The evolving relationship between open source software and standards development in the EU

16 April 2024

Mirko Boehm

THE LINUX FOUNDATION | Europe

mirko@LF: > whoami

Free and Open Source Software contributor.

Senior Director, Community Development, Linux Foundation Europe.

Open Source contributor since 1997.

Visiting lecturer and researcher at the Technical University of Berlin.

Openforum Academy fellow.

Berlin, Germany.

mirko@linuxfoundation.eu

mirko@LF: > whoarewe

As the European chapter of the Linux Foundation, LF Europe:

- Grows regional opportunities for our participants to contribute to LF's global collaboration,
- Amplifies the reach of LF projects in the European ecosystem, and
- Represents LF and its Members in European policy making, standards development and R&D funding programs

The EU regulatory aspiration

€65-95B

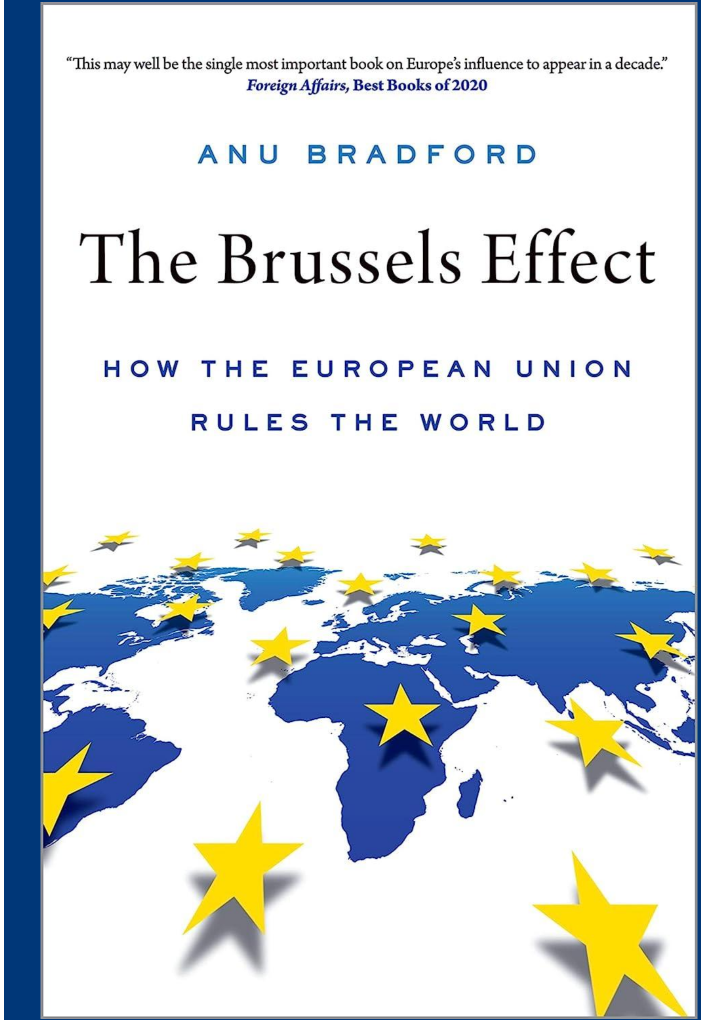
... Open source software contributes between €65 to €95 billion to the European Union's GDP and promises significant growth opportunities for the region's digital economy.

Open source communities are an integral part of the ICT sector and require careful regulation.

SMEs are the backbone of open source success in Europe.

THE LINUX FOUNDATION | Europe

“With great power comes great responsibility."



“This may well be the single most important book on Europe’s influence to appear in a decade.”
Foreign Affairs, **Best Books of 2020**

ANU BRADFORD

The Brussels Effect

HOW THE EUROPEAN UNION RULES THE WORLD

THE LINUX FOUNDATION | Europe

CRA

PLD

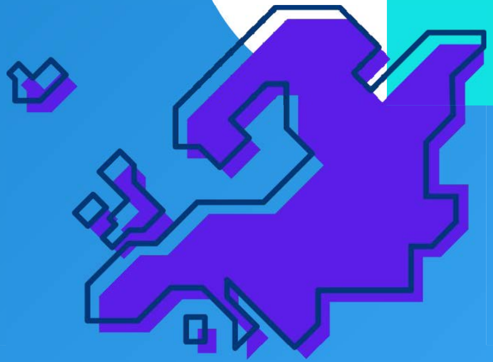
SEP

AI

Data

eIDAS

Few exceptions for Open Source



- The open source commons, as an integral part of the ICT ecosystem, is unlikely to remain unregulated.
- Instead, the trend is towards a principled approach that provides suitable mechanisms for regulating digital products.

Case Study:
The EU Cyber Resilience Act

EU Cyber Resilience Act

The EU acts to strengthen the approach to cybersecurity regulation at union level. The CRA aims to achieve 3 policy goals:

- To reduce vulnerabilities in digital products,
- To ensure cybersecurity is maintained throughout a product's life cycle and
- To enable users to make informed decisions when selecting and operating digital products

The CRA establishes horizontal mandatory cyber-security requirements for all digital products, software and/or hardware.

The EU intends to play a leading international role in cybersecurity regulation.

Essential cybersecurity requirements: Cascade

- Manufacturers should develop *all* digital products according to the essential CRA requirements,
  - since less critical devices may serve as a springboard for security attacks.
- Stricter requirements are applied to devices targeted at vulnerable consumers (like children’s toys),
- Even stricter regime to devices where exploits can cause wider damage (network routers, operating systems).

Essential cybersecurity requirements: Basics

Products shall

- Be designed and developed in accordance with essential requirements
- Be made available on the market without known exploitable vulnerabilities,
- Be made available on the market with a secure by default configuration
- Be designed so that vulnerabilities can be addressed through security updates
- Ensure protection from unauthorised access,

…and more.

Essential cybersecurity requirements: Boundaries

- Member states cannot impose additional cyber-security requirements on market access.
- They may however define additional rules for the operation of devices in specific fields within the scope of union law.
- National security remains the responsibility of the member states, they may
    - impose additional requirements for defence
    - or national security purposes.
- More specific regulations may take precedence (medical devices, radio equipment), however EU "should harmonise" as they are updated.

Commercial products with OSS components

- Provision of OSS products that are not monetised is not considered a commercial activity (18)
- Development by non-profit organizations is not considered a commercial activity (19)
- Manufacturers should exercise due diligence when integrating OSS (34)
- Upstream and manufacturers may apply voluntary security attestation programmes to support due diligence

Result: Two separate operator roles, manufacturers and open source software stewards

Manufacturers and OSS stewards

Manufacturer: full range of obligations

…means any natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under his or her name or trademark, whether for payment, monetisation or free of charge

(Article 3(13))

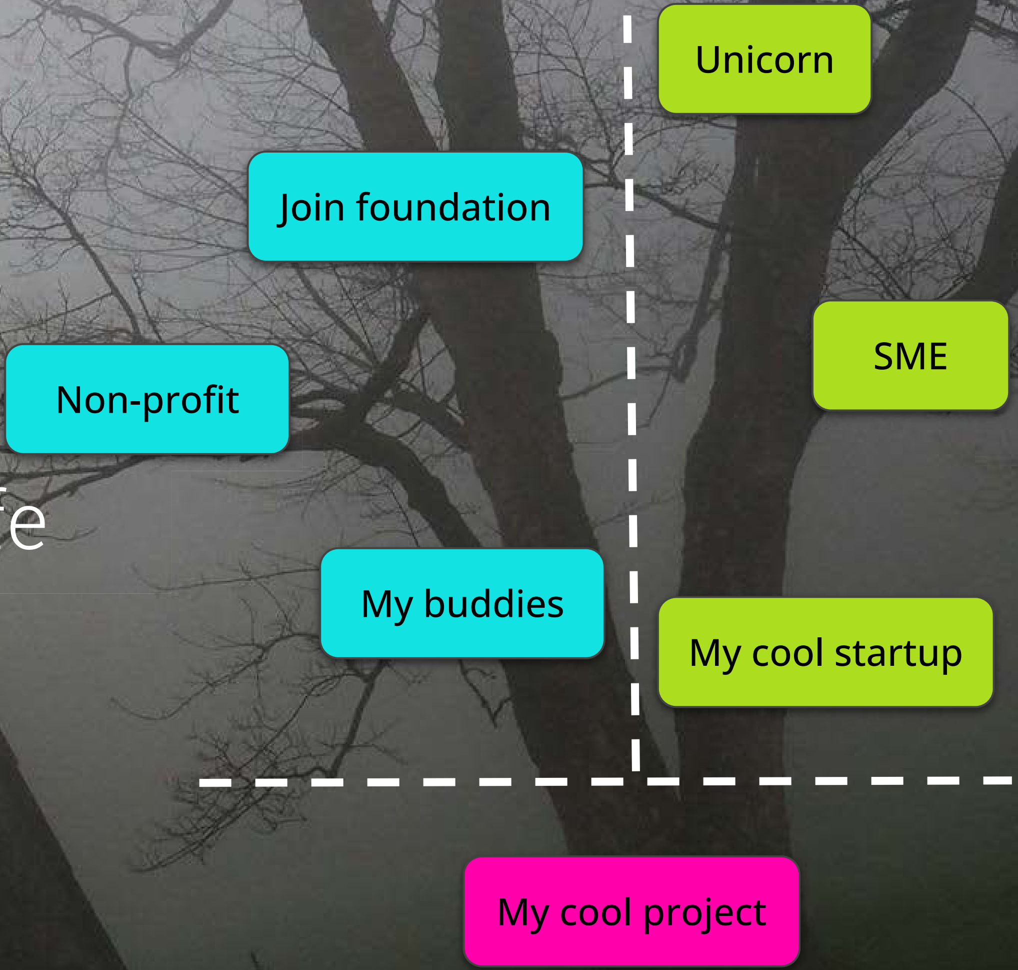
Open source software steward: light-touch regulatory regime

…means any legal person, other than a manufacturer, which has the purpose or objective to systematically provide support on a sustained basis for the development of specific products with digital elements qualifying as free and open-source software that are intended for commercial activities, and ensures the viability of those products

(Article 3(14))

Manufacturers versus Open Source Software Stewards

The (FOSS) Tree of Life



Unicorn

Join foundation

SME

Non-profit

My buddies

My cool startup

My cool project

Photo by m wrona on Unsplash

Individual developers and upstream contributions

- Individual developers (hobbyists, occasional contributors, as long as participation remains non-commercial) are exempt
- Contributing to projects where you don't have responsibility is exempt (the upstream project takes responsibility)
- Individual developers may be manufacturers (e.g., one-person businesses) or stewards (e.g., long-term maintainers)
- Be aware: Projects grow from ideas to large communities or businesses - hobbyists and individuals can become manufacturers or stewards

Manufacturers: Software updates, support period

- Manufacturers must supply vulnerability fixes throughout the support period
- Products should be designed to support software updates, especially for consumer products, ideally automated
- End of support must be communicated on the device without restricting the functionality available to the user
- Security updates must be provided separately from functionality updates
- Support period should be no less than 5 years
- ..., unless the product has a shorter lifetime
- ..., or more if a longer lifetime can be reasonably expected

Manufacturers: Notification and disclosure obligations

- Manufacturers should notify actively exploited vulnerabilities
- … as well as severe incidents
- via a single reporting platform to both CSIRTs and ENISA
- Information to be shared in an European vulnerability database
- Vulnerabilities discovered in good faith (intrusion tests, review) do not need to be reported
- Manufacturers may apply for brief delays, e.g. if a fix is forthcoming
- Manufacturers should establish a vulnerability disclosure policy for reporting and inquiry by consumers
- Manufacturers should draw up SBOMs but are not required to make them available to the general public

Manufacturers: Conformity and Penalties

Conformity:

- (Only) the CE marking communicates that a product complies with the CRA
- CI is considered part of the production process and subject to conformity assessment
- A regulatory sandbox will be developed where dry-run conformity assessments can be performed
- Accreditation for conformance assessment bodies to be implemented

Penalties:

“The penalties … shall be effective, proportionate and dissuasive” (Article 64):

- 5..15M€ or 1..2.5% of global turnover in prior fiscal year, whichever is higher
- Fines should be proportionate, take circumstances into account
- Possible enforcement through “representative actions for the protection of the collective interests of consumers” (125)

Community/manufacturer relationship

- The upstream project hosts open source projects under neutral governance
- Maintainers form the TSC usually as an additional role in their day job
- Contributors usually work downstream or in service businesses
- Remember: Open Source Maintainers Owe You Nothing

Photo by Daniel Funes Fuentes on Unsplash

Responsibilities of Open Source Software Stewards*

- The legal entity is the open source software steward
- Stewards should
  - Have a single point of contact for reporting and inquiring about vulnerabilities: https://www.linuxfoundation.org/security
  - Implement a cybersecurity policy and communicate it widely
  - Cooperate with market surveillance authorities on their request
  - Notify widely about reported vulnerabilities
- Governance reports should document the non-profit character of the organization

* tentative, preliminary, not final

Collaborative lifecycle support

- The best way to ensure the viability of an open source dependency is to participate in the governance of the project
- Through participation in governance, members gain influence on the long-term project roadmap and the contribution process
- By identifying their essential dependencies and engaging with their stewards, manufacturers are able to ensure maintenance throughout the required support period

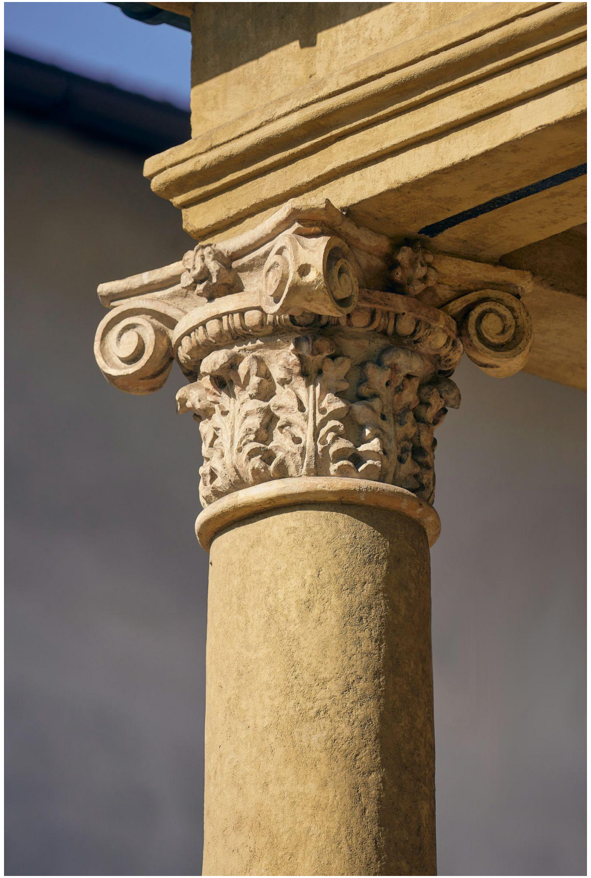


Photo by Jakub Pabis on Unsplash

Outlook

- Legislative status: CRA approved by European Parliament on 12 March 2024 (still subject to lawyer-linguistic review, translations ongoing)
- The CRA is the first union-level regulation that models open source software stewards separately from manufacturers
- Many implementation details to be decided during the upcoming development of harmonised standards, Linux Foundation participates as a stakeholder

Timeline

- CRA should come into effect in mid/second half of 2024
- Vulnerability reporting obligations kicking in after 21 months (early 2026)
- The remaining obligations after 3 years (mid/late 2027)

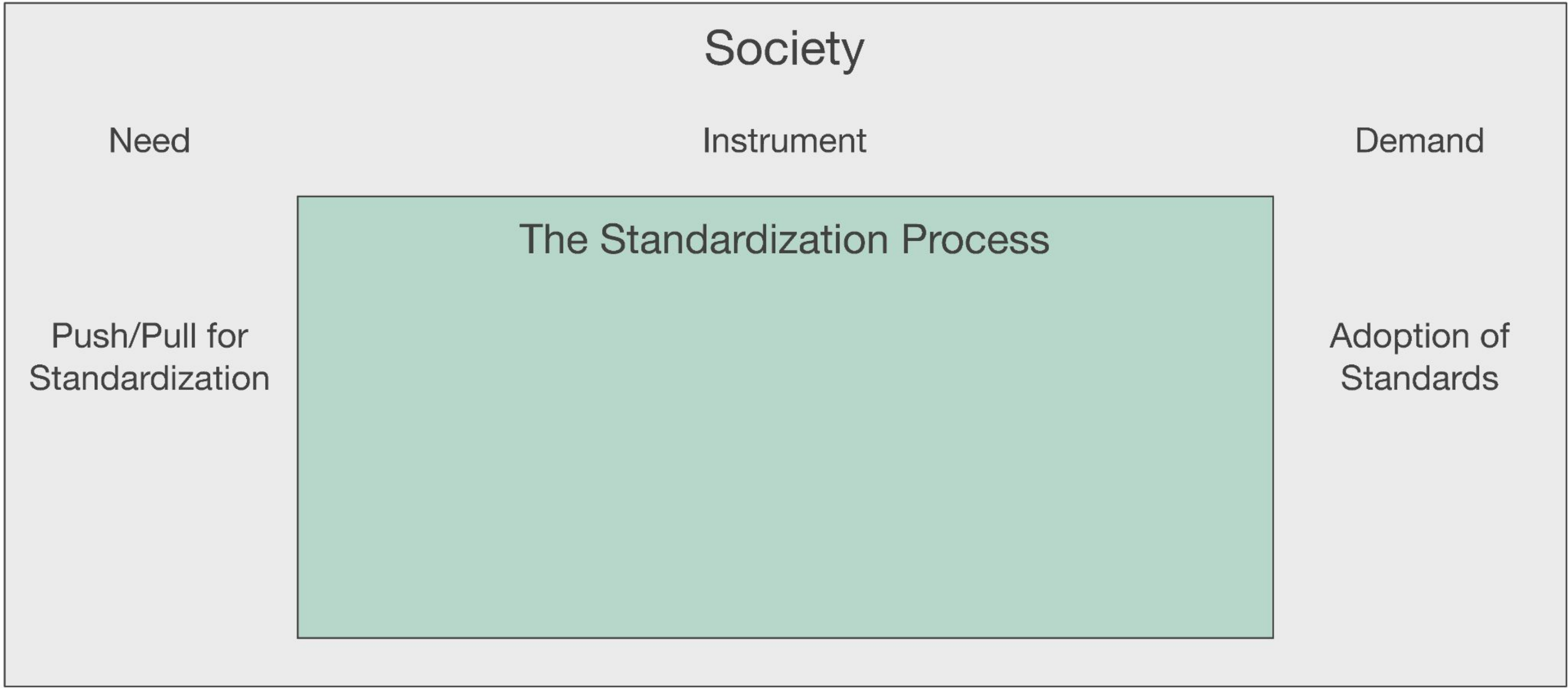
Regulation via harmonized standards

CRA standards development*

- A draft standards development request for 44 standards is being prepared
- Many of the CRA implementation details will be defined in standards
- There will be 2 main groups of standards:
  - Requirements for all products, e.g. “How to deliver products with digital elements without any known exploitable vulnerabilities” or “How to build products with limited attack surfaces”
  - Requirements for specific product types, e.g. “essential cybersecurity requirements for standalone and embedded browsers” or “essential cybersecurity requirements for microprocessors”
- LF Europe is engaged in European standards development

* currently a draft request from EC to CEN/CENELEC

The phase model of standardization



Society

Need

Instrument

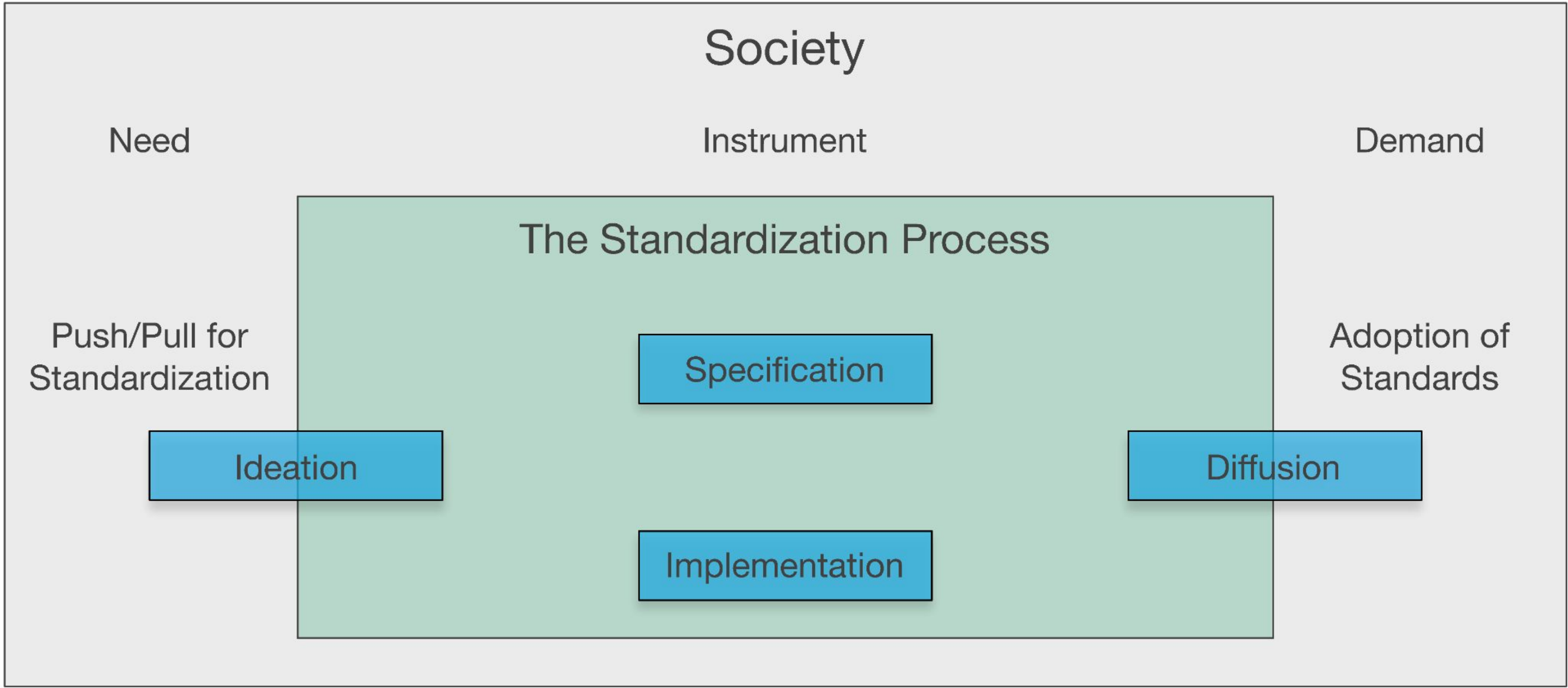
Demand

The Standardization Process

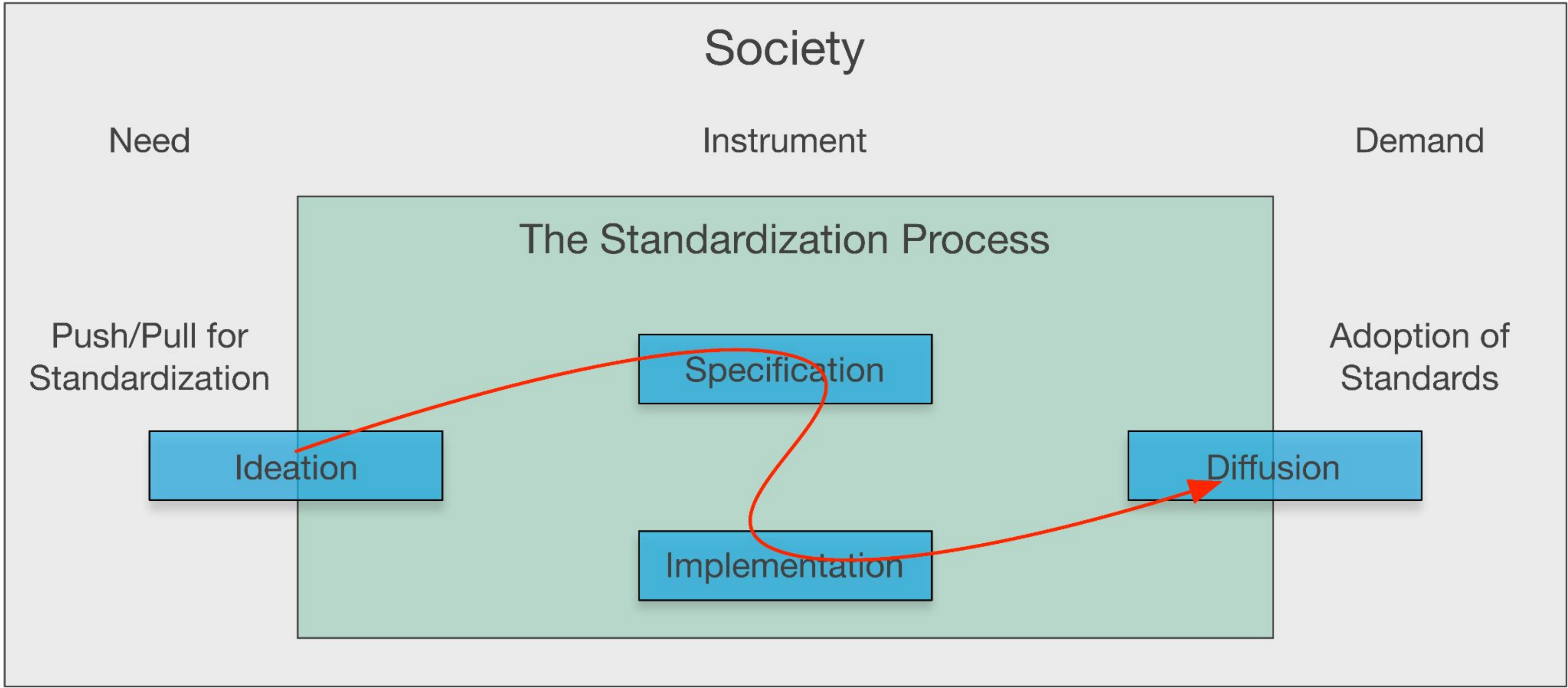
Push/Pull for Standardization

Adoption of Standards

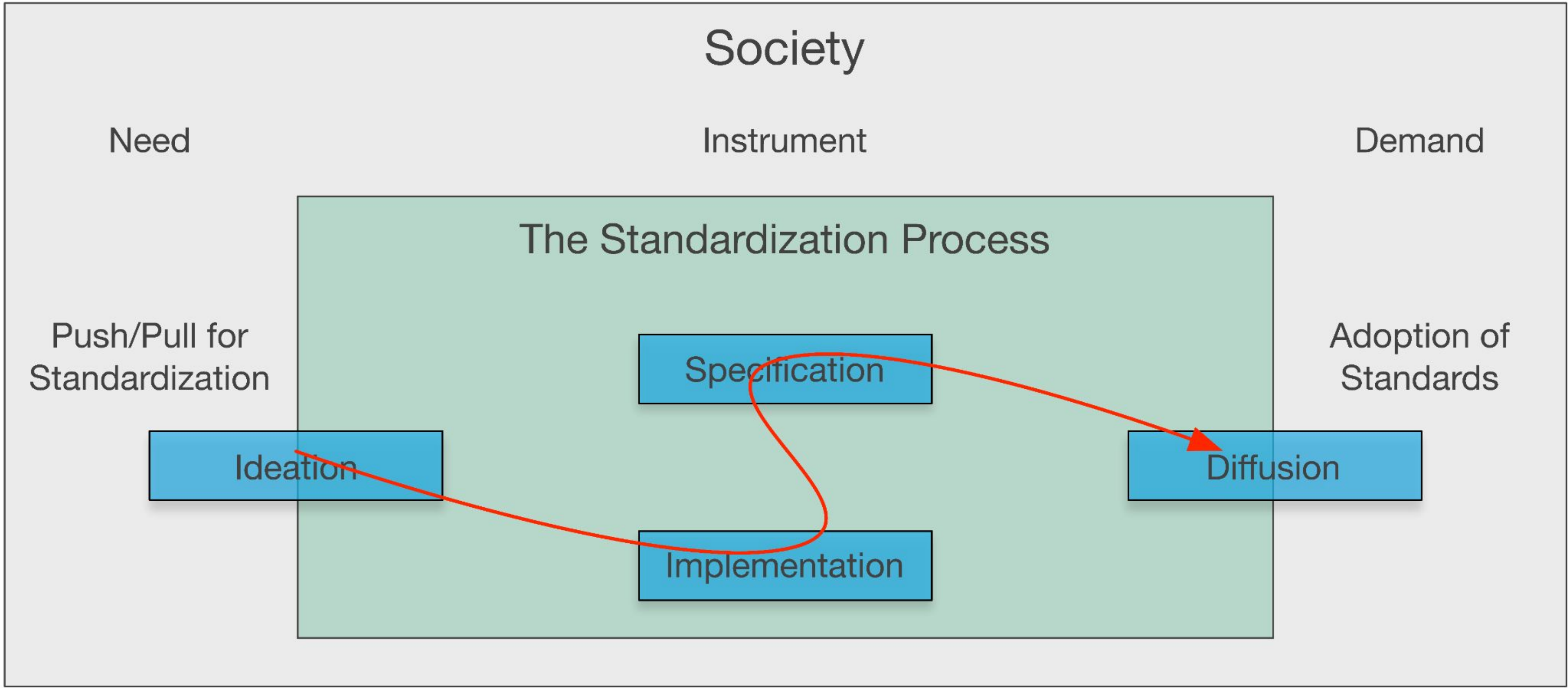
The phase model of standardization



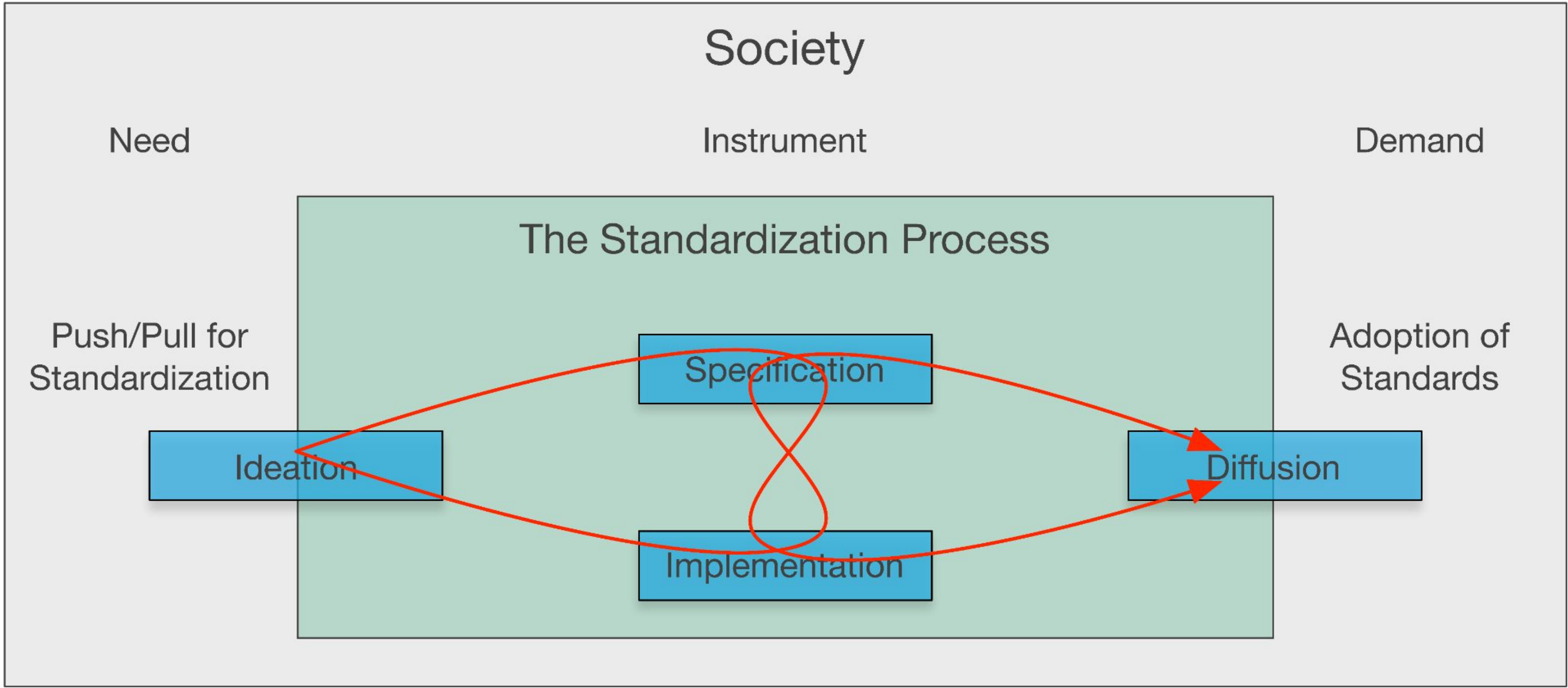
The phase model of standardization



The phase model of standardization



The phase model of standardization



Stakeholder feedback: AI Act draft

- "…concerns about the excessive delegation of regulatory power to private European standardisation organisations…"
- …due to "the impossibility for stakeholders (civil society organisations, consumer associations) to influence the development of standards"
- …advocate that "European policymakers should strengthen democratic oversight of the standardisation process"

(European Parliamentary Research Service, EU Legislation in Progress - Artificial intelligence act.)

Conclusions

1. How does open source software and methods impact innovation (other than being software)?
    a. Governance
    b. IPR framework
    c. Standards development
2. Digital products are being increasingly regulated
3. EU still only applies specification-first approaches in regulation
4. Governance of the OSS ecosystem is forced to level up and mature
5. Manufacturers and Open Source Software Stewards need to establish long-term relationships to cover the mandatory support period
6. Public sector actors still need to develop approaches to adopt open source software and to being a contributor

Thank you!

mirko@linuxfoundation.eu

THE LINUX FOUNDATION | Europe

European Parliament - A smile hidden behind the European flag. European Parliament, CC BY 2.0

Bradford, Anu, "The Brussels Effect: How the European Union Rules the World" (2020). Faculty Books.

The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy - Final study report

Boehm, M., & Eisape, D. (2021). Standard setting organizations and open source communities: Partners or competitors?. First Monday, 26(7). https://doi.org/10.5210/fm.v26i7.10806

European Parliamentary Research Service, EU Legislation in Progress - Artificial intelligence act. Third edition. European Union, 2024.

Cailean Osborne, Mirko Boehm, and Ana Jimenez Santamaria, “The European Public Sector Open Source Opportunity: Challenges and Recommendations for Europe’s Open Source Future,” foreword by Gabriele Columbro, The Linux Foundation, September 2023.