Unlocking Software Supply Chain Security Updates from Ecma International: TC54 and OWASP

September 2025

Session and Speakers

Samina Husain (Secretary General, Ecma International)

- Introduction and Ecma’s role in CRA-related global standards

Steve Springett (Chair Technical Committee TC 54)

- Introduction to TC54, CRA relevance, and an overview of current work in CycloneDX 1.7 and 2.0.
- Common Lifecycle Enumeration (CLE) (Co-Convenor)
- The Transparency Exchange API (TEA) (Co-Convenor)

Philippe Ombredanne

- Package-URL (Convenor)

Q&A

Open Regulatory Compliance
CRA Mondays
Unlocking Software Supply Chain Security:
Updates from Ecma TC54 and OWASP
Steve Springett | Olle E Johansson | Philippe Ombredanne

Outline

1. Overview Ecma
2. CRA and SBOM
3. TC54 - Software and system transparency

Thank you - Open Regulatory Compliance - Eclipse Foundation:

Shanda Giacomoni

Senior Marketing Manager

Juan Rico

Senior Program Manager

Overview

Founded in 1961

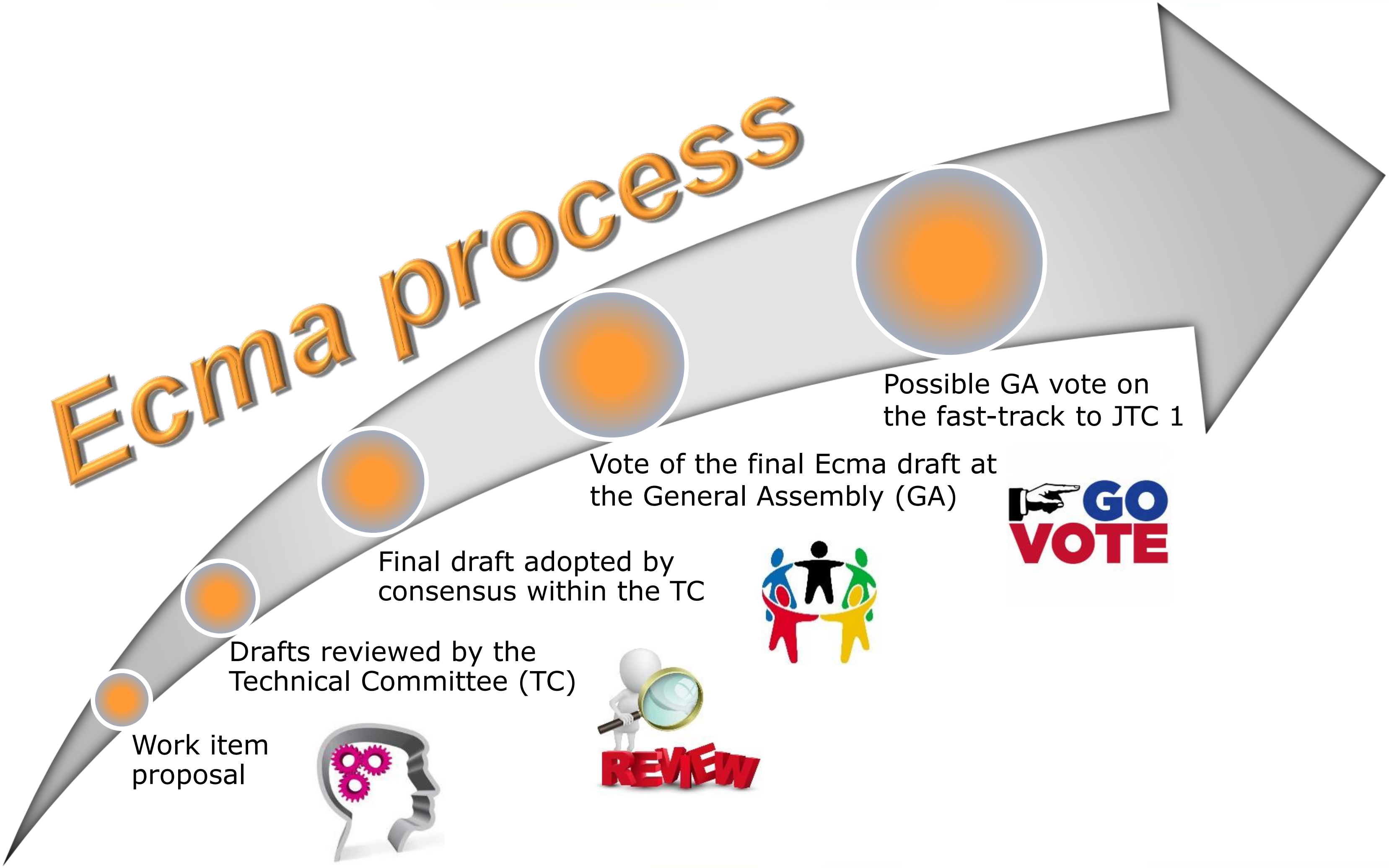
- **Ecma International** is a global industry association that develops standards for ICT, based in Geneva Switzerland.
- Covering a wide range of standardization topics, including hardware, software, communications, media, storage, consumer electronics, environmental technologies, and AI.
- Track record: Over **530** publications (standards/technical reports) and over **230** published by ISO/IEC.

https://ecma-international.org/

Experts-driven standards development

- Proactive group of experts
- Internationally recognized publication of standards
- Efficient and agile process

The Path



Ecma process

Work item proposal

Drafts reviewed by the Technical Committee (TC)

Final draft adopted by consensus within the TC

Vote of the final Ecma draft at the General Assembly (GA)

Possible GA vote on the fast-track to JTC 1

TC54 – In relation to CRA and SBOM

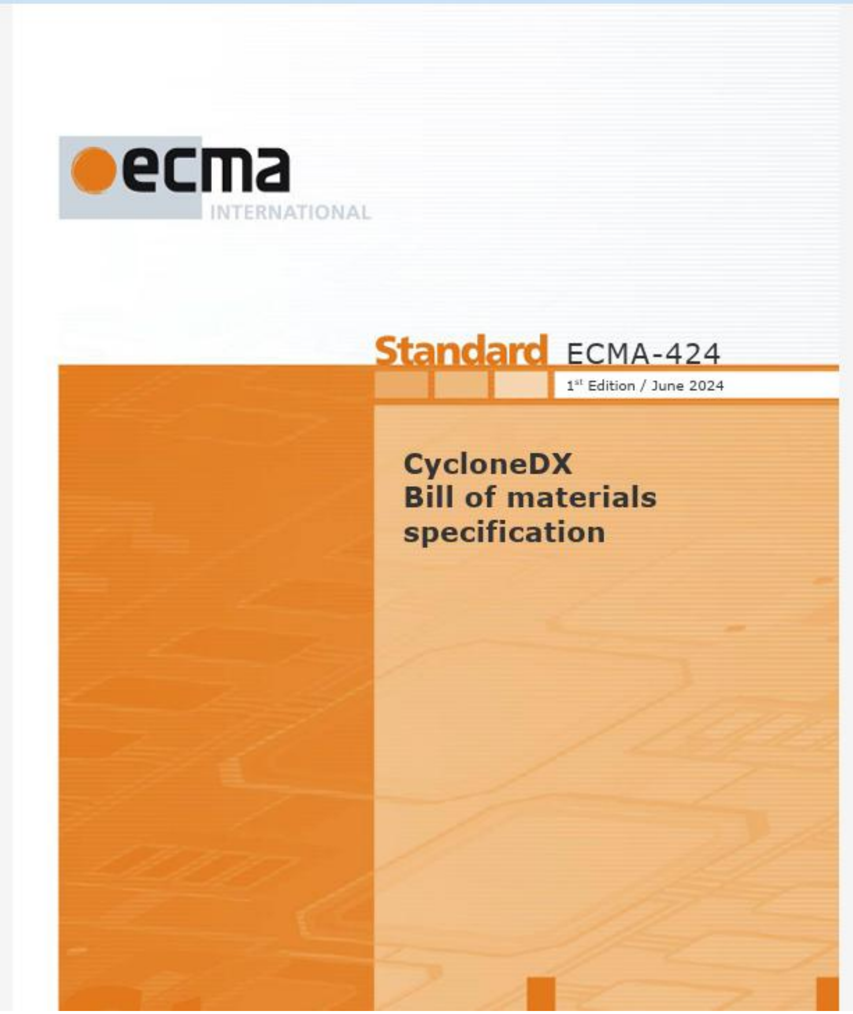
Ecma in collaboration with OWASP:

- **ECMA-424 -** CycloneDX Bill of materials specification, *1st edition, June 2024*
- This Ecma International standard defines the CycloneDX v1.6 Bill of materials specification.

https://ecma-international.org/technical-committees/tc54/?tab=published-standards

Key items:

- SBOM
- Data model
- Security features
- *and more…*



ecma INTERNATIONAL

Standard ECMA-424

1st Edition / June 2024

CycloneDX
Bill of materials
specification

TC54 - Software and system transparency

Programme of work:

- To develop a standard for the CycloneDX software transparency and Bill of Materials specification.
- To develop a standard for the Transparency Exchange API (Project Koala) for discovering and sharing of software transparency information.
- To develop a standard and guidance for multiple BOM merging algorithms.
- To investigate the further direction of standards in the software transparency space.
- To evaluate and consider proposals for complementary or additional technology.

https://ecma-international.org/technical-committees/tc54/

TC54 – Task Groups

- *TC54-TG1 Transparency exchange API*
- *TC54-TG2 Package URL*
- *TC54-TG3 Common Lifecycle Enumeration*
- *TC54-TG4 OS Sustainability Specification* ***To be announced soon***

Thank you

Rue du Rhône 114
CH-1204 Geneva
T: +41 22 849 6000
F: +41 22 849 6001

www.ecma-international.org

Liaisons

Ecma International has collaboration with other formal SDOs such as ISO, IEC, JTC 1, ITU-T, W3C, OWASP and IETF.

- Liaison relationships:
  - *ISO/IEC JTC 1 (Category A)*
    - Ability to propose Ecma standards as international standards
    - Ecma follows JTC 1 fast-track procedure which accelerates the path to approval and publication of the ISO/IEC standard
  - *ITU-T (A.5)*
    - Enables technical cooperation, exchange of documents and reference to Ecma standards

Ecma International and the Open Compute Project collaboration.

MoU relationships: https://www.opencompute.org/about/alliance-partners

- *to collaborate, explore and establishing new global standards in areas needed*

Members 1 of 2

Ordinary

- Bloomberg®
- Google
- HUAWEI
- IBM
- Meta

Associate

- Alibaba Group 阿里巴巴集团
- JET BRAINS
- ByteDance
- Lockheed Martin
- CLOUDFLARE
- Microsoft
- DELL
- ORACLE®
- f5
- salesforce
- servicenow
- Functional Software
- shopify
- HITACHI Inspire the Next
- Sony Interactive Entertainment
- hp
- 360 www.360.cn

Small and Medium Enterprise

- HEAD acoustics
- Lyten
- herodevs
- Vercel
- igalia

Small Private Companies

- AGORIC
- Replay
- Deno
- RunKit (*Pax Andromeda*)
- GVE Ltd.
- Sujitech *(Mask Network)*
- moddable
- orama
- Zalari

Members 2 of 2

Not For Profit

AboutCode

Archive Disc Test Center

Ben-Gurion University of the Negev

DATLAS

Dr. G.R. Damodaran College of Science

EPFL

ETH

IT R&D Global Leader ETRI

法政大学 HOSEI University

humanitarian TOOLBOX

imec

Imperial College London

INDIANA UNIVERSITY

Indian Institute of Technology Delhi

Inria INVENTEURS DU MONDE NUMÉRIQUE

IT University of Copenhagen

NHK Japan Broadcasting Corporation

JBMIA

Kahu Research

慶應義塾 Keio University

KOREA UNIVERSITY

BERKELEY LAB

MICHIGAN STATE UNIVERSITY Founded 1855

mozilla

OITDA

OpenJS Foundation

OSB Open Source Business ALLIANCE Bundesverband für digitale Souveränität e.V.

Osaka Metropolitan University

大阪産業大学 OSAKA SANGYO UNIVERSITY

OWASP

PURDUE UNIVERSITY

SFW Small Fan Workshop

TAMA UNIVERSITY 多摩大学

The LIBRARY of CONGRESS

UEC TOKYO

UNIVERSITY OF BERGEN

UC Santa Cruz

USF UNIVERSITY OF SOUTH FLORIDA

UNIVERSITY OF TURKU

University of Victoria

VCI