- **Distinguishability**
  Classical components are distinct physical objects, if one ist defect the other is not necessarily. This is not true for vulnerabilities in code.
- **Scaling**
  Economies of scale exist for classical components but properly set-up digital solutions scale with negligible costs.

Classical vs. digital supply chains - what's the difference - technical

- **Distinguishability**
  Classical components are distinct physical objects, if one is defect the other is not necessarily. This is not true for vulnerabilities in code.
- **Scaling**
  Economies of scale exist for classical components but properly set-up digital solutions scale with negligible costs.
- **Code Rot**
  Due to the constant evolution of their ecosystem digital solutions deteriorate in usefulness quickly.

Classical vs. digital supply chains - what's the difference - technical

- **Distinguishability**
  Classical components are distinct physical objects, if one is defect the other is not necessarily. This is not true for vulnerabilities in code.
- **Scaling**
  Economies of scale exist for classical components but properly set-up digital solutions scale with negligible costs.
- **Code Rot**
  Due to the constant evolution of their ecosystem digital solutions deteriorate in usefulness quickly.
- **Scaling properties**
  For classical components relevant properties of the system can be deduced from the components. Technical documentation allows for risk and responsibility allocation and thus legal frames that cover risks.

Classical vs. digital supply chains - what's the difference - non tech

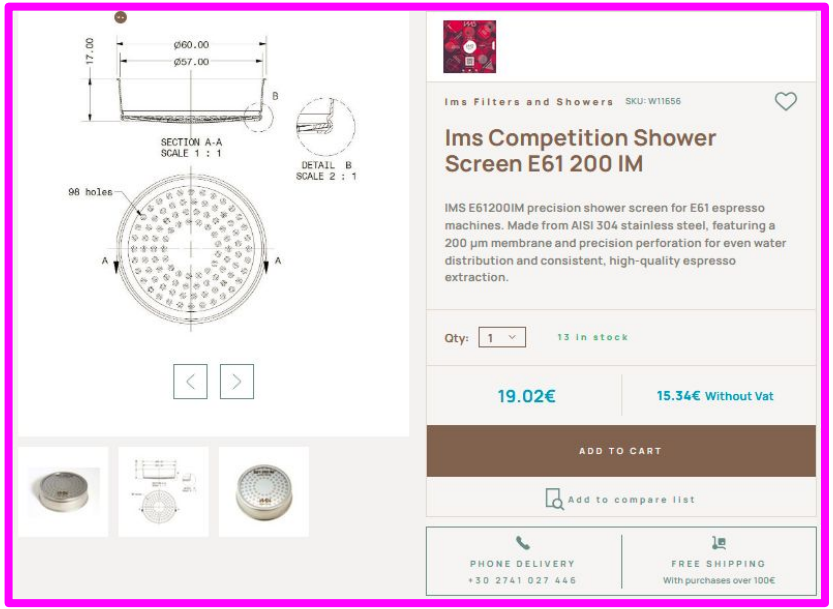
- Legal person: S.P.A. vs. not incorporated

Classical vs. digital supply chains - what's the difference - non tech

- **Legal person:** S.P.A. vs. not incorporated
- **Documentation & Accountability**

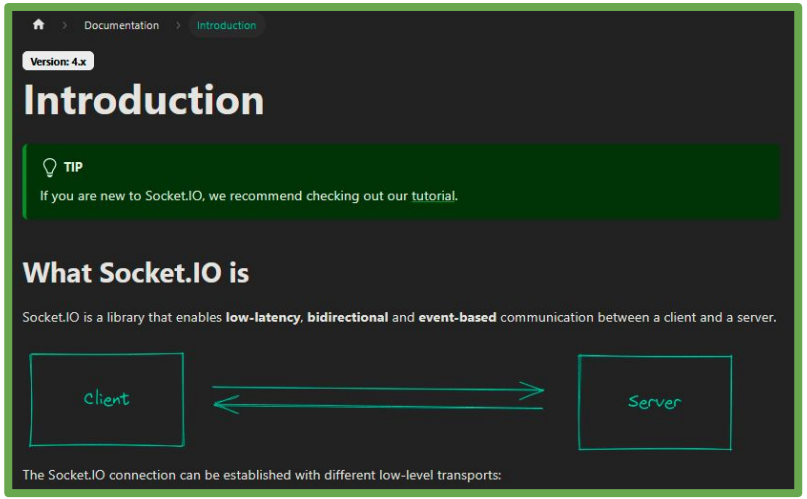
Classical vs. digital supply chains - what's the difference - non tech

- **Documentation:**



≠

MIT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY



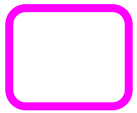
What do those three items have in common? Subject to the CRA



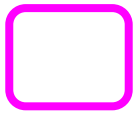
The manufacturer's instructions suggest that the product can be installed with two wires under a screw terminal. This may cause sparking and lead to a fire.

formerly known as **RAPEX**

Classical vs. digital supply chains - what's the difference - non tech

- **Legal person:**  S.P.A. vs.  not incorporated
- **Documentation & Accountability:**
  
  
  - **Customer protection rights apply, e.g. exchange policy**
  - **Accountability is partially based on technical documentation**
  - **Software is provided "as is", without warranty.**
  - **Technical documentation sparse and not legally relevant**

Classical vs. digital supply chains - what's the difference - non tech

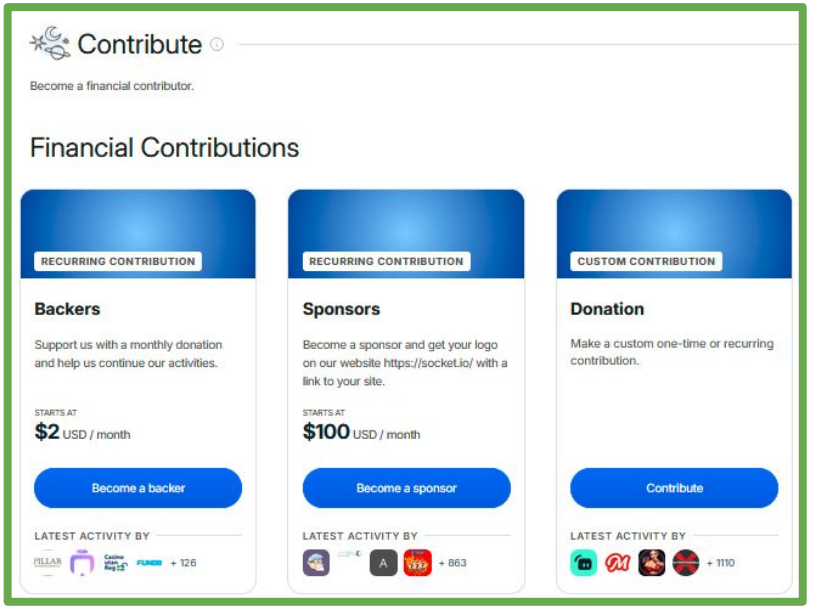
- **Legal person:**  S.P.A. vs.  not incorporated
- **Documentation & Accountability:**
  - 
  - 
  - Customer protection rights apply, e.g. exchange policy
  - Accountability is partially based on technical documentation
  - Software is provided "as is", without warranty.
  - Technical documentation sparse and not legally relevant
- **Business model**

Classical vs digital supply chains - what's the difference - non tech

- **Business model:**



≠

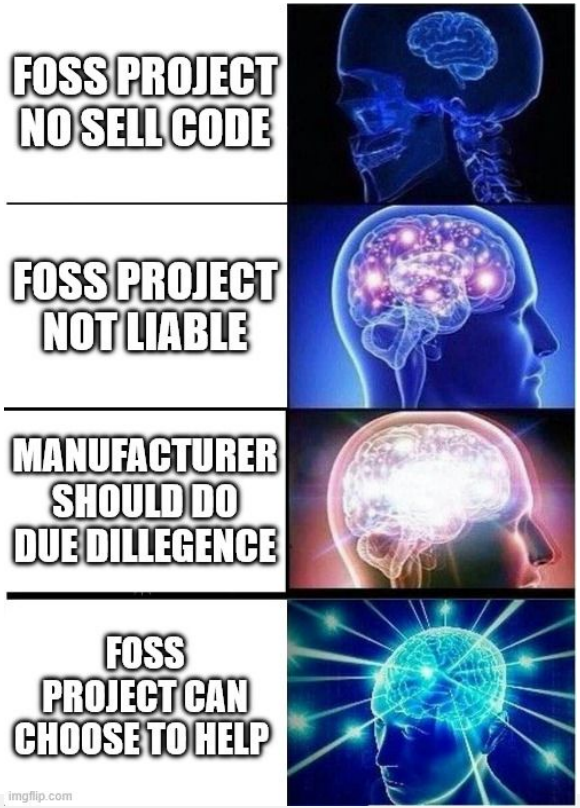


Classical vs. digital supply chains - what's the difference - non tech

- **Legal person:** S.P.A. vs. not incorporated
- **Documentation & Accountability:**
  - Customer protection rights apply, e.g. exchange policy
  - Accountability is partially based on technical documentation
  - Software is provided "as is", without warranty.
  - Technical documentation sparse and not legally relevant
- **Financing**
  - **No money, no product**
  - **Pls, pretty pls, donate to our financial host**

Why public benefit stewards for digital commons?

Why public benefit stewards / 501 (c)3s for digital commons?



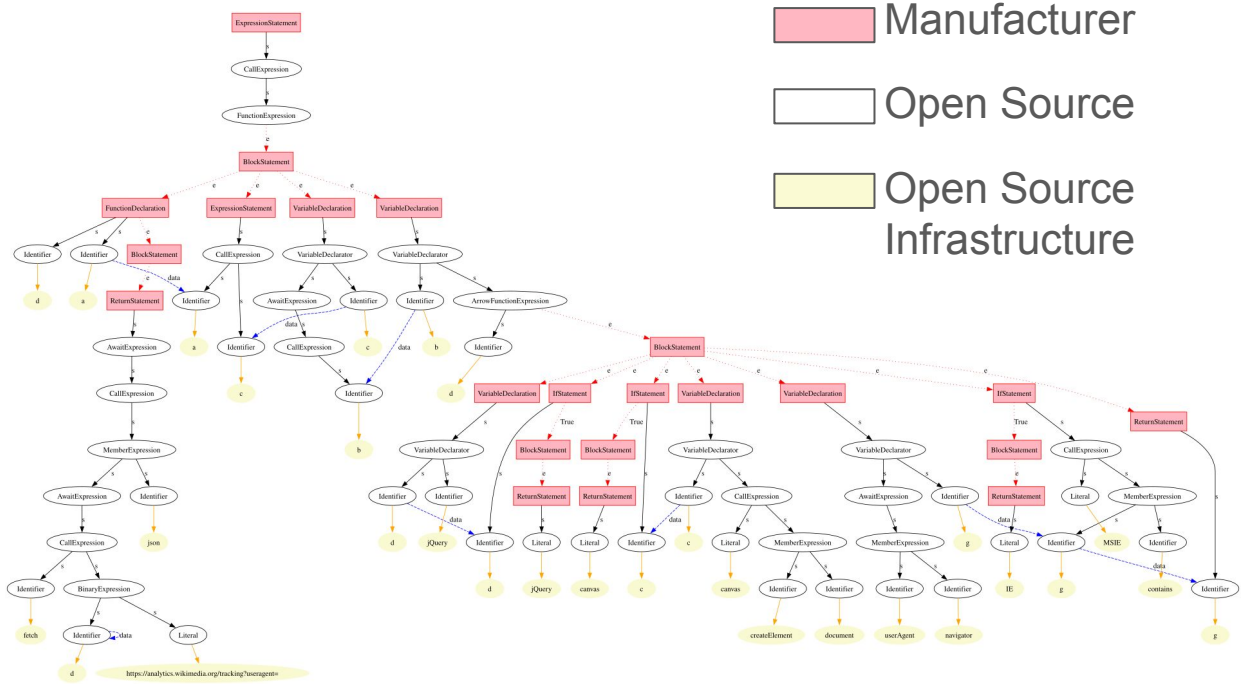
Art 25

*In order to **facilitate the due diligence obligation set out in Article 13(5),** in particular as regards manufacturers that integrate free and open-source software components in their products with digital elements, [...]*

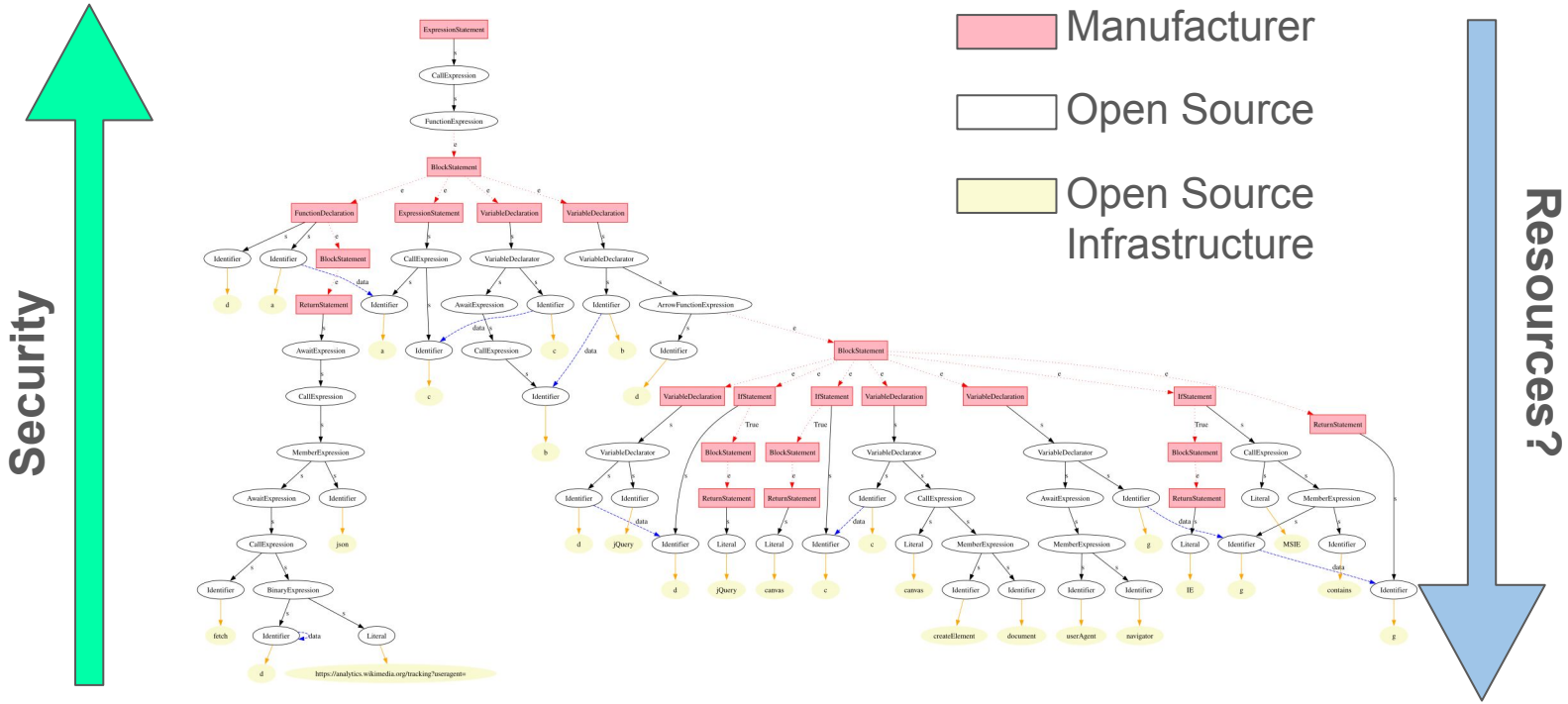
establishing voluntary security attestation programmes allowing the developers [...of ...] free and open-source software [...]

to assess the conformity [...] with all or certain essential cybersecurity requirements

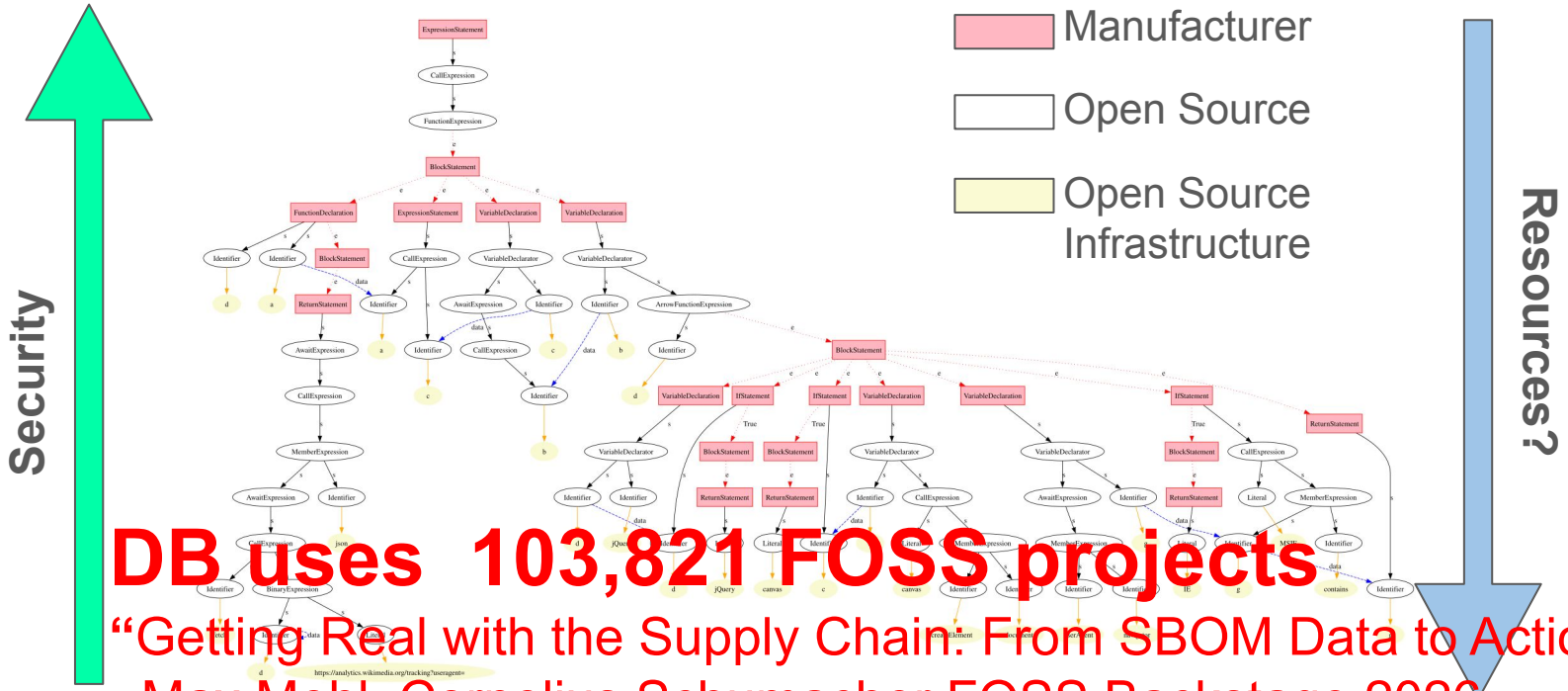
Why public benefit stewards / 501 (c)3s for digital commons?



Why public benefit stewards / 501 (c)3s for digital commons?



Why public benefit stewards / 501 (c)3s for digital commons?



DB uses 103,821 FOSS projects

"Getting Real with the Supply Chain: From SBOM Data to Action"
- Max Mehl, Cornelius Schumacher FOSS Backstage 2026

Why public benefit stewards / 501 (c)3s for digital commons?

Manufacturers (13)

- Natural or legal persons
- Develops or manufacture
  Products with digital elements
- Markets them for:
  - Payment
  - Monetisation
  - Free of charge

Why public benefit stewards / 501 (c)3s for digital commons?

Manufacturers (13)

- Natural or legal persons
- Develops or manufacture Products with digital elements
- Markets them for:
  - Payment
  - Monetisation
  - Free of charge

Open Source Software Stewards (14)

- Legal person other than a manufacturer
- Systematically provide support Free and open source software
- Markets them for:
  - ~~Payment~~
  - ~~Monetisation~~
  - Free of charge

Why public benefit stewards / 501 (c)3s for digital commons?

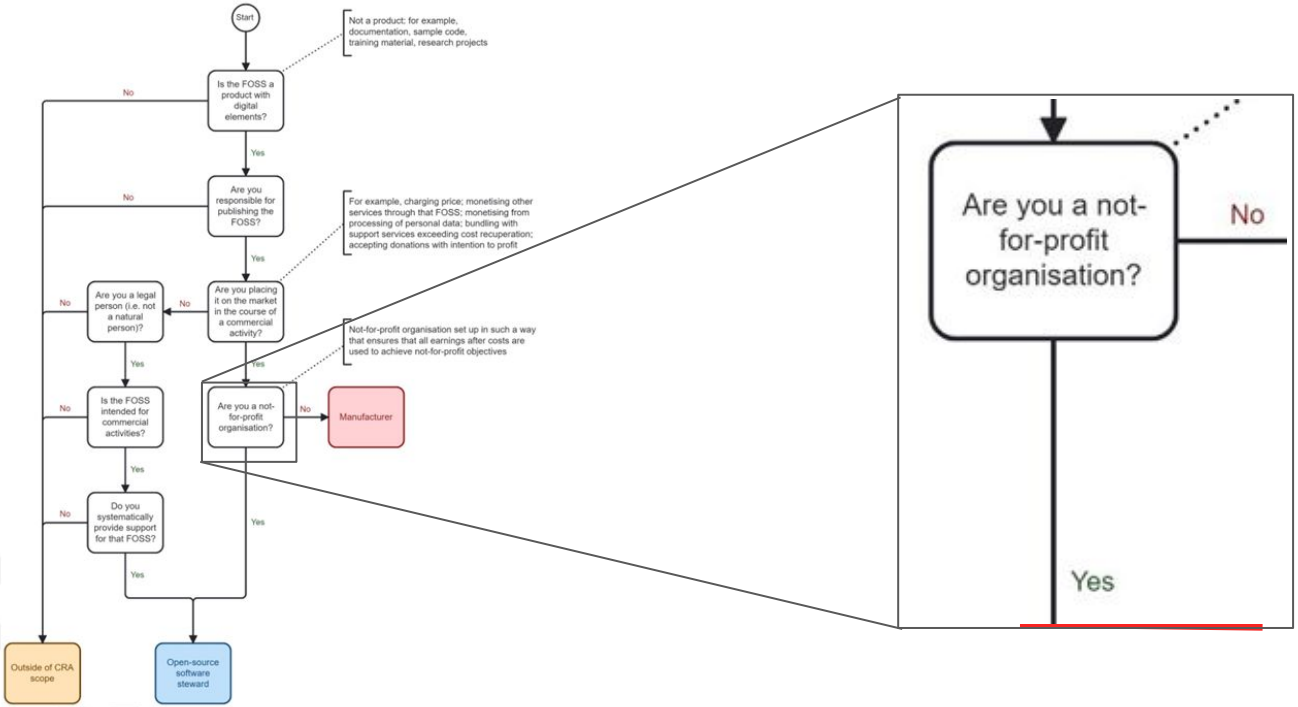


Figure 1: Stylised flowchart for CRA coverage of free and open-source software

Why public benefit stewards / 501 (c)3s for digital commons?

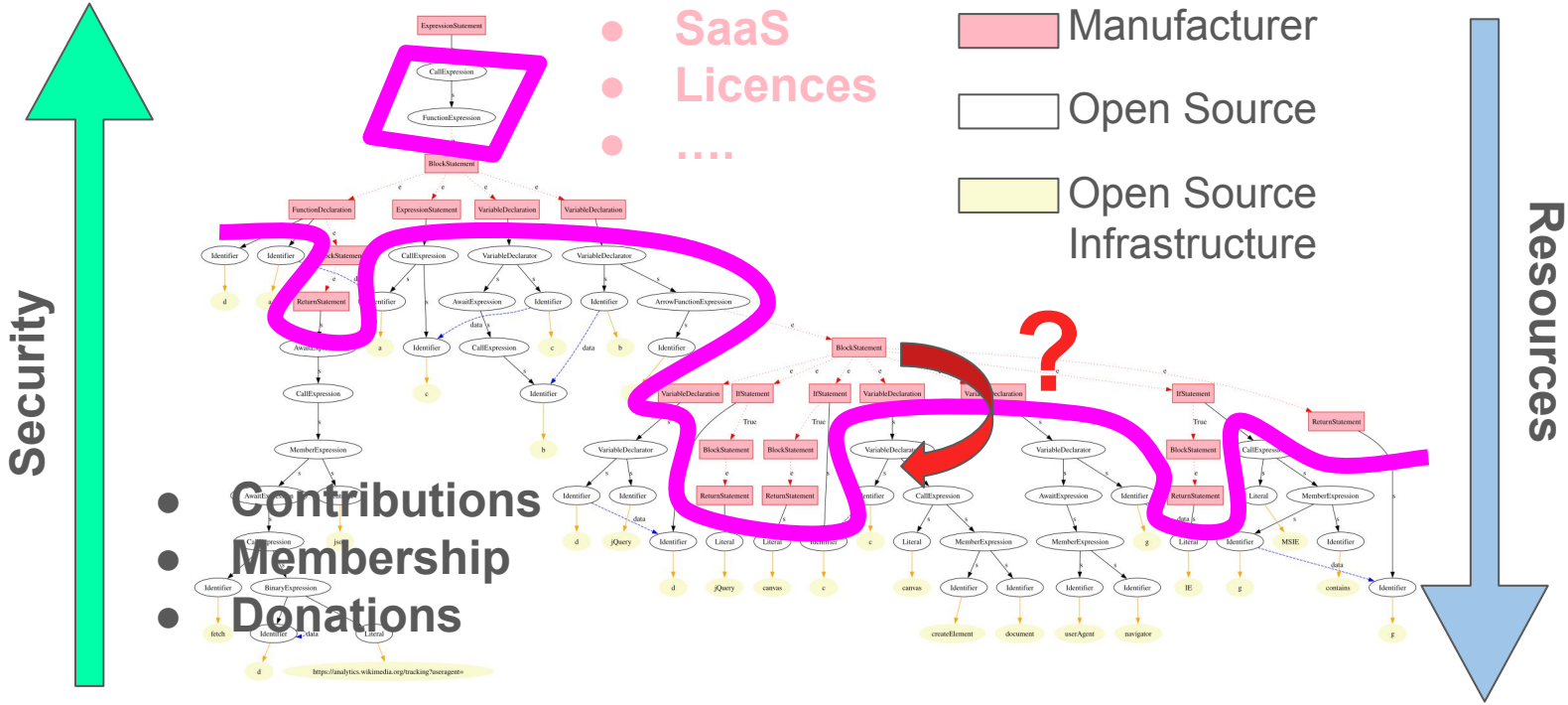
Manufacturers (13)

- Natural or legal persons
- Develops or manufacture Products with digital elements
- Markets them for:
  - Payment
  - Monetisation
  - Free of charge

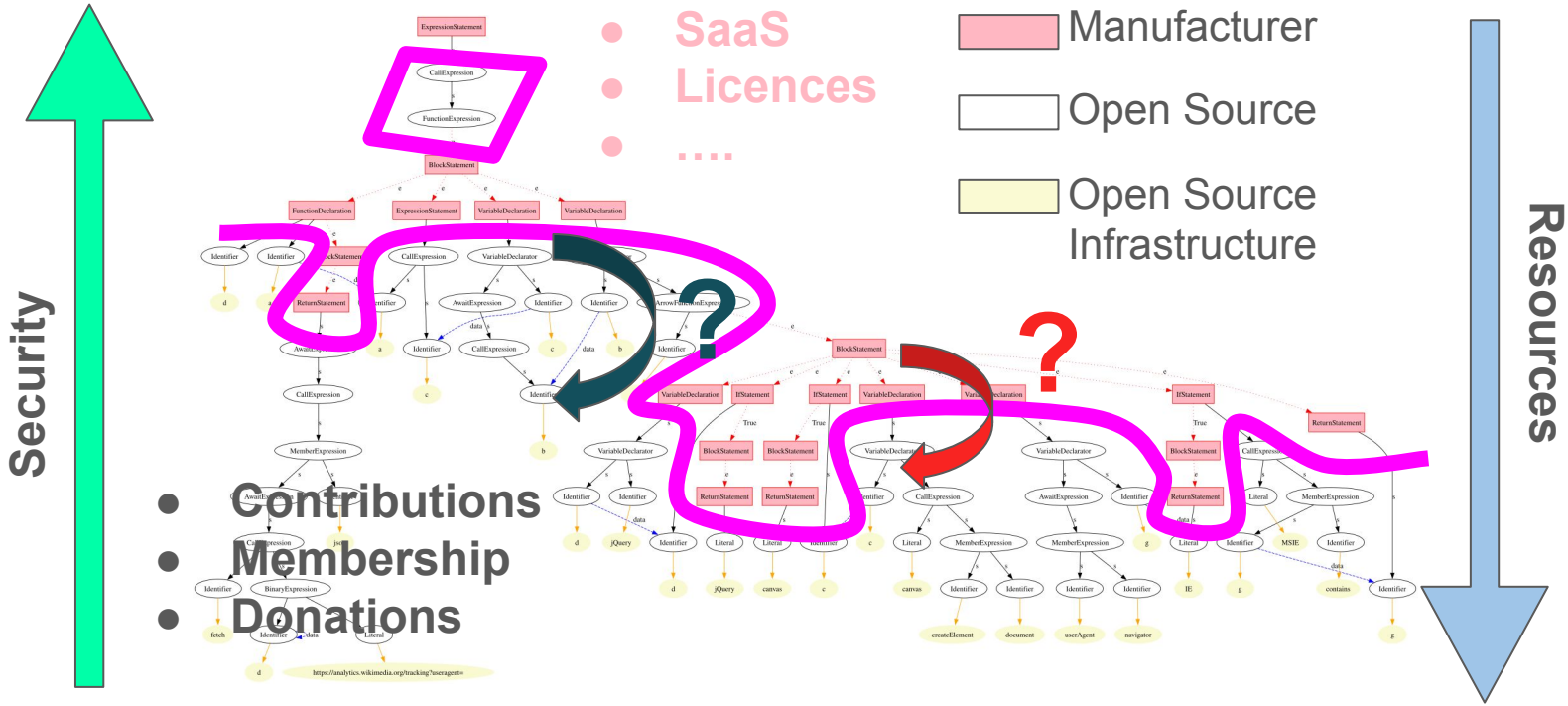
Open Source Software Stewards (14)

- Legal person other than a manufacturer
- Systematically provide support Free and open source software
- Markets them for:
  - Contribution
  - Membership
  - Donations
  - Condition: Reasonable Living Expensens

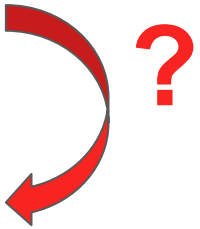
Why public benefit stewards / 501 (c)3s for digital commons?



Why public benefit stewards / 501 (c)3s for digital commons?



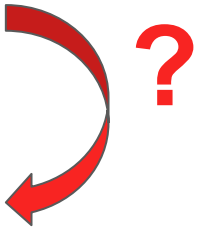
Why public benefit stewards / 501 (c)3s for digital commons?





- Best Practice: Contributions upstream stuff
  - SME Have your engineers commit
  - Cooperate: Have an OSPO

Why public benefit stewards / 501 (c)3s for digital commons?

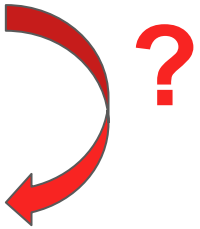


- Best Practice: Contributions upstream stuff
  - SME Have your engineers commit
  - Cooperate: Have an OSPO



- Challenges for contributions - it does not scale
  - I bet Open Source Companies do not Upstream to EVERY project they use
  - Open Source projects are picky whom they wanna work with
  - There are non-software companies they still wanna use software

Why public benefit stewards / 501 (c)3s for digital commons?

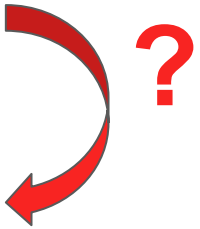


- Best Practice: Contributions upstream stuff
  - SME Have your engineers commit
  - Cooperate: Have an OSPO



- Challenges for contributions/memberships - it does not scale
  - I bet Open Source Companies do not Upstream to EVERY project they use
  - Open Source projects are picky whom they wanna work with
  - There are non-software companies they still wanna use software

Why public benefit stewards / 501 (c)3s for digital commons?





- Best Practice: Contributions upstream stuff
  - SME Have your engineers commit
  - Cooperate: Have an OSPO
- Challenges for contributions/memberships - it does not scale
  - I bet Open Source Companies do not Upstream to EVERY project they use
  - Open Source projects are picky whom they wanna work with
  - There are non-software companies they still wanna use software
- Legal accountability towards 3rd parties?

Why public benefit stewards / 501 (c)3s for digital commons?



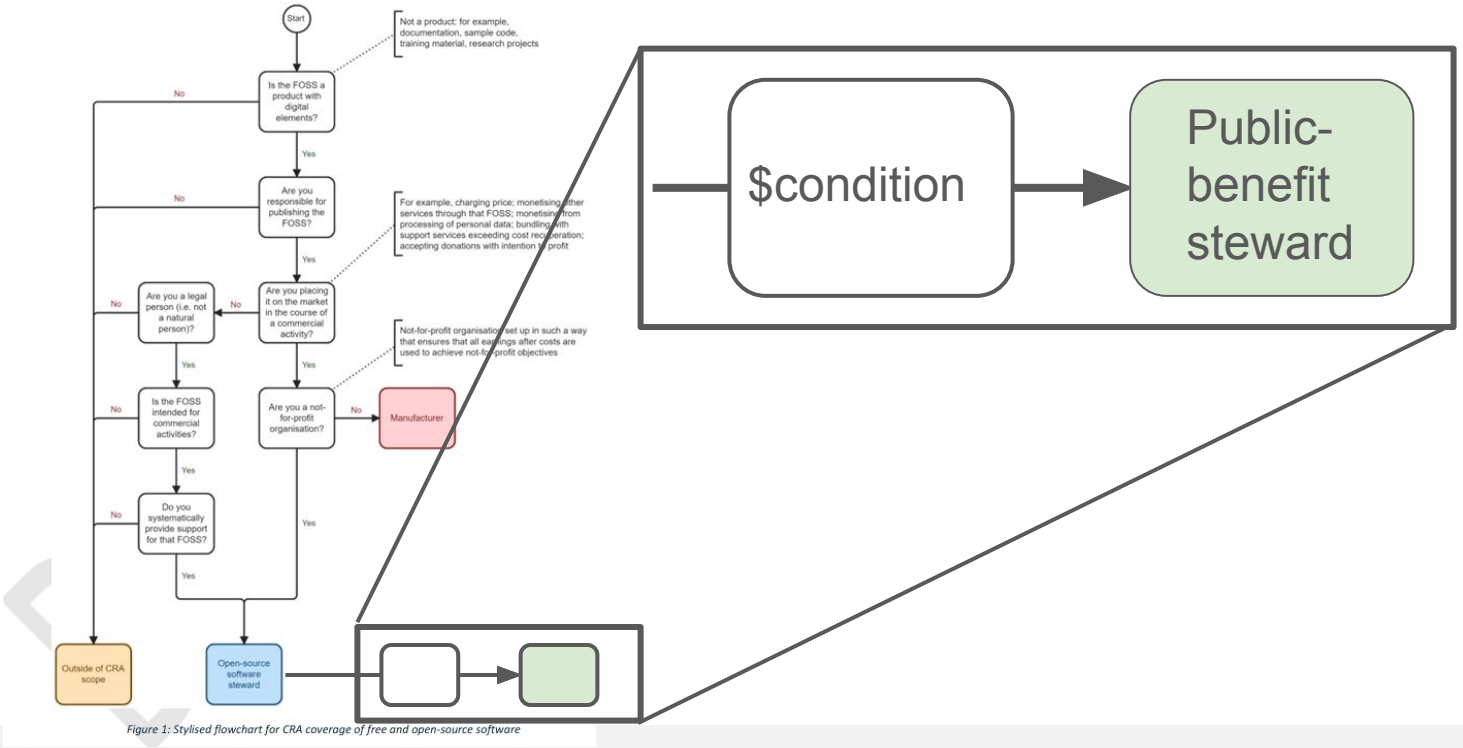


Figure 1: Stylised flowchart for CRA coverage of free and open-source software

Digression: not-for-profit vs. public benefit



not-for-profit

- Accountable to:
  - Stakeholders
  - Members

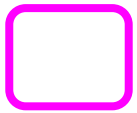
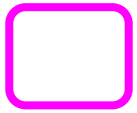
- Allows for collaboration to the limit of antitrust law
- Can become neither a standards nor verification body

public - benefit

- Accountable to:
  - Stakeholders
  - Members
  - Oversight by tax-offices

- Limited to public benefit & General interest activities,
- Donations bound to cause.
- Best-practice when it comes to R&D, standards, verification

Why public benefit stewards / 501 (c)3s for digital commons?

- **Legal person:**  S.P.A. vs.  **incorporate as public benefit org**
- **Accountability & Documentation:**
  - 
  - Regular customer protection rights apply, exchange policy
  - Technical specification to hold accountable
  - 
  - **Article 25 Attestation, including financial health indicators**
  - **Supervision by the tax office thus no gouging of demand**
- **Financing**
  - 
  - No money, no product
  - 
  - **If the FOSS project has no sustainable financing, Art 13 (5) due-diligence is required to reduce financial risks**

Software Supply Chain Communication - The Ecosystem



Software Supply Chain Communication - The Ecosystem

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klima

Port of Rotterdam

1. **Market Surveillance Authority**

NixOS

Software Supply Chain Communication - The Ecosystem

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

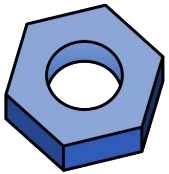
Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klima

Port of Rotterdam

1. **Market Surveillance Authority**





NixOS

2. **FOSS - Up & Downstream**

Software Supply Chain Communication - The Ecosystem

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

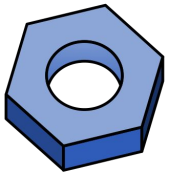
Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klima

Port of Rotterdam

1. **Market Surveillance Authority**





NixOS

SkyPilot

Determinate Systems

2. **FOSS - Up & Downstream**

3. **Dependents aka Manufacturers**

Software Supply Chain Communication - The Ecosystem

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

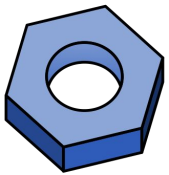
Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klima

Port of Rotterdam

1. Market Surveillance Authority





2. FOSS - Up & Downstream

NixOS

SkyPilot

Determinate Systems

3. Dependents aka Manufacturers




Codeberg

4. Your Forges

Software Supply Chain Communication - The Ecosystem

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

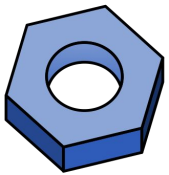
Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klima

Port of Rotterdam

1. Market Surveillance Authority





2. FOSS - Up & Downstream







3. Dependents aka Manufacturers





4. Your Forges





5. White AI Blackhats

Software Supply Chain Communication - 4 ideas

1. publish supply chain data, decentralized, globally interoperable
2. Identify compliance critical communication (c3) within the ecosystem
   a. by Market Surveillance Authorities (MSAs)
   b. by FOSS Projects Up- and Downstream
   c. by proprietary dependents

Software Supply Chain Communication - 1. idea

1. publish supply chain data, decentralized, globally interoperable



2. FOSS - Up & Downstream







3. Dependents aka Manufacturers



4. Your Forges

Software Supply Chain Communication - 1. idea

1. publish supply chain data, decentralized, globally interoperable

Standards Badges - SB

Allow FOSS projects to flag on their repositories which standards they implement



2. FOSS - Up & Downstream







3. Dependents aka Manufacturers



4. Your Forges

Software Supply Chain Communication - The Ecosystem

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klima

Port of Rotterdam

1. **Market Surveillance Authority**

NixOS

2. Identify compliance critical communication (c3)
    a. with Market Surveillance Authorities (MSAs)

Software Supply Chain Communication - The Ecosystem

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klima

Port of Rotterdam

1. **Market Surveillance Authority**

NixOS

2. Identify compliance critical communication (c3)
   a. with Market Surveillance Authorities

MSAs should have a PKI

Software Supply Chain Communication - The Ecosystem



2. FOSS - Up & Downstream





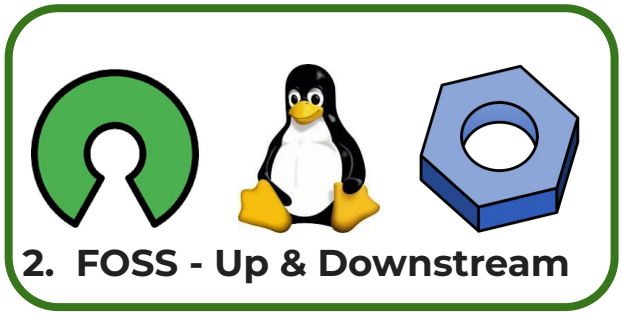
4. Your Forges

2. Identify compliance critical communication (c3)
b. by FOSS Projects Up- and Downstream

Software Supply Chain Communication - The Ecosystem

I) Write message

I)



NixOS

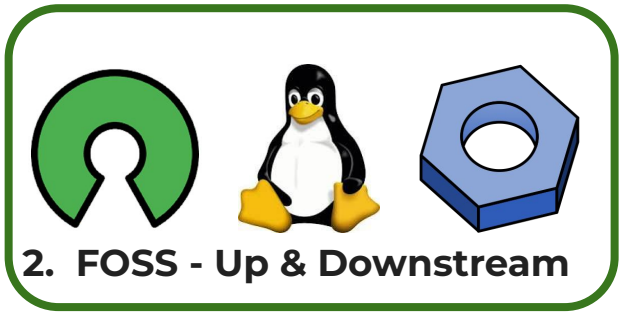


2. Identify compliance critical communication (c3)
b. by FOSS Projects Up- and Downstream

Software Supply Chain Communication - The Ecosystem

I) Write message
II) Publish hash of message with forge account

I) II)



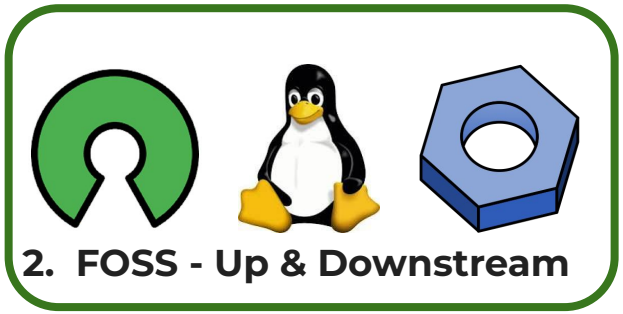
NixOS



2. Identify compliance critical communication (c3)
b. by FOSS Projects Up- and Downstream

Software Supply Chain Communication - The Ecosystem

I) II) III)



NixOS

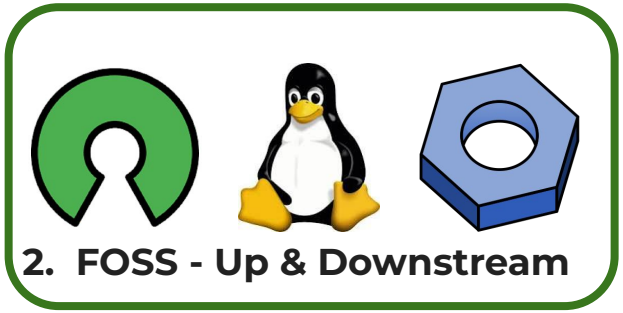
I) Write message
II) Publish hash of message with forge account
III) Send mail to security@ with pointer to hash



2. Identify compliance critical communication (c3)
b. by FOSS Projects Up- and Downstream

Software Supply Chain Communication - The Ecosystem

I) II) III)



IV)



I) Write message
II) Publish hash of message with forge account
III) Send mail to security@ with pointer to hash
IV) Run centrality measure on forge account of sender



2. Identify compliance critical communication (c3)
b. by FOSS Projects Up- and Downstream

Software Supply Chain Communication - The Ecosystem

I) Use Package

I)







3. Dependents aka Manufacturers

2. Identify compliance critical communication (c3)
   c. by proprietary dependents







4. Your Forges

Software Supply Chain Communication - The Ecosystem

I) Use Package
II) get receipts of properties of package (receipts has UID)

I) II)







3. Dependents aka Manufacturers







4. Your Forges

2. Identify compliance critical communication (c3)
   c. by proprietary dependents

Software Supply Chain Communication - The Ecosystem

I) Use Package
II) get receipts of properties of package (receipts has UID)
III) send donation with UID

I) II) III)







3. Dependents aka Manufacturers







4. Your Forges

2. Identify compliance critical communication (c3)
   c. by proprietary dependents

Software Supply Chain Communication - The Ecosystem

I) Use Package
II) get receipts of properties of package (receipts has UID)
III) send donation with UID
IV) send c3 with list of UIDs



I) II) III) IV)





3. Dependents aka Manufacturers

2. Identify compliance critical communication (c3)
   c. by proprietary dependents







4. Your Forges

Software Supply Chain Communication - The Ecosystem

I) Use Package
II) get receipts of properties of package (receipts has UID)
III) send donation with UID
IV) send c3 with list of UIDs
V) Asses validity by UIDs

V)

NixOS

I) II) III) IV)

SkyPilot

Determinate Systems

3. Dependents aka Manufacturers

2. Identify compliance critical communication (c3)
   c. by proprietary dependents

Codeberg

4. Your Forges

Software Supply Chain Communication - The Ecosystem

I) Use Package
II) get receipts of properties of package (receipts has UID)
III) send donation with UID
IV) send c3 with list of UIDs
V) Asses validity by UIDs

V)



I) II) III) IV)





3. Dependents aka Manufacturers

2. Identify compliance critical communication (c3)
   c. by proprietary dependents







4. Your Forges

In scope - technical specs

1. Security and privacy guardrails for all stakeholders
2. Technical Soundness
3. Applicability

Out of scope - Interference with governance

1. Interference with the governance of FOSS Projects, thus:
    a. Free choice of regulation to be adhered
    b. Free choice of revealed information
    c. Free choice of payment channels
    d. Free choice of centrality measures
    e. dataformats for payload content
    f. etc. etc.
2. Create obstacles for
    a. business innovation
    b. market creation

Open Questions - Caveats

1. Trust is a social question. Technology can help, not answer it.
2. Malicious fixes - downstream targets
3. Fraud
4. Impersonation and relay attacks
5. Open Source Software Stewards - a vehicle for money laundering?
6. What did we miss?

Current state of project

1. Since 2024: Constant Exchange with the Erlang Ecosystem Foundation
2. 24 July 2026: Concepts presented at Supply Chain Integrity and Trust (SCITT) @IETF126
   a. Talk (5min): https://youtu.be/zvTPgr0bh5Q?t=3444
   b. Slides:https://datatracker.ietf.org/meeting/126/materials/slides-126-sc[illegible]nna-scitt-04#page=52

   → Adoption for future work
3. 13 Oct. 26: Community over Code - Apache Foundation:
   → BoF FOSS SUITE - this room in 10 min
4. 28 Oct. 26: Code & Compliance - Eclipse Foundation - Brussels
   → Meet the Orcs



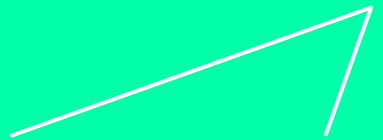
Summary

- Products with digital elements - a supply chain perspective
  - There two supply chain around different kinds of technologies
- Classical vs. digital supply chains - what´s the difference?
  - There is not yet technical documentation for FOSS
- Why public benefit stewards / 501 (c)3s for digital commons?
  - FOSS stewards would be reliable suppliers to various dependents
  - FSCT could allow for funding of basic needs of FOSS projects
- rfc: supply chain centered communication
  - Volunteers for standards wanted
  - See you at the BoF?
  - See you in Brussels?
  - Stewards are not liable they don´t have to white whash their documentations

Summary: The CRA makes it mandatory, let´s make it usefull

- Products with digital elements - a supply chain perspective
  - There two supply chain around different kinds of technologies
- Classical vs. digital supply chains - what´s the difference?
  - There is not yet technical documentation for FOSS
- Why public benefit stewards / 501 (c)3s for digital commons?
  - FOSS stewards would be reliable suppliers to various dependents
  - FSCT could allow for funding of basic needs of FOSS projects
- rfc: supply chain centered communication
  - Volunteers for standards wanted
  - See you at the BoF?
  - See you in Brussels?
  - Stewards are not liable they don´t have to white whash their documentations

Looking forward to the discussion - What is missing?



© Innovationsverbund Öffentliche Gesundheit 2021

Current state of project

1. Timeless: Erlang Ecosystem Foundation interested
2. 24 July 2026: Concepts presented at Supply Chain Integrity and Trust (SCITT) @IETF126
   a. Talk (5min): https://youtu.be/zvTPgrObh5Q?t=3444
   b. Slides:https://datatracker.ietf.org/meeting/126/materials/slides-126-scitt-ietf-126-vienna-scitt-04#page=52

   → Adoption for future work
3. 6 Oct. 26: OpenSSF Community days

   → ORBIT WG discusses holding workshop of integration of security insights.
4. 12 Oct. 26: Community over Code - ASF:

   → BoF FOSS SUITE

Asks

1. Did we miss relevant connections to the CRA or guidance



Asks

1. Did we miss relevant connections to the CRA or guidance
2. Are you familiar with:
   a. EO 14028
   b. SSDF
   c. SEC Cyber Rule
   d. SLSA
   e. NTIA
   f. other regulation ..
      or compliance tooling?



Asks

1. Did we miss relevant connections to the CRA or guidance
2. Are you familiar with:
   a. EO 14028
   b. SSDF
   c. SEC Cyber Rule
   d. SLSA
   e. NTIA
   f. other regulation ..
      or compliance tooling?
3. How to put badges on repositories?



Asks

1. Did we miss relevant connections to the CRA or guidance
2. Are you familiar with:
   a. EO 14028
   b. SSDF
   c. SEC Cyber Rule
   d. SLSA
   e. NTIA
   f. other regulation ..
      or compliance tooling?
3. How to put badges on repositories?
4. How to identify AI hats?





Open Policy Question: How to tax Open Source Software Stewards?



