UnlockOpen

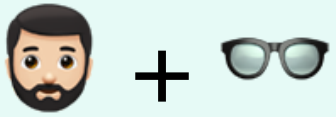
Can security attestations simplify CRA due diligence & strengthen FOSS sustainability?

CRA in practice, FOSDEM

January 2026 – Brussels, Belgium

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen



Who am I?

Tobie Langel

- 🎶 Jazz drummer → open source dev → consulting
- 💼 UnlockOpen, boutique consulting firm
- Bootstrapped the Open Regulatory Compliance (ORC) WG
- 🇪🇺 EU CRA Expert Group member through Eclipse Foundation
- 🪑 CPC Vice Chair & Board Director OpenJS
- ♻️ *Sustainability & supply chain security advocate before it was cool*

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Agenda

- 🏭 CRA requirements for 3rd party component integration
- 🏭 How do manufacturers meet those obligations?
- 📋 Security attestations
- 🏔️ Three layers of attestations
- 🐋 Professionalization of maintenance

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

CRA requirements for component integration

- 🔍 Req. 1: due diligence
- 🚒 Req. 2: vulnerability handling for full support period
- 🔗 For FOSS, these obligations extend to all transitive dependencies

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Req. 1: due diligence

- Ensure integration of components does not compromise the cybersecurity of its own product
  - No requirement for component to meet all of the essential requirements of Annex I, Part I
- Level of due diligence proportionate to:
  - Nature and level of cybersecurity risk of the component itself
  - Risk assessment of **manufacturer's own product!**

- For FOSS, increasing consensus to use BSI's *"Secure Software Lifecycle for Open Source Software"* (BSI TR-03185-2) as baseline.

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Req. 2: vulnerability handling

- 📋 Comply with Annex I, Part II
- ⏳ During full support period
- 📦 Applies to products in their entirety, including all components
- 🔗 For FOSS, this includes all transitive dependencies

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

How do manufacturers meet those obligations?

- 🏠 Option 1: Do everything in-house
- 🏭 Option 2: Rely on a supplier
- 🌱 Option 3: Rely on stewards
- 📋 Option 4: Use security attestations

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Option 1: Do everything in-house

- 🔍 Manually assess components and all dependencies
- 👁️ Continuously monitor them over time
- 🔧 Fix vulnerabilities as they appear
- 💸 Economically unrealistic for most manufacturers
- 🌐 Incredibly inefficient at scale
- 🔗 Manufacturer responsible for transitive deps

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Option 2: Rely on a supplier

- 🍽️ End of the free lunch
- 🏭 Supplier is itself a manufacturer
- ✅ Packages open source components, apposes CE marking, and manages vulnerability handling obligations during entire product lifecycle
- 📋 Greatly simplifies due diligence obligations
- 🤝 Traditional supplier–client relationship
- 🔗 Supplier is responsible for transitive dependencies

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Option 3: Rely on stewards

- ⚠️ Stewards do not help with due diligence
- 👉 Steward's vulnerability handling obligations are a small subset of the manufacturer's
- 🔗 Manufacturer remains responsible for transitive dependencies

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Most projects aren't stewarded

- 🔢 Black Duck's 2024 audit of 965 commercial codebases during M&A across 16 industries identified:
  - 282,521 unique JavaScript packages
  - 33,327 unique Rust packages
- 🟨 OpenJS Foundation stewards 35 projects
- 🦀 Rust Foundation stewards 232 projects
- 👉 That's a massive gap

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Option 4: Security attestations

- 🇪🇺 Defined in Article 25 of the CRA
- 🔎 Purpose: facilitate the due diligence of manufacturers
- ⬅️ Emerged from the idea of “shifting security left”
- 💰 And the need for a mechanism to pay for that
- ✅ Can be thought of a FOSS equivalent to CE marking

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Option 4: Security attestations

- 🙋 Voluntary
- ⚠️ Can be issued by stewards, maintainers, integrators, external parties
- 🏛️ EU Commission is empowered to establish security attestations programs through delegated acts
- 🛡️ Ongoing work and discussions in ORC lead by Æva Black

Tobie Langel, Principal
tobie@unlockopen.com

For attestations to be viable

- 📈 Provide meaningful value to manufacturers
- 💰 Be cheaper than in-house or outsourced alternatives
- 🔗 Somehow help tame the transitive dependency scale issue

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Three layers of security attestations

1. Public, automatable signals
2. Private security information
3. Commitment to longterm maintenance

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

1️⃣

Layer 1: Public, automatable signals

- 📊 Externally observable project data:
  - Commit frequency, PR activity, project health metrics
- 📄 Codebase and process signals:
  - Documented practices, basic security hygiene
- ✅ High value for baseline security decisions
- 💰 Very low cost to produce, easily automated

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

1️⃣

Layer 1: Likely providers

- 👨‍💻 Code hosting platforms
- 📦 Package managers
- 🌱 Stewards
- 🔧 Security tooling vendors
- 💸 Limited monetization potential

Tobie Langel, Principal
tobie@unlockopen.com

2️⃣

Layer 2: Private security information

- 🔒 Non-public, project-internal data:
  - CVE history, time-to-fix metrics
  - Internal security processes (CI/CD, deployment, package management, etc.)
- 🔍 More relevant to due diligence
- 🛡️ Better insight into security posture
- 💸 Difficult for maintainers to monetize, perhaps easier for stewards

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

3️⃣

Layer 3: Commitment to longterm maintenance

- 🤝 Explicit commitment to:
  - Address future security issues
  - Respond within defined timelines
  - Manage dependencies
- ⏳ Directly supports longterm CRA obligations
- 🔐 Ensures products remain secure over their lifecycle
- 👷 Maintainers best positioned for this

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Layer 3: is where the value is

- 🔗 Helps tame transitive dependencies
- 💰 Addresses total cost of acquisition (TCA) not just due diligence
- 👨‍🔧 Maintainers are uniquely positioned to benefit from this this layer

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Concerns

- ⚖️ Does this make maintainers take on liability or contractual obligations?
- 🛡️ Can attestations sustain maintainers without implicating them?

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Professionalization of maintenance

- 🙋 Feature development remains volunteer-driven
- 🐋 Maintenance provided by “maintainer pods” of **paid** maintainers focused on longterm security maintenance & provide attestations
- 🌱 Could be stewards or separate organizations:
  - 💼 For-profit (e.g. HeroDevs, Tidelift)
  - 🏛️ Nonprofit (e.g. OSTIF)
  - 👨‍💼 Maintainer coops
  - 👨‍💻 Possibly solo maintainers depending on liability aspects

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Maintainer pods: focus

- 🛡️ Security support & training
- 🔧 Tooling & infrastructure
- 🐞 Bug triaging
- 🚀 Release engineering
- 📚 Documentation
- 👨‍⚖️ Compliance

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Maintainer pods: team organization

- 📋 Develop dedicated practices
- 👨‍🏫 Security training for maintainers
- 👨‍💼 Proper management & career path
- ⅕ Fractional maintainers for smaller projects
- 💰 Share resources across projects

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Benefits for maintainers

- 💼 Part-time opportunities
- 👨‍⚕️ Proper management support
- ❤️‍🩹 Healthcare & mental health support
- 🛝 Better separation between work & play
- 💰 Fund development through maintenance, not maintenance through development

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Benefits for manufacturers

- 🛡️ Improved software supply chain security
- ✅ Simplified due diligence for compliance
- 👨‍💼 Fewer, more easily identified and professional interlocutors
- 🔐 Alternative to gated (vendored) open source solutions

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

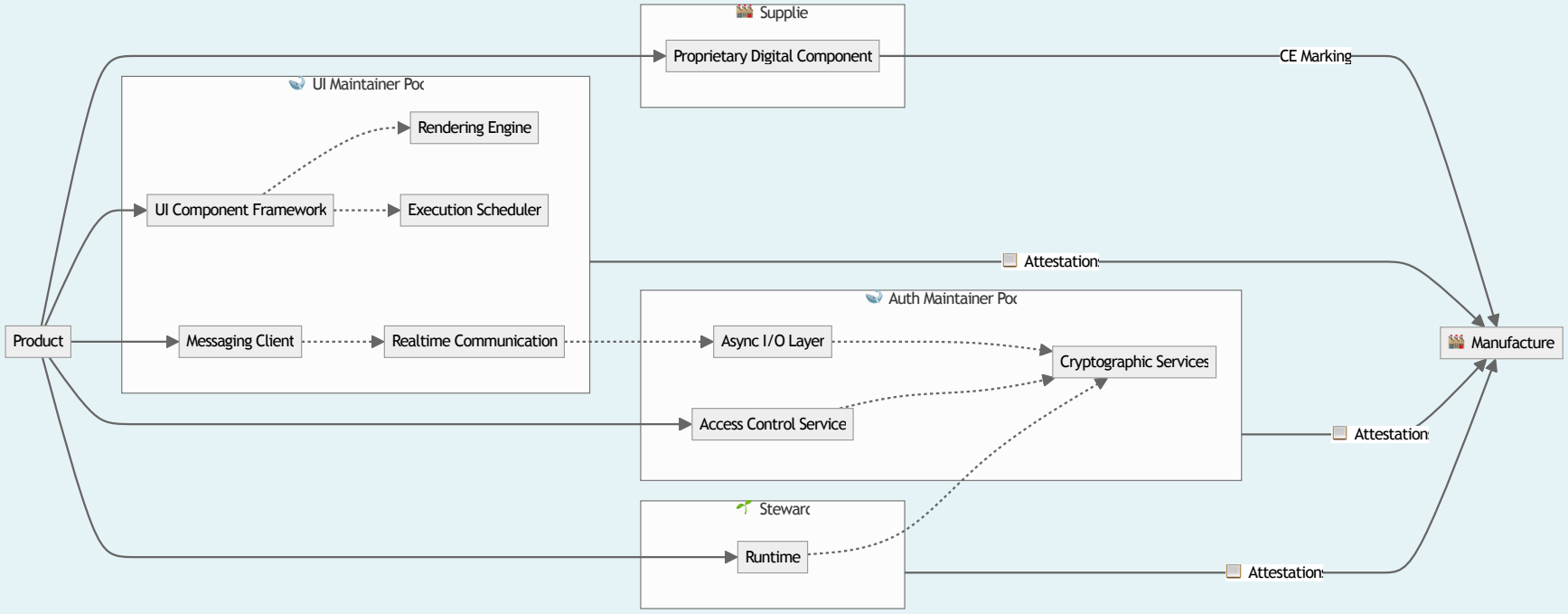
Maintainer pods vs. stewards

- 🌱 Stewards have tight coupling with their hosted project
- 🐋 Pods are closer to commercial offerings like HeroDevs or Tidelift:
  - looser coupling
  - focus on manufacturer needs
  - fractional maintenance
- 🌐 Great fit for ecosystems with many small projects (e.g. JavaScript)
- ⚠️ Might not be a good fit everywhere
- ⚠️ May require additional coordination at project level

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Example dependency coverage map



Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Summary

- 🔎 CRA requires due diligence and vulnerability handling for all components, including transitive dependencies
- 📋 Security attestations can help facilitate this
- 3️⃣ Three layers: public signals, private info, maintenance commitment
- 💰 Greatest value add of maintainers is in providing long term maintenance
- 🛡️ Shielding maintainers away from personal liability requires professionalizing maintenance
- 🏭 Focus on manufacturer needs is key to create value → sustainability.

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Tobie Langel, Principal
tobie@unlockopen.com

