cen CENELEC

European Standardization Organizations

CRA Standards Unlocked: Cybersecurity requirements for Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers

We start at 11:00 CET

Webinar moderator

Lucia LANFRI

Project Manager

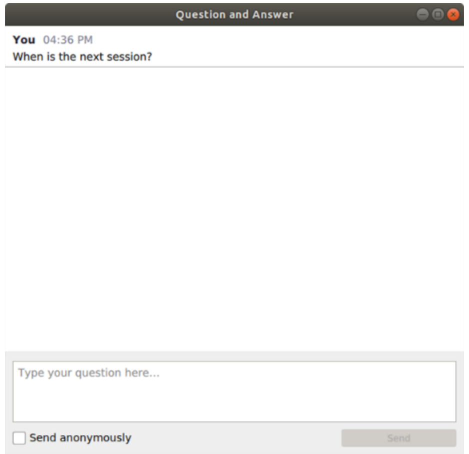
Electrotechnology

CEN-CENELEC

llanfri@cencenelec.eu

Get the most out of the webinar today

- You are muted
- Use the Q&A panel to submit your questions



You 04:36 PM
When is the next session?

Type your question here...

- Talk about us with #training4standards #standards4CRA
  - On X @Standards4EU
  - On Bluesky @cen-cenelec.bsky.social
  - On LinkedIn www.linkedin.com/company/cen-and-cenelec

Your speaker today

Stefane Mouille

Rapporteur CEN/TC 224 WG 17, work item for Line 16: Cybersecurity Requirements for Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers

CRA Standards Unlocked

Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers

Webinar, 2026-02-25

Stefane Mouille

Rapporteur for TC224 WG17 Standardization of CRA Vertical Category 16

Reminder : Essential security requirements (CRA Annex I, part I & II)

1. Security by design
2. No known vulnerabilities
3. Secure by default when placed on EU market
4. Security updates
5. Access control (to PwDE)
6. Confidentiality protectio
7. Integrity protection
8. Data minimization
9. Basic functionality available despite of incident
10. Minimize negative impact around PwDE
11. Limit attach surface
12. Mitigation of incidents
13. Recording & monitoring
14. Deletion of data & settings by end-user

14

Requirements on product

1. Identify and document components and vulnerabilities
2. Address vulnerabilities
3. Perform regular security testing
4. Publish fixed vulnerabilities
5. Implement and practice vulnerability disclosure policy
6. Support 3rd party reporting
7. Ensure secure distribution of updates
8. Dissemination of updates

8

Requirements on vulnerability handling

EC Mandate M/606

European Commission

Mandate
M/606
2025-02-03

CEN CENELEC

CEN/TC 224 WG 17

CLC/TC 47X

CLC/TC 65X WG 3

CEN-CLC/JTC 13 WG 9

CEN-CLC/JTC 13 WG 6

16

"Identity and access control"

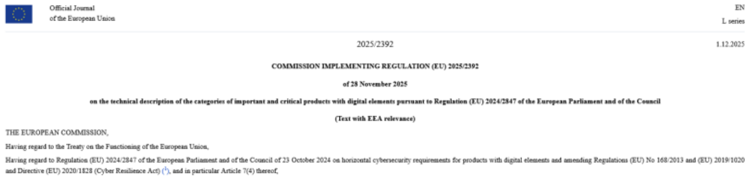
Scope of the line 16

IMPLEMENTING REGULATION (EU) 2025/2392

ETSI

ETSI CYBER

ETSI USER



Official Journal
of the European Union

EN
L series

2025/2392 1.12.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/2392

of 28 November 2025

on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council

(Text with EEA relevance)

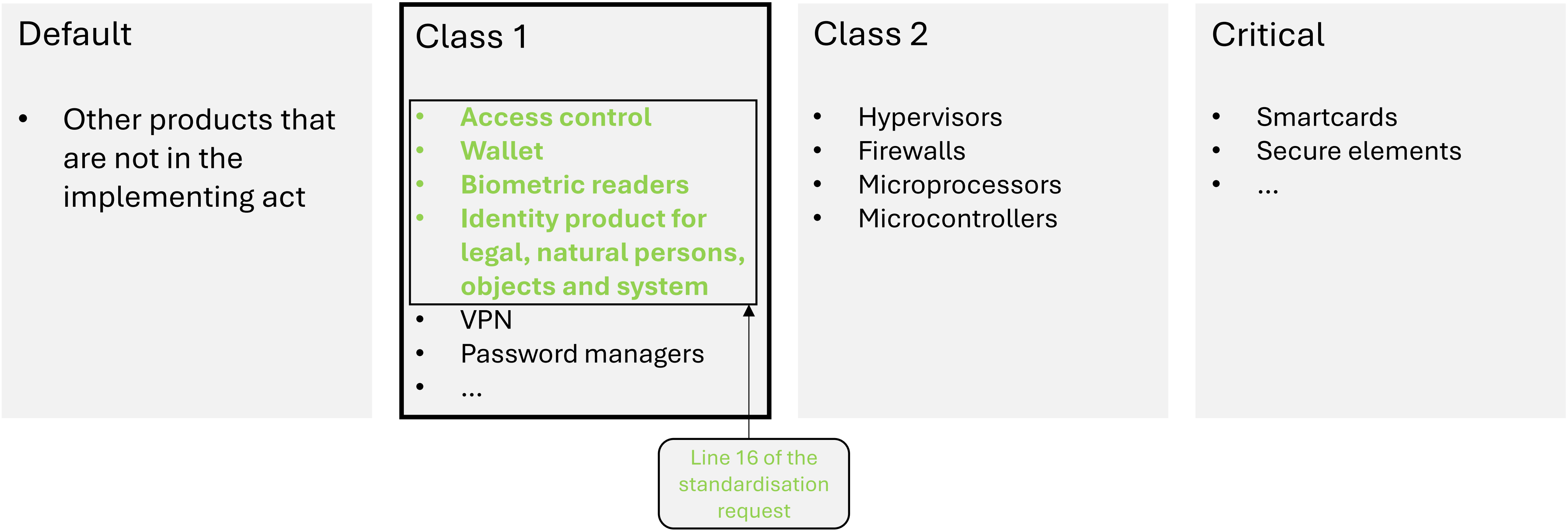
THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [1], and in particular Article 7(4) thereof,

CRA class of products

Categorized products are given in the **Commission implementing regulation 2025/2392**. A few examples are given below:



Default

- Other products that are not in the implementing act

Class 1

- **Access control**
- **Wallet**
- **Biometric readers**
- **Identity product for legal, natural persons, objects and system**
- VPN
- Password managers
- …

Class 2

- Hypervisors
- Firewalls
- Microprocessors
- Microcontrollers

Critical

- Smartcards
- Secure elements
- …

Line 16 of the standardisation request

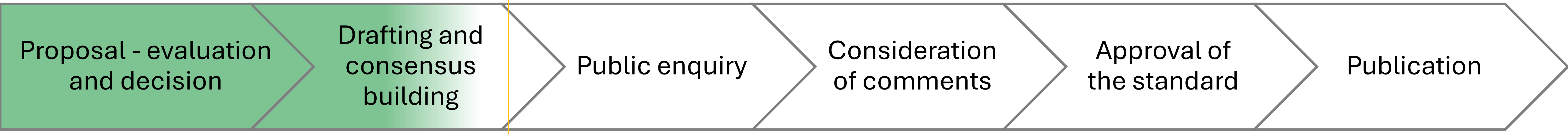
COMMISSION IMPLEMENTING REGULATION (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council

Team: TC224 WG17 Task Force for 16

Name	Organisation
GUIN Marc	TUVIT – Convenor of the TTC 224 - WG 17
FERAUD Alban	IN Groupe
WAJNGLAS Mickael	SPAC Alliance
PLAJH Ivan	Rapporteur line 41b
URMANN Jens	VERIDOS
RIDEAU Alice	ANSSI
CHAPUT Jean	Cabinet Louis Reynaud – CLR Labs
SANCHEZ-REILLO	UC3M
SABADELLO Markus	ELEVAT

Name	Organisation
GONZALEZ Laurent	ANTS – Ministère de l’interrieur
MEISTER Gisela	EUROSMART
PRATONE Davide	HUAWEI
HOVTO Asbjørn	Norway
ANDRUKIEWICZ Elżbieta	Instytutu Łączności
MIELNICKI Tomasz	IDENTONIC
DORNIER Camille	EU Commission
LANFRI Lucia	CENCENELEC
KIP Aylin	AFNOR
LAVATELLI Carolina	Internet of Trust

Progress of this standard by now



Proposal - evaluation and decision

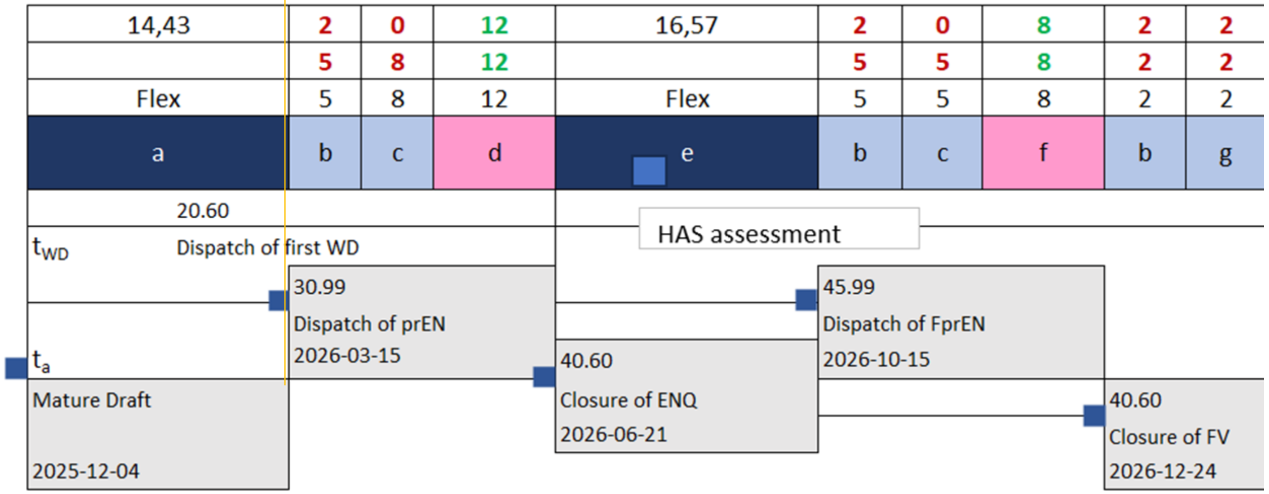
Drafting and consensus building

Public enquiry

Consideration of comments

Approval of the standard

Publication



14,43	2	0	12	16,57	2	0	8	2	2
	5	8	12		5	5	8	2	2
Flex	5	8	12	Flex	5	5	8	2	2
a	b	c	d	e	b	c	f	b	g

20.60
t_{WD} Dispatch of first WD

t_a
Mature Draft
2025-12-04

30.99
Dispatch of prEN
2026-03-15

HAS assessment

40.60
Closure of ENQ
2026-06-21

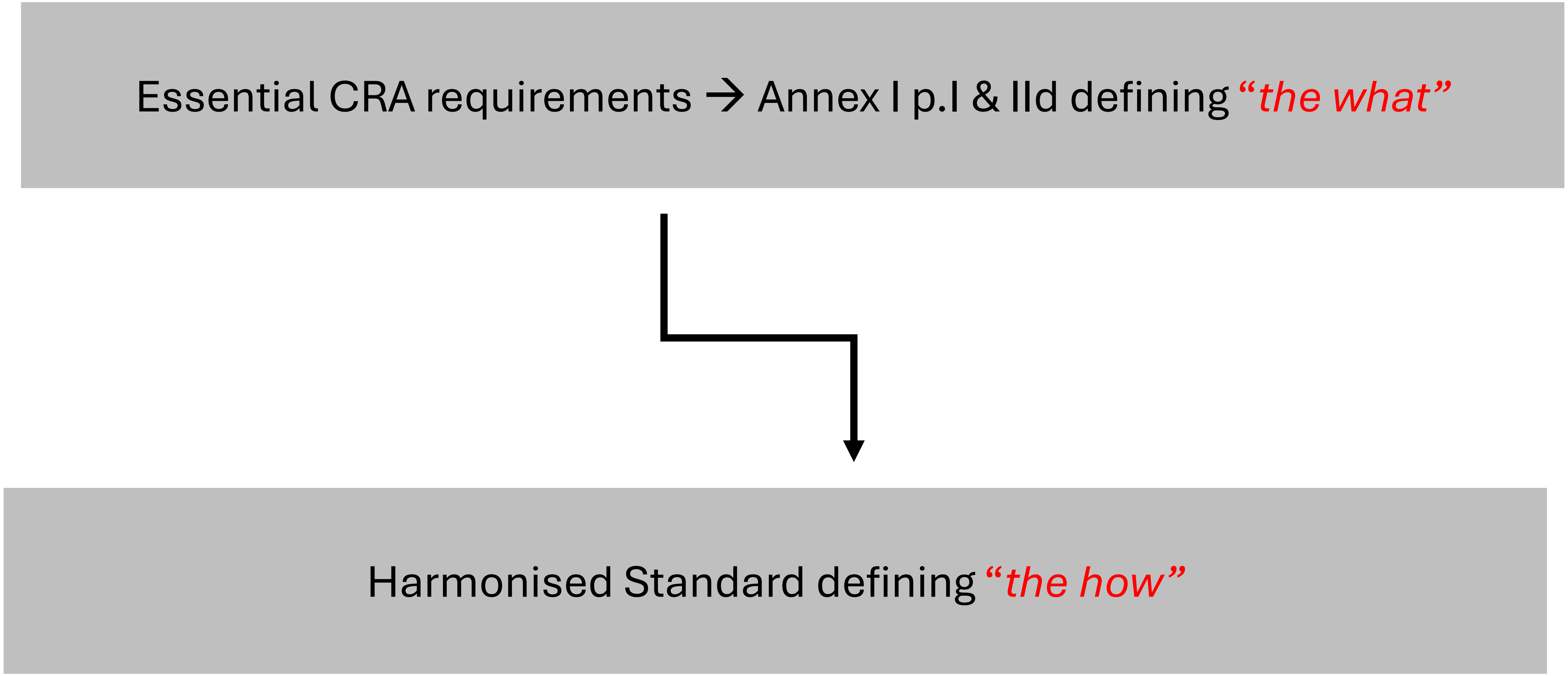
45.99
Dispatch of FprEN
2026-10-15

40.60
Closure of FV
2026-12-24

a	Drafting of prEN
b	Editing
c	Translation and preparation of national publication
d	Enquiry
e	Comments handling/preparation of FprEN
f	Formal Vote
g	TC Proofing

🟦	Internal process
■	Technical work
🟪	Voting

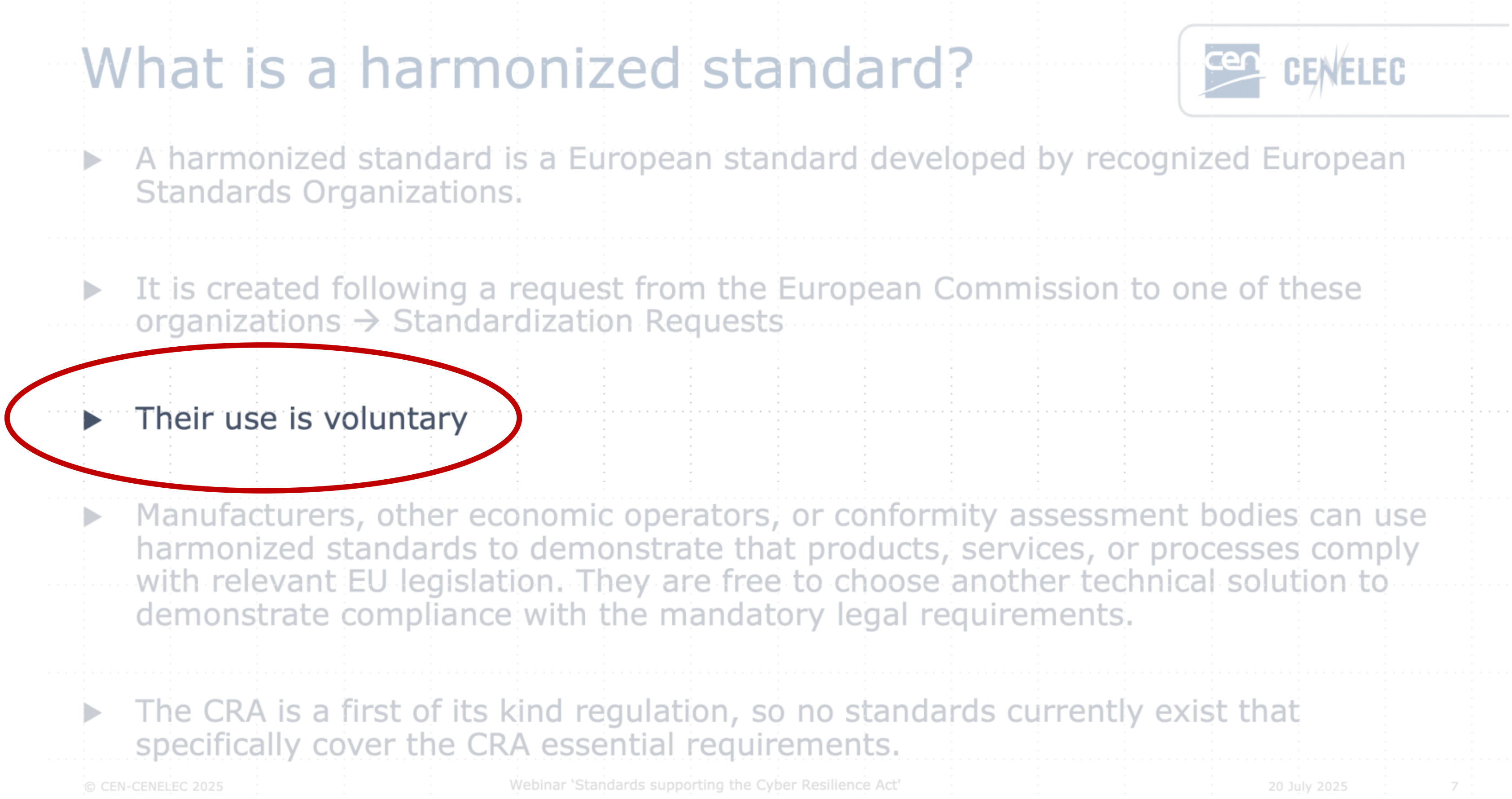
Principles – 16



Essential CRA requirements → Annex I p.I & IId defining *“the what”*

Harmonised Standard defining *“the how”*

Important: **this one will be a CRA harmonized standard**



What is a harmonized standard?

- A harmonized standard is a European standard developed by recognized European Standards Organizations.
- It is created following a request from the European Commission to one of these organizations → Standardization Requests
- Their use is voluntary
- Manufacturers, other economic operators, or conformity assessment bodies can use harmonized standards to demonstrate that products, services, or processes comply with relevant EU legislation. They are free to choose another technical solution to demonstrate compliance with the mandatory legal requirements.
- The CRA is a first of its kind regulation, so no standards currently exist that specifically cover the CRA essential requirements.

© CEN-CENELEC 2025 Webinar 'Standards supporting the Cyber Resilience Act' 20 July 2025 7

Harmonization needs consensus & and validation by the HAS Consultant

Harmonised Standard provides presumption of conformity to the essential cybersecurity requirements only if they are cited at the official journal of the EU

Definition : Category of product 1/2

Identity management systems are products with digital elements that provide mechanisms for authentication or authorisation and that may also provide mechanisms for the lifecycle management of identity credentials of natural persons, legal persons, devices or systems, such as identity registration, provisioning, maintenance, deregistration. These systems include access management systems that control access of natural persons, legal persons, devices or systems to digital resources or physical locations.

Privileged access management software is an access management system that controls and monitors access rights to IT or OT systems and sensitive information within an organisation, including systems enforcing differentiated access control policies for privileged users.

COMMISSION IMPLEMENTING REGULATION (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council

Definition : Category of product 2/2

This category includes but is not limited to authentication and access control readers, biometric readers, single sign-on software, federated identity management software, one-time password software, hardware authentication devices such as transaction authentication number (TAN) generators, authentication software and multi-factor authentication software.

Line 16 is the broder product catagory of the Product classification IMPLEMENTING REGULATION (EU) 2025/2392

COMMISSION IMPLEMENTING REGULATION (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council

Product in the scope and not in the scope

In the scope (Hardware & Software):

- Identity products for legal, natural persons, objects and system
  - Identity Wallets,
  - DTC,
  - MDL,
  - Middleware,
  - National registery,
  - Biometrics data base...
- **Online authentication token**
- **Physical and logical access product for Employees :**
  - Reader, Local unit, Access control and supervision software
  - 2 factor authentication and OTP token
  - High security
- **Privileged access management software**
- **Electronic Identification products (Digital Product Passport**
- **....... and much more ! See appendix A & B of the draft harmonized standard**

Not In the scope (Hardware & Software) and covered by other harmonised standards:

- Chip, Embedded OS, Applets
- PKI products
- Cyber security products needed for securing IT infrastructures
- All other products that are covered by harmonised standards as per the standardisation request Mandate M/606 2025-02-03

Not in the scope

- Anti fire detectors products for organisation

Remote Data Process Services (RDPS):

Remote data processing services of Product are the in-scope of essential cybersecurity requirements if they are essential for a product's functionality, **developed by or for** the manufacturer, and involve bidirectional data exchange

These services must meet the same cybersecurity standards as the hardware and software, ensuring end-to-end security from design to the placing of the Product on the EU market.

The Serveur SDK running on a docker container running on a cloud service of an Mobile Application (such as Digital Identity Wallet) is part of the scope

Structure of the standard

Descriptive / Informative	Part IV : Product context - informative	Informative
Normative	Part V : Requirements	Normative
	Part VI : Conformity assessment against the normative requirements	Normative

Harmonised Standard in a nutshell:

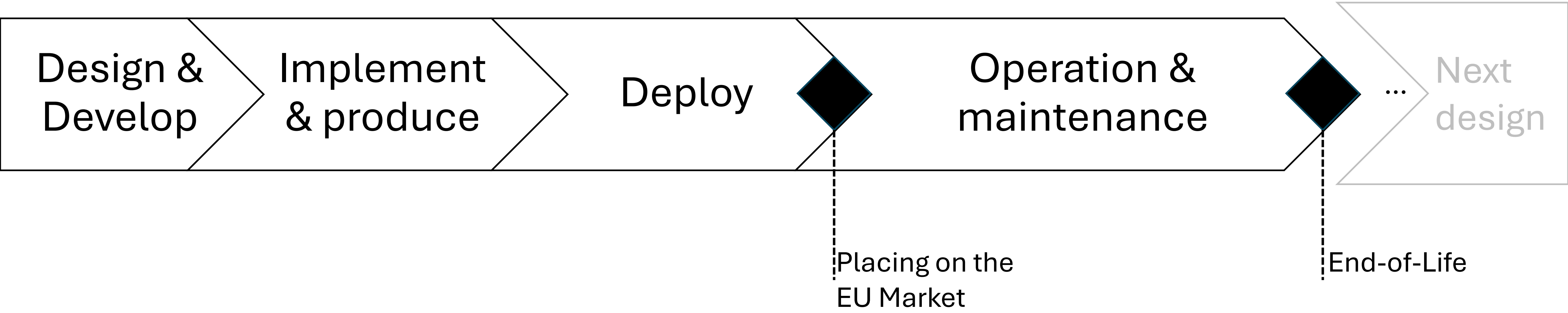
1. Have a clear product description and use case that help in building securing analysis

2. Have a clear cybersecurity product requirements that cover the essential cybersecurity requirements of the CRA – Annex 1

3. Have a clear cybersecurity testing product requirements that cover cybersecurity requirements

4. Comply with the CEN BOSS requirements when establishing a harmonized standard

Life cycle management



Life cycle management – why descriptive?

- There are industry specific Life Cycle Management Systems (LCMS) which
  - Are covering functional parts that are evidently out of the CRA scope
  - Are rather specific to a use case and therefore may require an exception that is still within regulative compliance boundaries

- CRA standard(s) is(are) focused on response to (essential) regulative requirements and manufacturers may have some freedom to accommodate them within their life-cycle systems
  - LCMS must be well documented and auditable
  - CRA requirements from this standard must be consistently implemented and maintained throughout the entire lifecycle of the Product

Reference to normative reference

Normative :

prEN 40000-1-1 (on-going Enquiry), Cybersecurity requirements for products with digital elements - Vocabulary

prEN 40000-1-2:2025, *Cybersecurity requirements for products with digital elements, Principles for cyber resilience*

prEN 40000-1-3:2026, *Cybersecurity requirements for products with digital elements, Vulnerability handling*

What is a Use Case ?

- A Use Case is the combination of
  - A specific Product Environement
  - A Specific User category
  - A Set of Product Functions

- Based on a Given Use Case the manufacturer may :
  - Performe a Security Analisys
  - Use pre-defined Security Profiles provided by the harmonised standard
  - Apply the Cybersecurity product requirements attached to the corresponding Security Profile

Some example of Use Case related to the line 16

UC 1 :

Environnement : Product is connected at public network (internet)

Users: Natural persons, legal persons, devices or systems

Product Function : electronic identification and authentification

UC 2 :

Environnement : Product is connected at private network (intranet , isolated LAN, isolated network)

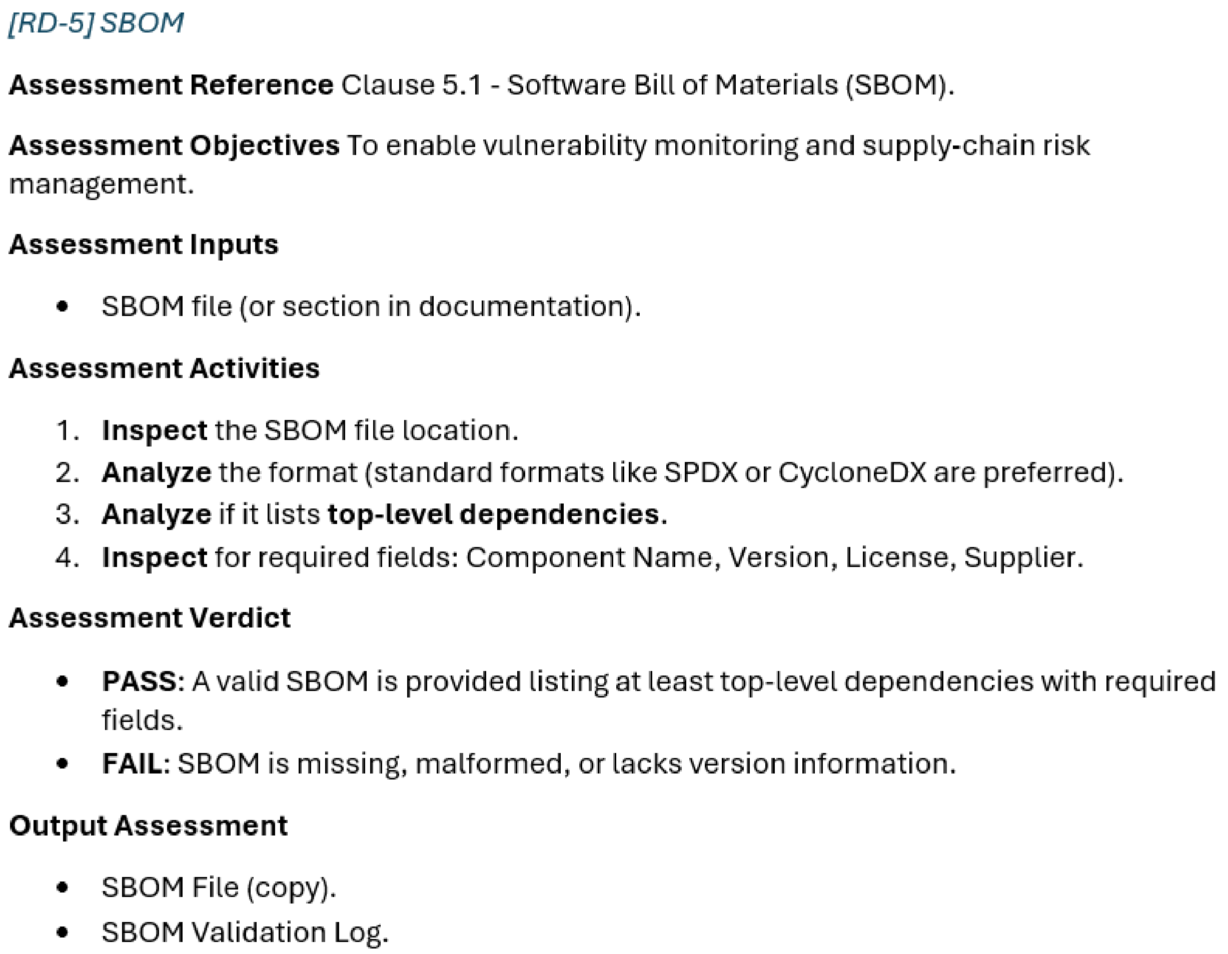
Users : Natural persons working on a given organisation

Product Function : electronic identification and authentification

Work under Process for line 16 !

Example of a product cybersecurity requirements (clause 5) and its testing cybersecurity requirements (clause 6)

I : Inspect
A : Audit
D : Demonstrate
T : Test



[RD-5] SBOM

Assessment Reference Clause 5.1 - Software Bill of Materials (SBOM).

Assessment Objectives To enable vulnerability monitoring and supply-chain risk management.

Assessment Inputs

- SBOM file (or section in documentation).

Assessment Activities

1. **Inspect** the SBOM file location.
2. **Analyze** the format (standard formats like SPDX or CycloneDX are preferred).
3. **Analyze** if it lists **top-level dependencies.**
4. **Inspect** for required fields: Component Name, Version, License, Supplier.

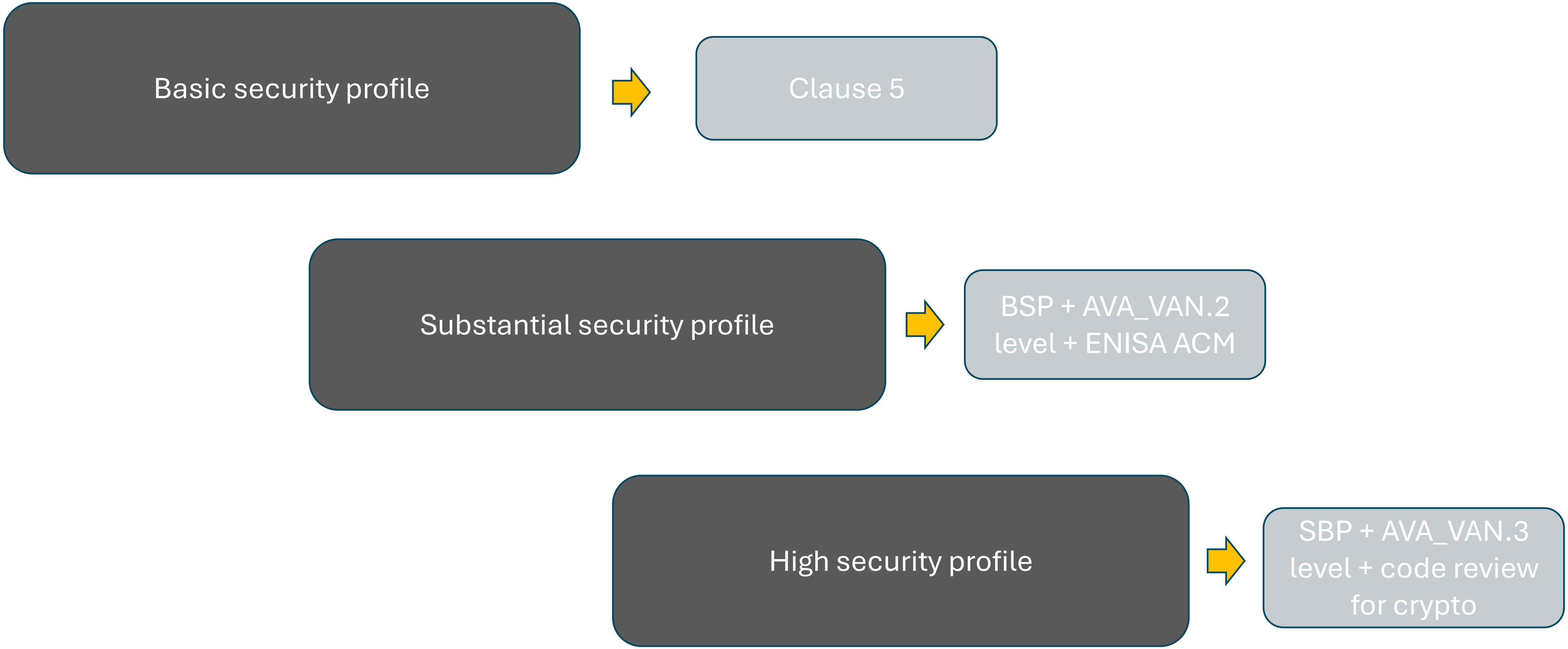
Assessment Verdict

- **PASS:** A valid SBOM is provided listing at least top-level dependencies with required fields.
- **FAIL:** SBOM is missing, malformed, or lacks version information.

Output Assessment

- SBOM File (copy).
- SBOM Validation Log.

Security Profile definition



Basic security profile → Clause 5

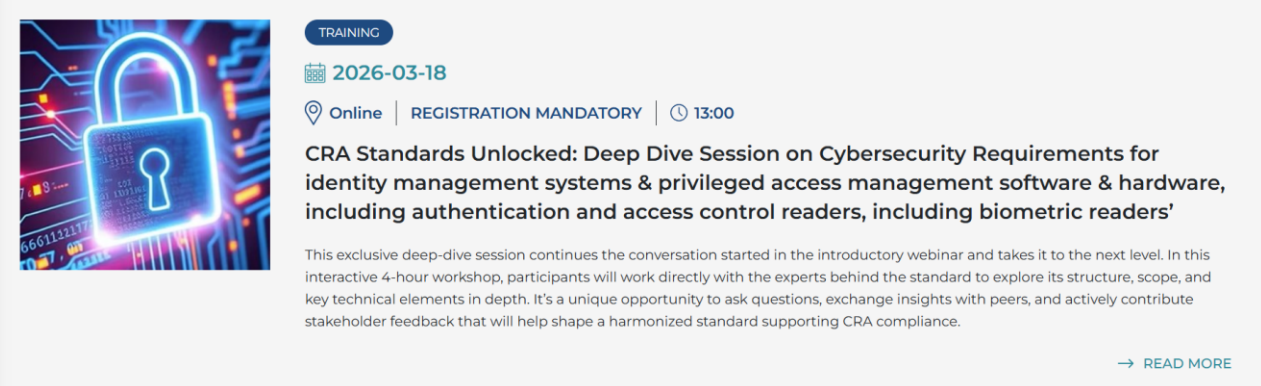
Substantial security profile → BSP + AVA_VAN.2 level + ENISA ACM

High security profile → SBP + AVA_VAN.3 level + code review for crypto

Outlook:
Deep Dive into this standard Scheduled on : 18th of March 2026

What to expect?

- Use cases
- Security Analysis
- Security profile
- Cybersecurity requirements – Clause 5
- Some explanation of some test cases – Clause 6
- Open discussion



TRAINING

2026-03-18

Online | REGISTRATION MANDATORY | 13:00

CRA Standards Unlocked: Deep Dive Session on Cybersecurity Requirements for identity management systems & privileged access management software & hardware, including authentication and access control readers, including biometric readers'

This exclusive deep-dive session continues the conversation started in the introductory webinar and takes it to the next level. In this interactive 4-hour workshop, participants will work directly with the experts behind the standard to explore its structure, scope, and key technical elements in depth. It's a unique opportunity to ask questions, exchange insights with peers, and actively contribute stakeholder feedback that will help shape a harmonized standard supporting CRA compliance.

JOIN OUR WORK!

Accelerating towards completion:

- Field experts welcome to join via national standardization bodies

Q&A

Thank you!

Stefane Mouille