ECLIPSE FOUNDATION

# Workshop For Voluntary Security Attestations for Free & Open Source Software

*Facilitated by:*
*Æva Black*
*Null Point Studio*

# Agenda

- short overview
- workshop structure
- break for discussions (45 min)
- reconvene and wrap up (20 min)

# Voluntary Attestations: Overview

# Opportunity

Recognising the unique characteristics of Free and Open Source Software (F/OSS), the CRA establishes a **differentiated, light-touch regulatory regime for F/OSS Stewards**.

Article 25 enables the European Commission to adopt a **delegated act specifying the nature and structure of voluntary security attestations**.

# Objectives

- Identify and propose mechanisms to reduce manufacturer’s compliance burden when using F/OSS that is supported by a Steward
- Prioritize improving the economic sustainability of F/OSS, e.g. by creating accountability for the shared costs associated with security, maintenance, and infrastructure
- Avoid approaches which would burden F/OSS or SMEs
- Account for all sizes of F/OSS projects

# Article 3: Definitions

(13) ‘manufacturer’

means a 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 its name or trademark, whether for payment, monetisation or free of charge;**

(14) ‘open-source software steward’

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

*Remember – this is only about F/OSS “intended for commercial activities”*

*It’s not about personal expression, hobby projects, etc,*
*and also not about other regulated industries (medical, aeronautics, etc)*

# Manufacturer's Obligations

*paraphrasing the legal text*

Article 13(5)

Exercise diligence when integrating FOSS, even from non-commercial sources.

Article 13(6)

Report vulnerabilities discovered in, and remediations developed for, FOSS, even from non-commercial sources.

Article 13(7)

Include FOSS in the documented risk assessment.

Article 13(8)

Handle vulnerabilities in the product for its lifecycle, including those resulting from FOSS.

# Steward's Obligations

*paraphrasing the legal text*

Publish documentation regarding:

- cybersecurity policy relevant to a project's use in a product.
- vulnerability handling policy, including how downstream developers can report.

Willingness and capacity to:

- cooperate with European market surveillance authorities.
- notify ENISA and Nat'l CSIRT of any severe incident affect project infrastructure.
- notify affected/known users of any severe incident or vulnerability with downstream effects.


CRA obligations apply to manuf. *regardless* of whether F/OSS is used in the product.

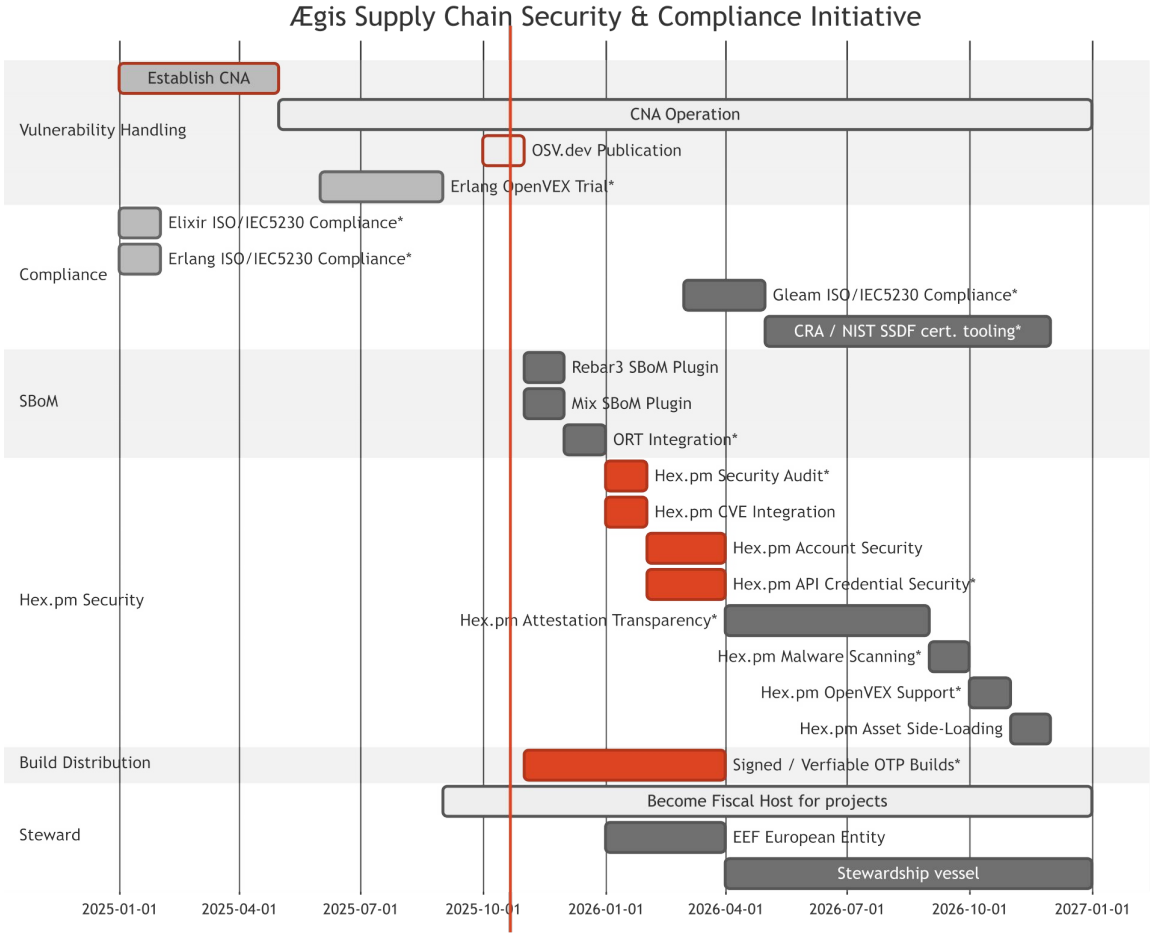
Art.25's attestations support the efficiency which emerges from transparent and open collaboration while improving cybersecurity for all digital products.

# Erlang’s Journey

# EEF Status

## Attestations –

- SLSA
  - Source / Build Provenance
- Hex.pm
  - Release Attestation
  - Malware / Malicious Package Scanning Result
  - OpenVEX Statements
- SBoM
  - SPDX / CycloneDX
- Process Evidence
  - OpenChain (ISO/IEC 5230)
  - NIST SSDF
  - OpenSSF Baseline
  - CRA

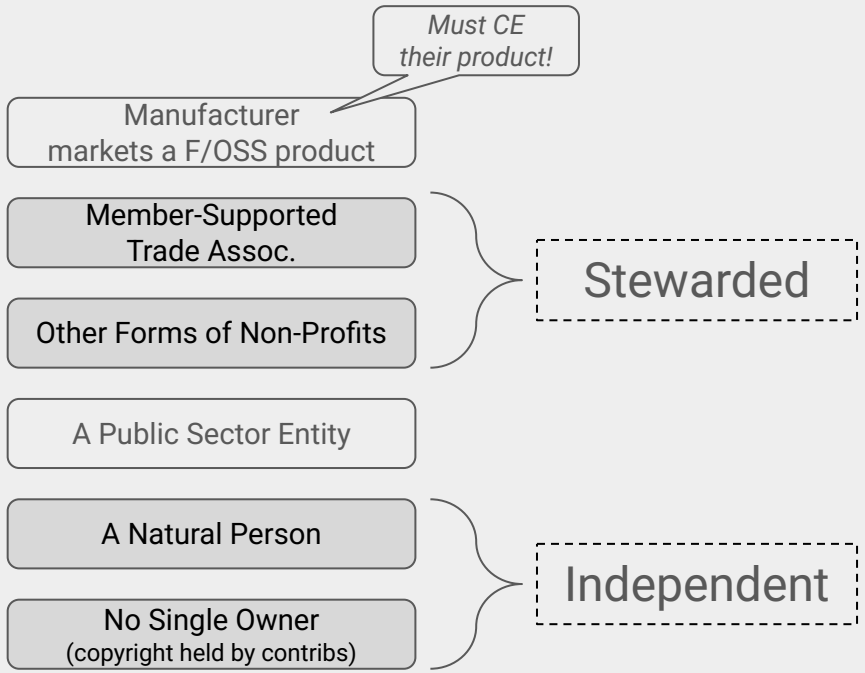


# Workshop Structure

# Scoping The 7 Breakouts

Each group should consider both Stewarded and Independent Projects

## Qualitative Differences based on legal owner of a Project



# Challenge #1A

# Process-based Attestations

Exactly *what* should be attested to?

How is it *useful*
to a manufacturer?

This should be a “light weight” requirement, based on F/OSS Projects self-attesting to their secure development processes and practices.

It should be accessible to projects that lack organizational supports, including non-stewarded projects.

This could be similar to OpenSSF SLSA + Scorecard… or …?

# Challenge #1B

# Outcome-based Attestations

Exactly *what* should be attested to?

How is it *useful*
to a manufacturer?

This should be a “heavy-weight” requirement. In terms of compliance effort, think of it as closer to a CE mark.

It could be self-attested
or verified by third-party audit.

It should be based on measurable conformity to CRA Annex II.

It may build on conformity to product-specific CRA vertical standards.

# Challenge #2

# Economic Mechanisms

What are practicable means to *receive and measure* sustainable economic support via an Attestation Programme?

Some potential solutions could be…

- Download tracking
- Token embedding, modelled after the media industry

*Consider*:
*- how will MSAs perform post-market verification?*
*- how will aggregators re-distribute support to upstreams?*

# Challenge #3

# Transmission Verification

How should an attestation be *transmitted to & used by* a manufacturer?

How can they be *verified* by market surveillance authorities?

Is it sufficient to email PDF files with a digital signatures? Do we need a more modern/scalable approach, e.g. Sigstore or SCITT?

Does this need to be decentralized – like a public ledger?

Does this need to be centralized – e.g., run by national bodies?

*Consider:*
*- operational costs*
*- handling trusted third parties*
*- handling bad actors*
*- revocations*

# Challenge #4

# Identifying Minimums

What's the small-project min-bar for an attestation to be useful?

For larger or stand-alone projects, what's the minimum that a manufacturer would benefit from?

Do SLSA, Scorecard, or other open source security frameworks come "close enough" to a common set of elements of Annex I(2) that common guidance could be given?

How would this apply to libraries that are never used in a stand-alone fashion?

How would this apply to stand-alone projects – those like a consumer product? Should these apply (portions of) the vertical standards?

# Challenge #5

# Complications of Third-Parties

The CRA provides for *third party attestations* of F/OSS

Consider the secondary effects –

- Are first-party attestations (ie. by the steward) more trustworthy than third-party?
- If attestations are public, will this require moderation and/or a dispute resolution process?
- Should there be limitations on who can issue attestations?
- What if different attesters use very different metrics?

# Challenge #6

# Transitive Dependencies

Can an Attestation programme account for transitive dependencies?

Should it try?

Most projects depend on other projects. Who attests to what?

Projects that are more like a Product could, theoretically, self-attest to vertical standards. Such projects generally have a very large number of dependencies.

Should projects aggregate attestations from their dependencies?
… If so, how does this work?
.. If not, how does that work?

Are we ready for full-depth SBOMs in OSS?

Can tools like Nix and OmniBOR help?

# Other Topics

Not for deep discussion today…
but we should come back to them

- Publishing guidance for independent projects transition to becoming stewarded
- Impacts/implications for Fiscal Hosts
- Interaction between non-EU-based Stewards and ENISA, MSA's, etc
- Tiered approach to compliance (Low/Med/High) such that new market entrants are not significantly burdened when using FOSS
- Projects that decide not to participate in issuing Attestations

# Reconvene in 45 minutes for group read-outs and planning next steps

# Read-outs & Discussion

# Thank you!

# END WORKING DECK