



Towards open source-compatible standards

Open Source Summit Europe
September 2024 – Vienna, Austria

Tobie Langel, Principal
tobie@unlockopen.com









Context

- 🇪🇺 Policy makers are rushing towards **standardizing open source** security best practices.
- 💰 The organisations responsible for standardisation generate their revenue by **selling standards**; they're *publishers*.
- 🍺 If standards need to be sold... they're generally **not freely available**.
- 👉 That's just... **not compatible** with how open source is developed and maintained.
- ⌚ This is **not a new problem**, addressing it has just become **much more pressing**.









Who am I?

-  +  Tobie Langel
-  Jazz drummer → open source dev → consultant
-  UnlockOpen, boutique consulting firm
-  Bridged open source & standards all my career
-  Now heavily involved with standardization related to the European Cyber Resilience Act (CRA).

Tobie Langel, Principal
tobie@unlockopen.com



Towards open source-compatible standards

-  Some necessary historical background
-  The business model of standards organization
-  The interplay between standards and legislation
-  OpenStand: a related, succesfull, earlier attempt
-  What is an open source-compatible standard?
-  Where do we go from there?



Some background history

Tobie Langel, Principal
tobie@unlockopen.com



Proto-standardization



Many stable measurement systems since the bronze age



E.g. the *carat* still in use today comes from the *carob* seed used as a measure of weight in Babylonian times.



Used for commerce, administrative, and tax purposes



Measuring length, weight, surface (cloth, land), volume, time...



More recently: introduction of the metric system during the French revolution



Early “modern” standardization

- “Modern” standards really appear with the **industrial revolution**
- Beyond measurement systems
- Describe basic norms
- Remain very much **in-house**



Humble beginnings

- Henry Maudslay is the first to standardizes *screw thread sizes*
- Allows for consistent creation of matching nuts and bolts
- Popularizes nuts and bolts
- Later pioneers *interchangeability* (the ability to purchase nuts and bolts from *different* providers)
- Only in 1841 that Joseph Whitworth's screw thread measurements spread across Britain and beyond



Acceleration during 2nd Industrial Revolution (1870 – 1914)

- Increase in trade (reduced transport costs because of rail lines)
- Mass production
- Complexity of products (requires supply-chains)
- Need for interoperability
- Build-up towards WWI
- WWI itself
- 👉 Mass adoption of standards
- 👉 Emergence of national and international standards organizations





Emergence of national & international standards organizations

- National:
 - Engineering Standards Committee (now BSI Group) established in London in 1901
 - Similar organisations spread across Europe, the US, Russia, China, and Japan after WWI
- International:
 - 1865: International Telegraph Union (ITU)¹
 - 1906: International Electrotechnical Commission (IEC)

1. Now International Telecommunications Union (still ITU)



Emergence of national & international standards organizations

-  At the national level, these organizations are **trade associations**.
-  Most international organisations bring together relevant national organizations, so they're **membership organizations** of trade associations.



Emergence of national & international standards organizations

- 🇺🇳 After WW II, a few organizations become **affiliated with the UN** (e.g. ITU).¹
- 💾 With the **rise of software**, new international industry consortia, like W3C, emerge in the 1980s.*

1. These aren't really relevant to our current issue, but show that other business models are possible and exist.



Business model of standards organizations¹

- National trade associations
- International membership organizations

1. Worth noting here that the monetization of patents plays an important part in the business model of some industries, it's—again—not really relevant for the standardization of best practices and processes which are rarely patentable.



Business model of *national* standards organizations

These are generally *not for profit* **trade associations** who:

1. Collect membership fees
2. Leverage their member's expertise to create standards
3. Sell those standards to practitioners for a fee



Business model of *international standards organizations*

These are generally *not for profit* international **membership associations** of trade associations who:

1. Collect membership fees from national organizations
2. Leverage the expertise of the members of the national organizations to create standards
3. License the standards that they create to their members who then have the exclusive rights to sell them nationally.



Business model of standards organizations

- 🙄 We shouldn't be judgmental of those business models
- 🙄 They make sense historically
- 🙄 They become more of an issue as the interplay between standards and legislation increases.



Interplay with legislation



Safety concerns, interoperability, trade, and competition drove governments to **push for standardization** since the industrial revolution.



Liability risk has driven practitioners to **adopt standards**: you'd like to be able to answer affirmatively when a judge asks you whether the house you sold has been “built to code.”



Formalization of relationship with legislation

- Since the 1980s: concerted effort by legislators, particularly in Europe, to **formalize** the relationship between standards and legislation
- Standard **move faster** and better **adapt** to **technological innovation**
- Legislators **lack domain expertise** to regulate increasingly complex industries
- 👉 Formalized in Europe: adopting the *harmonized standards* approved by the European Commission creates a **presumption of conformity**



Impact of formalizing the legal roles of standards

- 📖 If standards become part of legislation and aren't freely accessible... then *legislation itself* isn't freely accessible.
- 🏛️ This was successfully argued in court by the nonprofits *Public.Resource.Org* and *Right to Know* earlier this year.¹
- 😞 But the solution in discussion preserves the business model of the standards organizations at the expense of free and open access to those standards.

1. *Public.Resource.Org* and *Right to Know* argued that European harmonized technical standards on the safety of toys should be accessible to EU citizens. The case was won in appeal.



OpenStand

- Tension between business models of traditional standards organizations born during the industrial revolution and requirements of the information age is nothing new
- OpenStand was a successful attempt at addressing that
- Launched in 2012
- New paradigm for global, open standards
- Initial signatories: IEEE, Internet Architecture Board, IETF, ISOC, and W3C
- In tech, when we talk about standards, that's usually what we mean.



OpenStand Principles

1. **Cooperation** between standards organizations
2. Adherence to the **5 fundamental principles** of standards development: due process, broad consensus, transparency, balance, & openness
3. **Collective empowerment** through standards based on technical merit, which provide global interoperability, scalability, stability, and resiliency; enable global competition, further innovation, and benefit humanity.
4. **Accessible** to all for implementation and deployment either royalty-free or under fair, reasonable, and non-discriminatory (FRAND) terms.
5. **Voluntarily adoption**, success is determined by the market.



What is an open source-compatible standard?

Tobie Langel, Principal
tobie@unlockopen.com



What is an open source-compatible standard?

Essentially *OpenStand* plus:

1. Standard has an open source, creative-commons, or permissive document license, so that it can be *forked*.
2. Standard is available for free in an open format.
3. Must be royalty-free (no FRAND).
4. Open participation model based on open source working modes.

Tobie Langel, Principal
tobie@unlockopen.com



OSI's OSR

To my surprise, the Open Source Initiative has had a nearly perfect definition since 2006: the “Open Standards Requirement for Software.”

→ <https://opensource.org/osr-intro>

→ <https://opensource.org/osr>

Tobie Langel, Principal
tobie@unlockopen.com



Do we have a marketing problem?



I hate to admit this... but I learned about OSR rather accidentally.



This is my domain of expertise and I'm fairly well plugged-in... so this might be a bigger issue than just me missing it!



Where do we go from there?

Tobie Langel, Principal
tobie@unlockopen.com



Problem

- ✗ We **don't have good alternatives to offer** to the current standardization process.
- ✗ When asked, **we're hand-wavy** about what an open source-friendly model would look like.
- ✗ We're **bad at marketing** the existing solutions we have.



Opportunity

- ✓ With **OSI OSR**'s we have a pretty good definition of what we need
- 📖 With **OpenStand**, we have a play book of how to market it.
- 🛡️ **CRA-related standardization** is a unique opportunity to experience and document first hand the challenges current standardization models represent for open source.
- 🇪🇺 **Upcoming revision** of EU Regulation 1025 give us a window of opportunity in which to drive adoption of more open source-friendly standardization processes.



Where do we go from there?

Concerted, industry-wide effort to spread the new concept of open source-compatible standardization (OSCS?) through a new cross-organizational initiative.

Tobie Langel, Principal
tobie@unlockopen.com



Open discussion

Tobie Langel, Principal
tobie@unlockopen.com



Thank you!

Tobie Langel, Principal
tobie@unlockopen.com