COBALT AND DOSS EU PROJECTS

SUPPORTING AUTOMATED COMPLIANCE BASED ON OSCAL

Actions Beyond Words: Automating Audits for Streamlined Cybersecurity Policy Compliance in Europe

D. Antonio Skarmeta

D. Sara Matheu

University of Murcia

Europe towards cybersecurity certification and compliance

NIS2

To **promote cooperation and information exchange** among EU Member States to prevent and respond to cybersecurity incidents

Address **supply chain security**

Establish relationships with high-risk third-party service partners/providers/vendors and **make them aware of risks**

CSA

To create a **common framework for the cybersecurity certification** of any ICT product, service, or process

Monitoring compliance with certification requirements

Use of **repositories** listing vulnerabilities as additional cybersecurity information for certified products

EUCC, EUCS

CRA

To enhance cybersecurity and cyber resilience in the EU through **common cybersecurity standards** for products with digital elements

Mandates manufacturers **to manage security throughout the product's lifecycle** (updates for 5 years, handling of new vulnerabilities)

Establishes **essential requirements**

STILL SOME CHALLENGES

Cost and time:

The existing approaches for cybersecurity certification are often time consuming and complex, requiring formal documentation and processes

How to automate the process?

How to support from lifecycle?

Composition and transparency

Reuse as much as possible the evidence and the results that come with the certified component during the evaluation of the composed product

How to obtain the needed information for composition?

Dynamicity

A security change may require a re-evaluation and re-certification process

Security change could be a vulnerability but even an update

How to track changes? How to communicate?

Context

How to determine security level of a device if context is unknown?

How to guarantee a security by default configuration?

DOSS AND COBALT APPROACHES

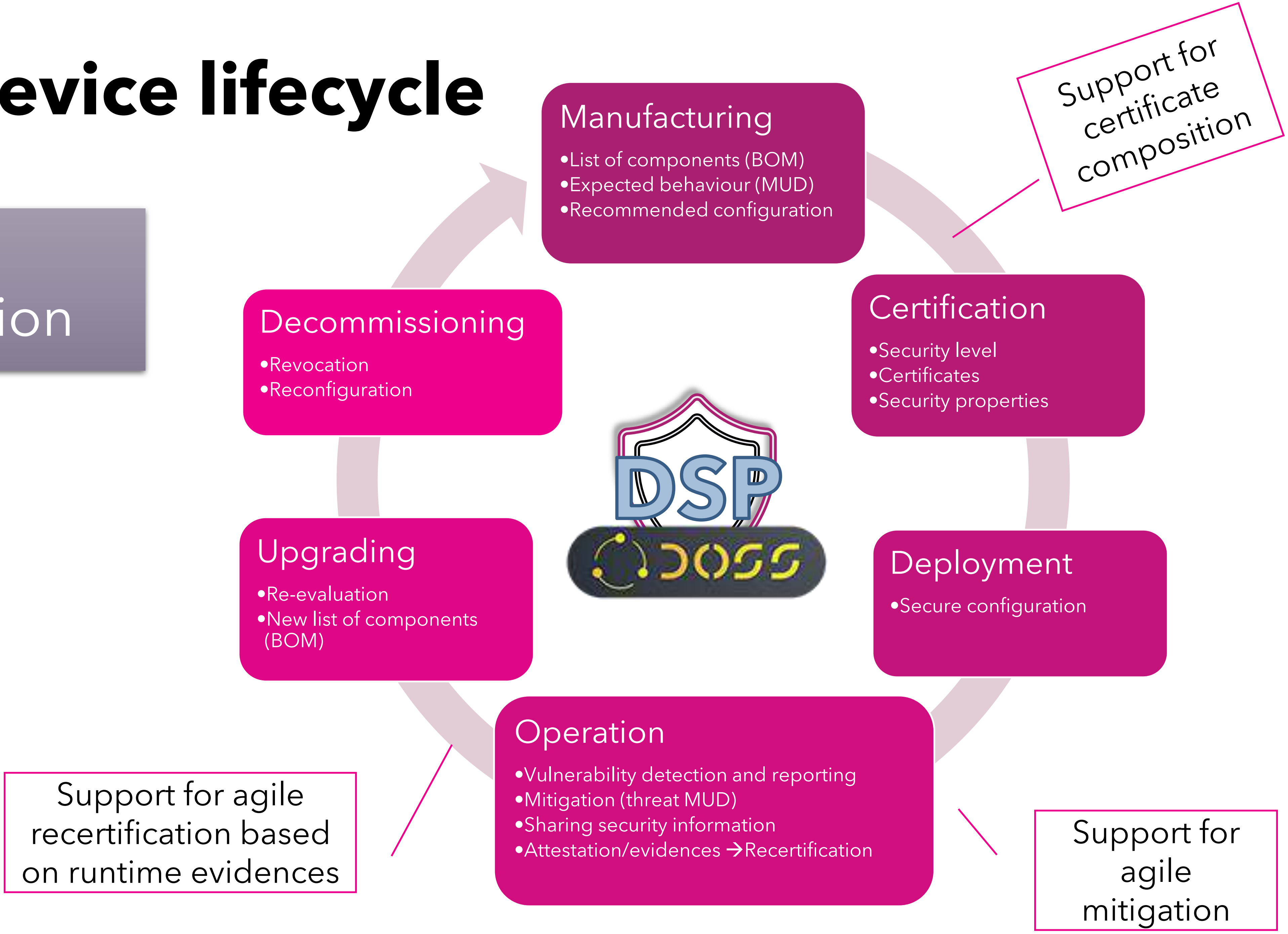
DOSS COBALT

The DOSS concept

- Providing more insight, visibility into the overall supply chain generates relevant security related information.
- Placing control points into key stages of the supply chain reduces the attack surface and mitigates risks.
- DOSS combines these two approaches by
  - Introducing a comprehensive machine-readable product documentation containing all security related information of a product and making it available to all stakeholders of the supply chain – Device Security Passport (DSP)
  - Operating a testing-modelling- validating architecture which ensures that product documentations are genuine and complete, products do not have vulnerabilities, systems are adequately configured and meet the related standard requirements.
- With this concept DOSS aligns with key cybersecurity regulations such as NIS2, the EU Cybersecurity Act (CSA), and specially with the Cyber Resilience Act (CRA) to establish a trusted and resilient supply chain.

DSP and device lifecycle

Many actors
A lot of information



Manufacturing

- List of components (BOM)
- Expected behaviour (MUD)
- Recommended configuration

Support for certificate composition

Certification

- Security level
- Certificates
- Security properties

Deployment

- Secure configuration

Operation

- Vulnerability detection and reporting
- Mitigation (threat MUD)
- Sharing security information
- Attestation/evidences →Recertification

Support for agile mitigation

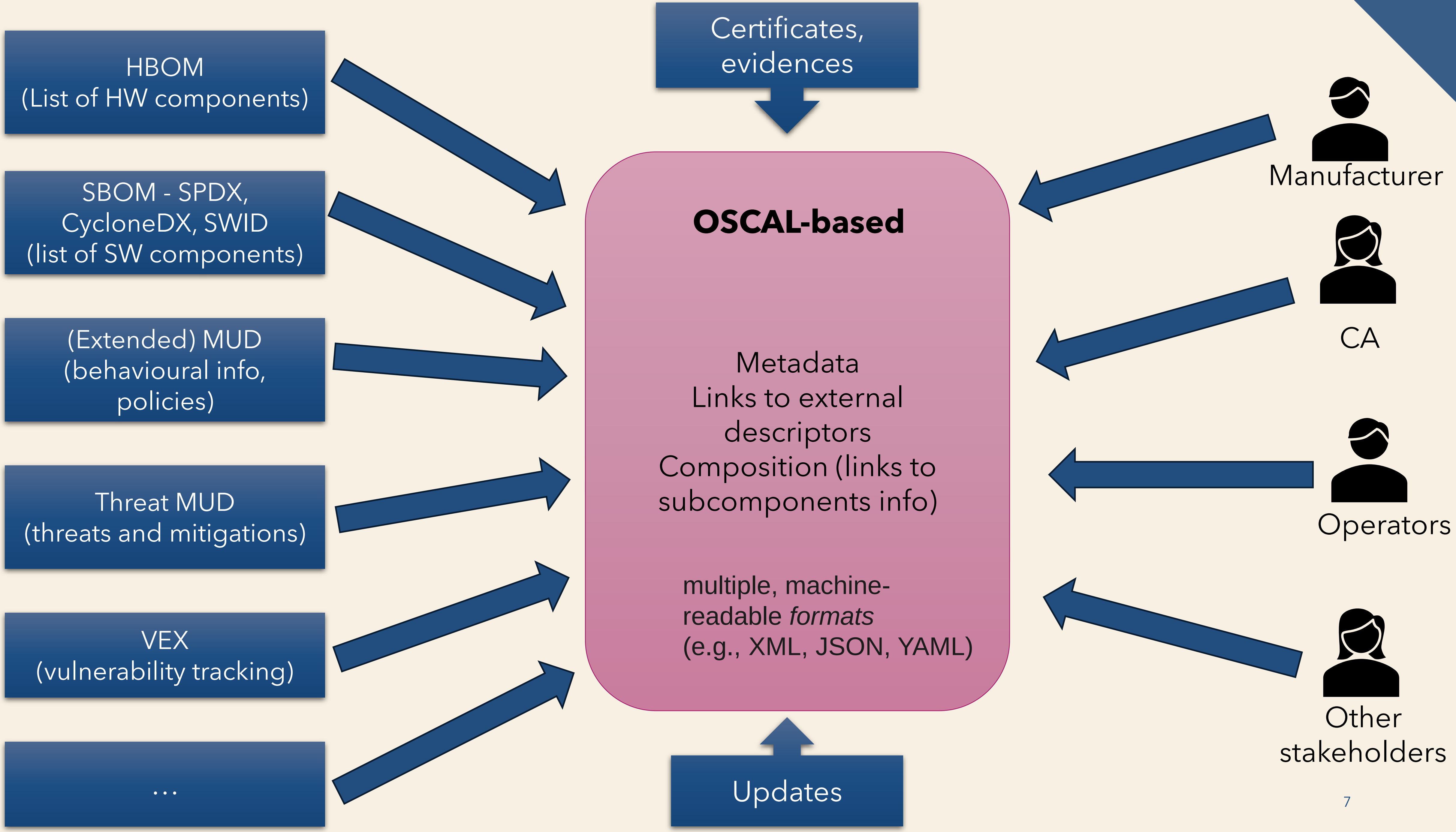
Support for agile recertification based on runtime evidences

Upgrading

- Re-evaluation
- New list of components (BOM)

Decommissioning

- Revocation
- Reconfiguration



HBOM
(List of HW components)

SBOM - SPDX,
CycloneDX, SWID
(list of SW components)

(Extended) MUD
(behavioural info,
policies)

Threat MUD
(threats and mitigations)

VEX
(vulnerability tracking)

…

Certificates,
evidences

OSCAL-based

Metadata
Links to external
descriptors
Composition (links to
subcomponents info)

multiple, machine-readable *formats*
(e.g., XML, JSON, YAML)

Updates

Manufacturer

CA

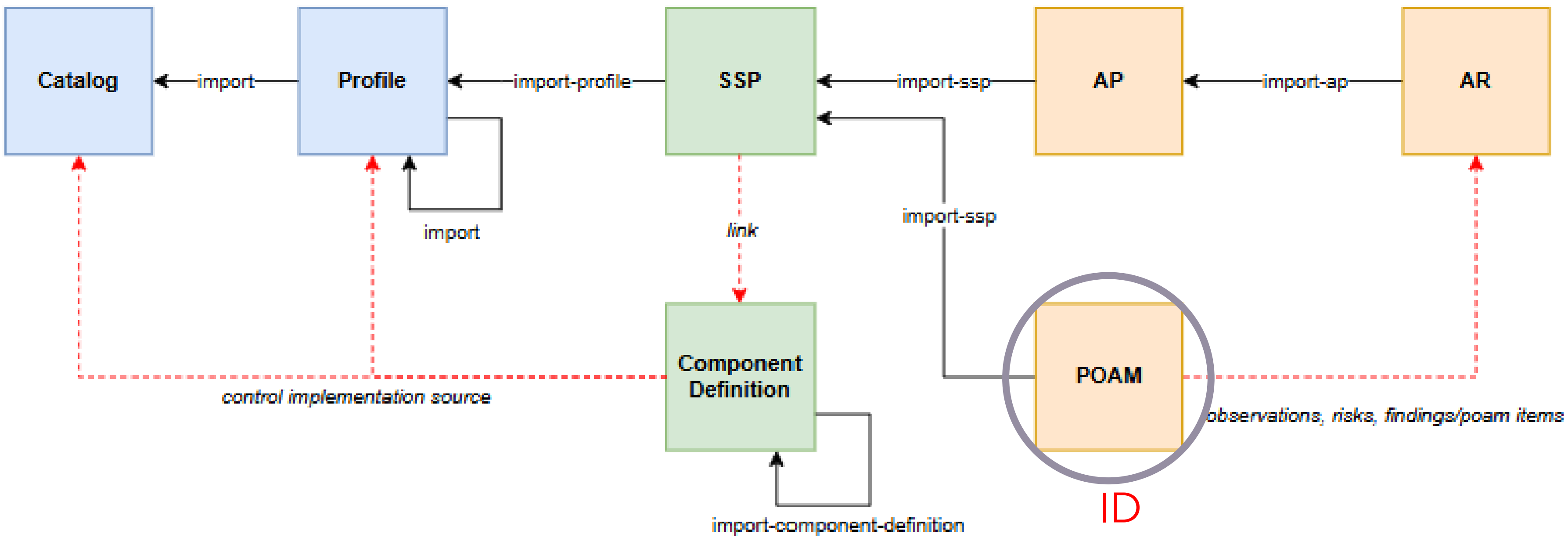
Operators

Other
stakeholders

DSP based on OSCAL models

MUD, BOMs

CT report, VEX, VDR, threat MUD



ID

Non used models are kept as optional for future extensions if needed

Plan of Action and Milestones (POA&M)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For Roles, People, Teams, Locations

Import SSP
URI pointing to an OSCAL SSP

System Identifier
Unique system ID – used when the SSP is not delivered with the POA&M

Local Definitions
For content not defined in the SSP

Observation
Individual observations and evidence, impacted assets

Risk
Enumerates , characterizes, and provides status for identified risks

Deviation Requests (DRs)
False Positives (FP)
Risk Adjustments (RA)
Operational Requirement (OR)

POA&M Items
POA&M ID
Impacted Controls
Weakness Details

Back Matter
Attachments and Embedded Images
DR Evidence
Other Attachments as Needed

A DSP supporting CRA requirements

CRA requirement	What the DSP contains to support it	How this information supports it
Identify and document components contained in the product, including software bill of materials	**NIST SBOM:** a formal, machine-readable inventory of software components and dependencies	• Transparency • Provenance • Analysis of cascade effects
Identify and document vulnerabilities contained in the product	**Vulnerability Exploitability eXchange (VEX), Vulnerability Disclosure Report (VDR):** lists vulnerabilities that affects or not a product or its dependencies.	• Transparency • Provenance • Analysis of cascade effects
Apply effective and regular tests and reviews of the security	**OSCAL (NIST):** machine-readable representations of control catalogues, control baselines, system security plans, and assessment plans and results.	• Composition • Agile certification based on previous assessments and information • Transparency on requirements evaluated
Ensure an appropriate level of cybersecurity, without any known vulnerabilities		
Secure by default configuration	**MUD:** IETF standard to express device behavior at network layer. MUD can be obtained during the bootstrapping to enforce the recommended configuration.	• Feedback from certification to deployment • Secure by default configuration • Different configurations for different contexts

Design and development

Deployment

Certification

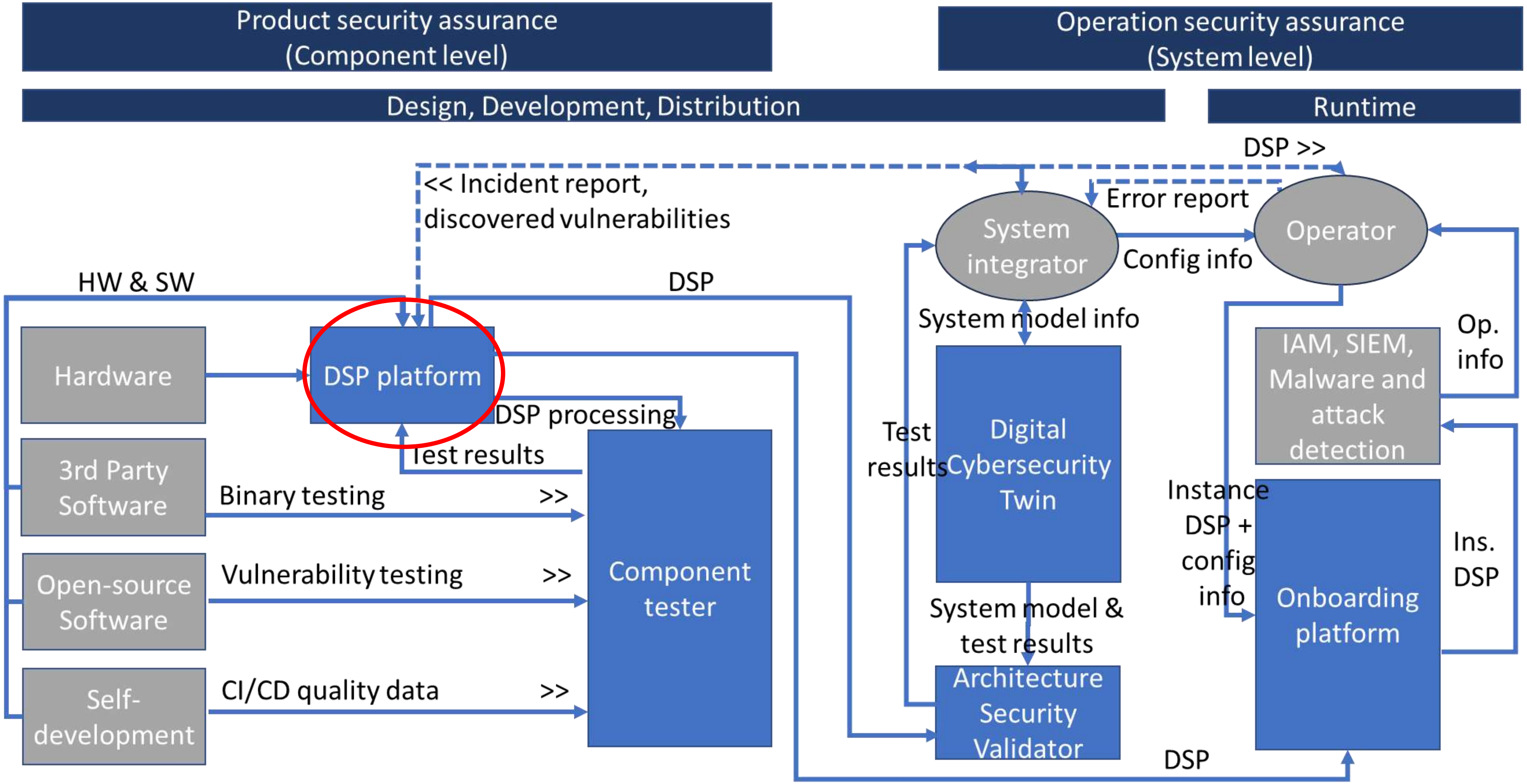
A DSP supporting CRA requirements

Certification

Operation and upgrading

CRA requirement	What the DSP contains to support it	How this information supports it
Address, remediate and disclose vulnerabilities	Threat MUD: NIST document based on IETF MUD to share mitigations associated with vulnerabilities (combined with SIEM, IDS, etc.) VEX, VDR, CTI sharing	• Disclosure of vulnerabilities to the manufacturer and CA → Alert possible recertification • Secure patching/mitigation approved by CA → Maintain security level • Reconfiguration before an update is released (fast actions)
Provide and securely distribute updates		
Apply effective and regular tests and reviews of the security		

The DSP management within the DOSS architecture



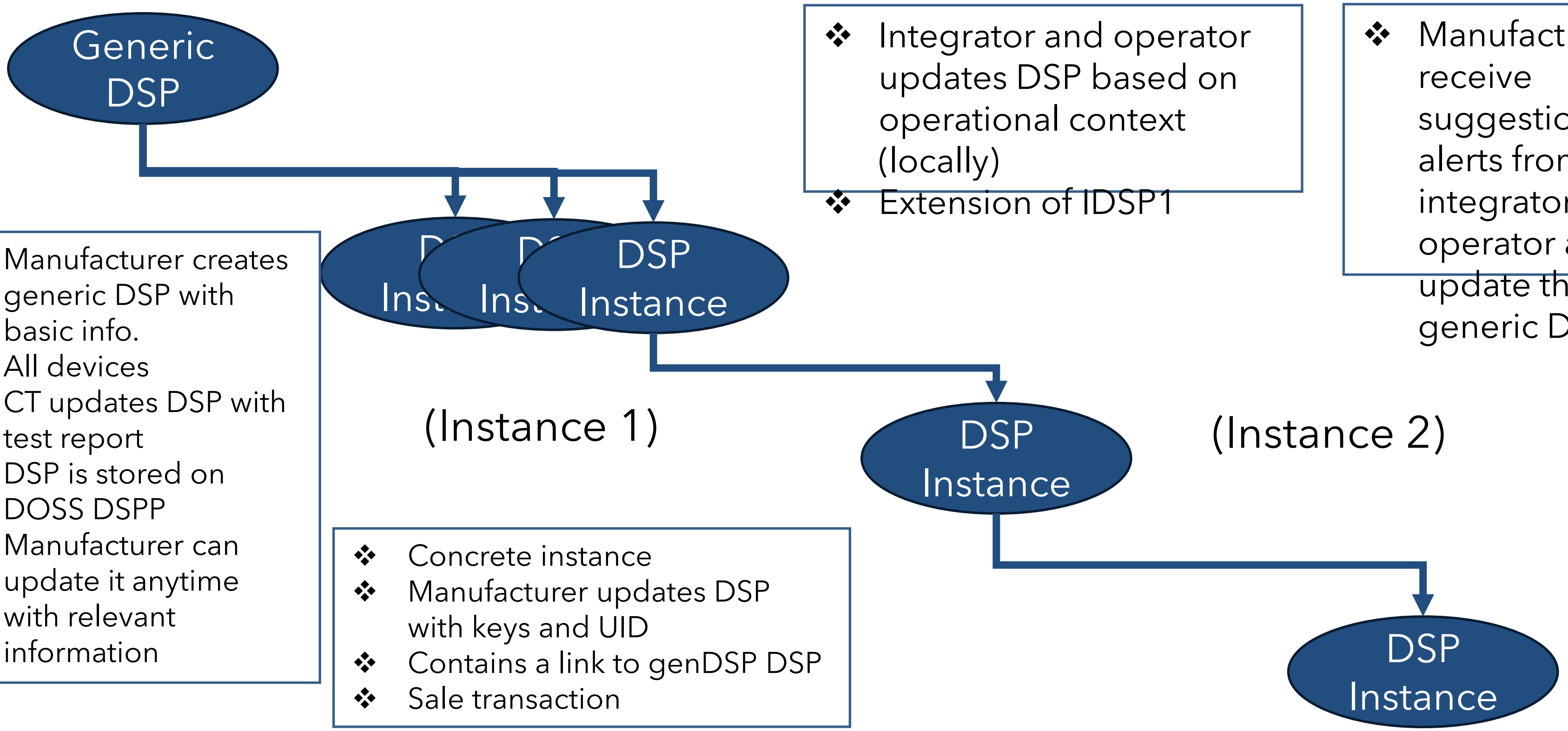
Actor	Manufacturer	Manufacturer	Integrator	Operator
Module	CT		DT + ASV	Security Modules
DSP storage	In DSPP	In DSPP	Local	

Production

Sale

Deployment

Operation



- ❖ Manufacturer creates generic DSP with basic info.
- ❖ All devices
- ❖ CT updates DSP with test report
- ❖ DSP is stored on DOSS DSPP
- ❖ Manufacturer can update it anytime with relevant information

- ❖ Concrete instance
- ❖ Manufacturer updates DSP with keys and UID
- ❖ Contains a link to genDSP DSP
- ❖ Sale transaction

- ❖ Integrator and operator updates DSP based on operational context (locally)
- ❖ Extension of IDSP1

- ❖ Manufacturer can receive suggestions and alerts from integrator and operator and update the generic DSP.

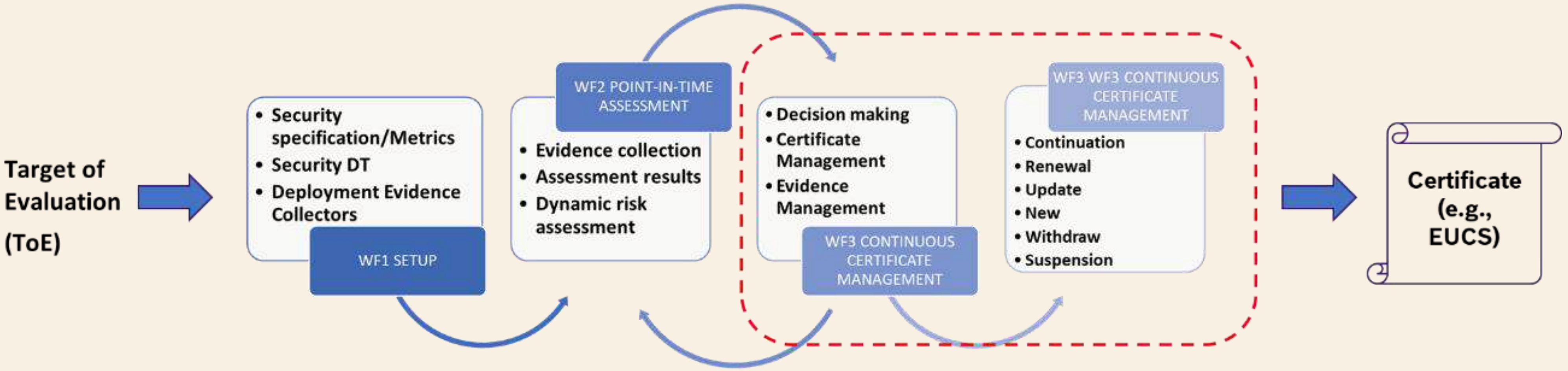
Content	SBOM HBOM VEX, VDR, MUD, threat MUD	Link to Generic DSP + Unique ID keys	Link to Generic DSP Unique ID Keys + Config data

The COBALT concept

- The COBALT project aims to build a multi-disciplinary ICT cybersecurity certification framework with a focus on AI and quantum
  - Certification toolkit to support relevant stakeholders to accomplish their certification tasks with a high level of automation
    - Digital Twin as a service
    - Evidence collectors
    - Risk assessment
    - Certificate decision and management
  - Common Certification Model (CCM) to detail assets and results → interoperability

BOSCH
BOSCH
TÜV SÜD
Fraunhofer FOKUS
ECS
InQbit
RED ALERT LABS IoT Security
UNIVERSIDAD DE MURCIA
UPC
cttc
PRACTIN
eBOS

COBALT CERTIFICATION WORKFLOWS



Target of Evaluation (ToE)

- Security specification/Metrics
- Security DT
- Deployment Evidence Collectors

WF1 SETUP

WF2 POINT-IN-TIME ASSESSMENT

- Evidence collection
- Assessment results
- Dynamic risk assessment

- Decision making
- Certificate Management
- Evidence Management

WF3 CONTINUOUS CERTIFICATE MANAGEMENT

WF3 WF3 CONTINUOUS CERTIFICATE MANAGEMENT

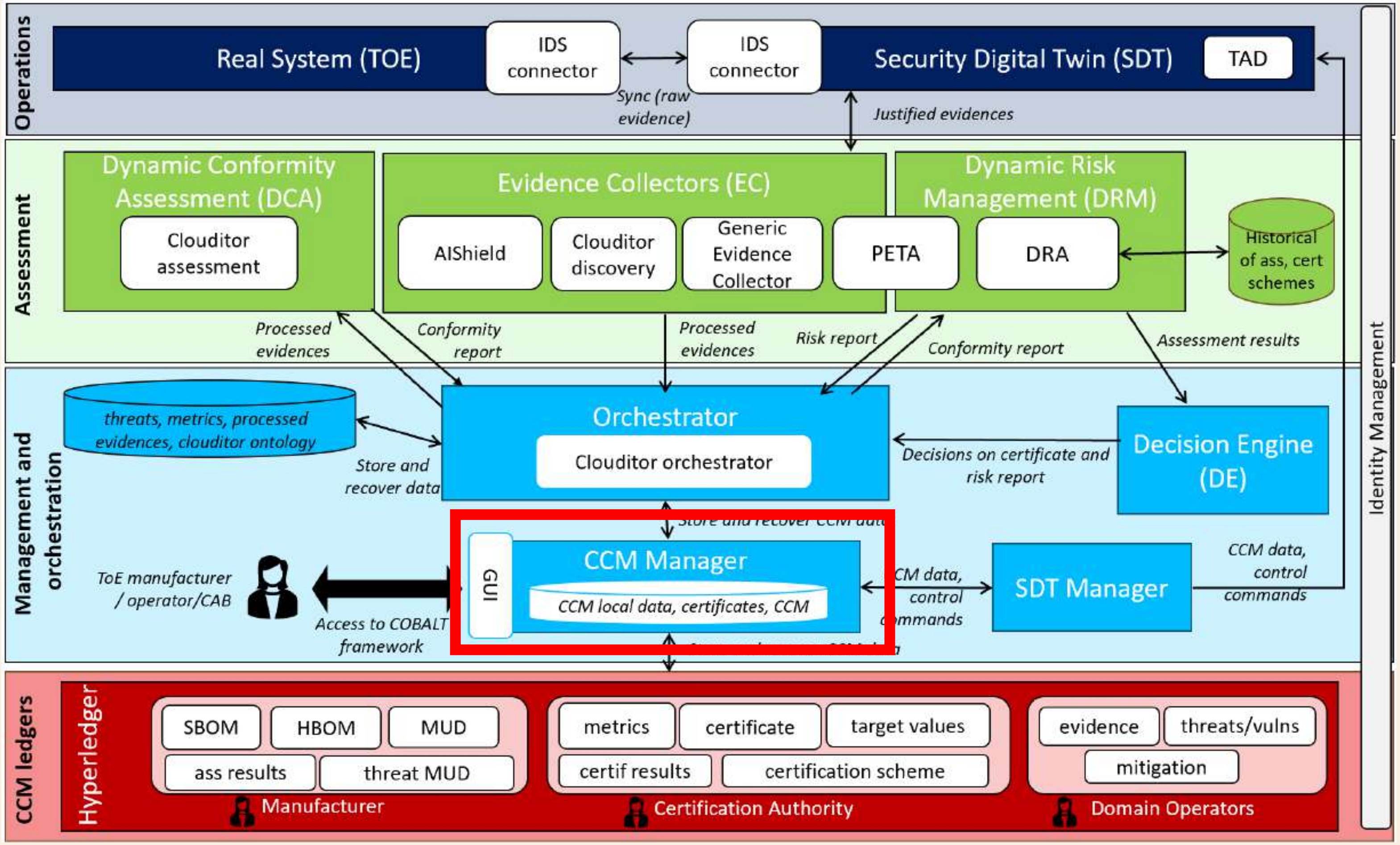
- Continuation
- Renewal
- Update
- New
- Withdraw
- Suspension

Certificate (e.g., EUCS)

OSCAL based CCM

Similar idea to DOSS

COBALT CERTIFICATION FRAMEWORK



KEY POINTS

Despite European efforts, certification and compliance still presents inherent challenges related to

- Cost and time
- Composition and transparency
- Dynamism and lifecycle management
- Context and security level

EU initiatives: DOSS and COBALT

- Certification not as an isolated process after manufacturing, but as a process supporting, and supported by the lifecycle management and the information exchanged throughout its lifecycle to facilitate automation
- DSP/CCM model to centralise all the security relevant information
  - Based on OSCAL to automatise the usage (machine readable)
  - Share, consult and reuse security information
  - In line with CRA

THANKS!!

https://dossproject.eu

https://horizon-cobalt.eu/

DOSS

COBALT