CRA Standards Unlocked

Identity management systems
Privileged access management software and hardware
Authentication and access control readers, including biometric readers
Deep Dive, 2026-03-18

Stefane Mouille
Rapporteur for TC224 WG17 Standardization of CRA Vertical Category 16

Objectives of the Deep Dive session

- Deep Dive on the mature draft harmonised standard presented during the webinar session hold on the 16/02/2026
  - Reply available at : https://www.youtube.com/watch?v=mdldrP3Dq1M
- Open discussion on the mature draft harmonised standard
- Get feedback from the on-line participants
- Get volunteers to join the expert group working at the CEN/TTC 224/WG17
- Deep Dive session is Quiz based !

Quiz number 1

Do you know the standardisation mandate from the EU Commission to prepare the harmonised standard for the CRA?

EC Mandate M/606

Mandate
M/606
2025-02-03

CEN CENELEC

- CEN/TC 224 WG 17 — 16 → "Identity and access control" — Scope of the line 16
- CLC/TC 47X
- CLC/TC 65X WG 3
- CEN-CLC/JTC 13 WG 9
- CEN-CLC/JTC 13 WG 6

ETSI

- ETSI CYBER
- ETSI USER

Quiz number 2

Do you know the reference document describing the technical description of the categories of important and critical products with digital elements?

Implementing regulation (EU 2025/2392)

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

ETSI

- ETSI CYBER
- ETSI USER

IMPLEMENTING REGULATION (EU) 2025/2392

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,

Quiz number 3

Do you know the essential security requirements of the CRA ?

Summary : 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 protection
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

Quiz number 4

Do you know the perimeter of the mature draft harmonised standard?

Summary : 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 protection
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

Based on the prEN 40000-1-3:2026 (PT3)

8

Requirements on vulnerability handling

Quiz number 5

Do you know why a harmonised standard is important for a manufacturer?

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.

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

Quiz number 6

What is the impact for manufacturers if there is no harmonised standard?

Conformity marking and declaration of conformity

- It is not possible to pronounce its conformity marking and declaration of conformity using the assessment procedure based on the module A

- Third party assessment is mandatory

Quiz number 7

Do you know the different product categories of the CRA?

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

Important Class 1

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

Line 16 of the standardisation request

Important Class 2

- Hypervisors
- Firewalls
- Microprocessors
- Microcontrollers

Critical

- Smartcards
- Secure elements
- …

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

Quiz number 8

Do you know the team drafting the mature draft harmonised standard?

Team: TC224 WG17 Task Force for 16

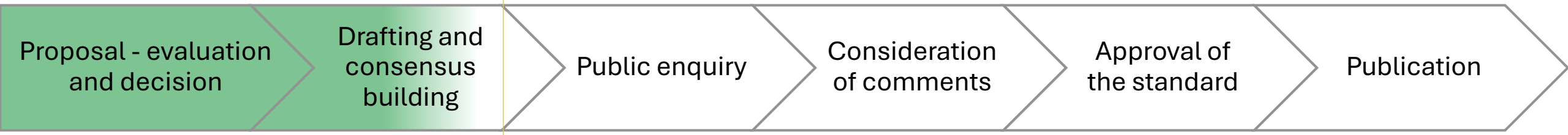
Name	Organisation
GUIN Marc	TUVIT – Convenor of the TTC 224 - WG 17
FERAUD Alban	IN Groupe
WAJNGLAS Mickael	SPAC Alliance
PLAJH Ivan	Rapporteur line 41b
URMANN Jens	VERIDOS
RIDEAU Alice	ANSSI
CHAPUT Jean	Cabinet Louis Reynaud – CLR Labs
SANCHEZ-REILLO	UC3M
SABADELLO Markus	ELEVAT

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

Quiz number 9

Do you know the expected planning of the harmonised standard?

Progress of this standard by now



Quiz number 10

Do you know the technical description of the products covered by this harmonised standard?

Definition : Product categories 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 : Product categories 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.

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

Products 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 database…
- **Online authentication token**
- **Physical and logical access product for Employees :**
  - Reader, Local unit, Access control and supervision software
  - 2 factor authentication and OTP token
- **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

Quiz number 11

Do you know the structure of this harmonised standard?

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

Quiz number 12

Do you know the difference between informative and normative clauses?

Normative vs informative

- Normative Clauses (**Mandatory**)
  - Normative clauses contain requirements that must be followed in order to claim compliance with the standard.

- Informative Clauses (**Optional / Guidance**)
  - Informative clauses provide additional information, guidance, or examples, but are not mandatory.

Quiz number 13

Do you know why the clause 4 (product context) is informative?

Clause 4 - informative

- The harmonised standard can only **define security requirements** and shall not impose any functional requirements

Quiz number 14

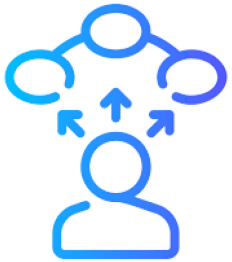
Do you know what is a use case in the clause 4?

What is a Use Case ?

A Use Case is the combination of:

A Specific User category

A specific Product Environement



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

Quiz number 15

Do you know why the clause 4 (product context) is very important even if it is informative?

Clause 4 - objective

- The clause 4 provide some guidance on a pre-set of Use cases

- The Use case allow to bridge :
  - Environments
  - Users
  - Product functions

The clause 4 also allows :

- The Use case link with security analysis and security profiles

Quiz number 16

Do you know the difference between a cyber risk analysis and security analysis?

Cyber Risk Analysis vs Security analysis

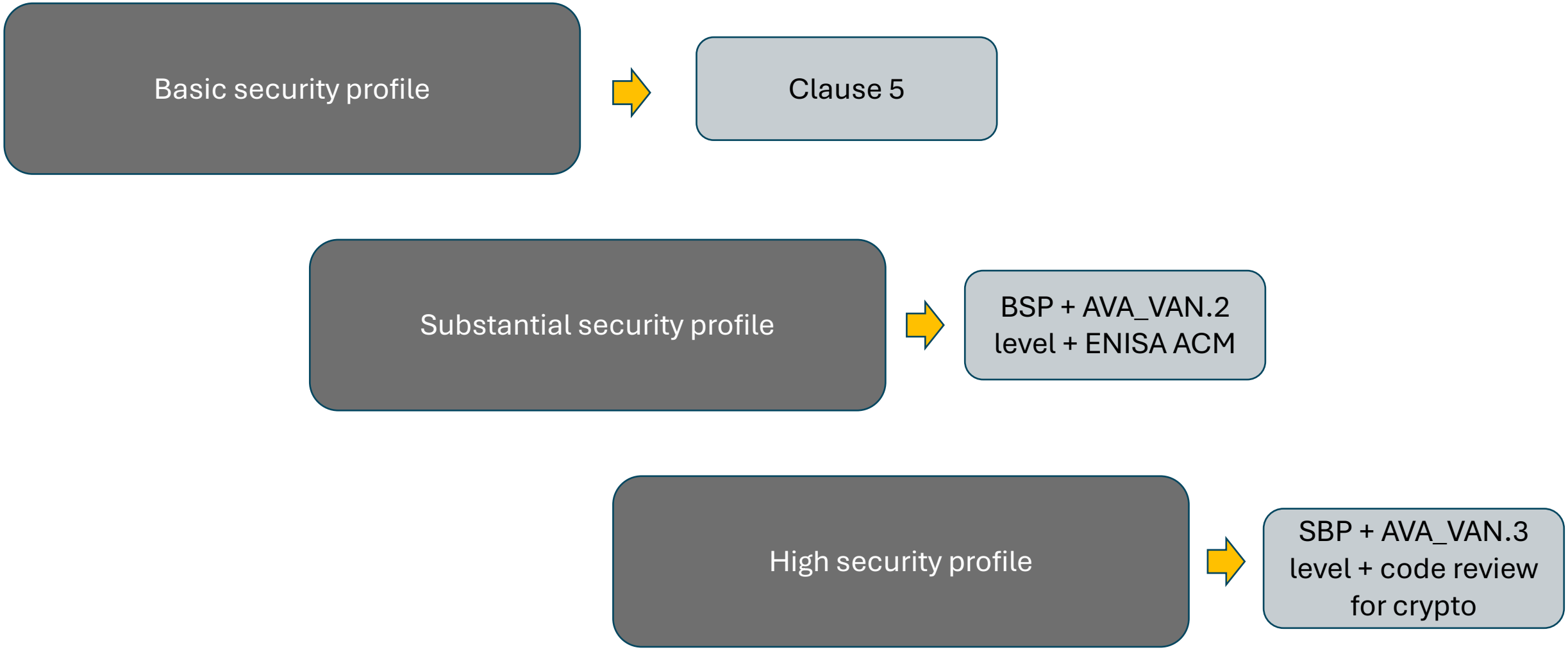
- Cyber Risk analysis is a legal obligation of the CRA (cybersecurity risk assessment referred to in Article 13(2))

- Security Analysis is a technical activity part of the harmonized standard
  - Note the Security Analysis may also help when preparing the legal obligation of the Cyber Risk analysis pursuant to Article 13(2) of the CRA.

Quiz number 17

Do you know the number of security profiles present into the harmonised standard?

Security Profile definition



Quiz number 18

Why are security profiles based on AVA VAN level?

AVA VAN levels benefits

1. Structured and Recognized Security Levels

- AVA_VAN (Vulnerability Analysis) already provides **well-defined assurance levels** (e.g., AVA_VAN.1 to AVA_VAN.5):
  - Low → basic vulnerability analysis
  - Medium → methodical testing
  - High → advanced attack resistance

2. Alignment with an Internationally Proven Framework

- AVA_VAN is widely used in certification schemes (e.g., Common Criteria)
- It is **mature, tested, and understood by labs and regulators**

3. Easier Mapping to Risk Levels (Cyber Risk Analysis)

- The CRA is risk-based. AVA_VAN levels naturally map to:
  - Product criticality
  - Threat sophistication
  - Attack potential

4. Objective and Measurable Evaluation

- AVA_VAN provides:
  - Clear methodology for vulnerability assessment
  - Repeatable evaluation criteria

5. Facilitates Work of Notified Bodies & MSA

- Evaluation labs already know AVA_VAN methodology
- Less need to create new assessment procedures

6. Scalability Across Product Types

- Three profiles based on AVA_VAN can be applied to any product covered by the harmonized standard

Quiz number 19

Do you know the risk registry present into the harmonised standard?

Risk registery

Risk ID	Risk	Risk description
R1	Counterfeit or Altered Identity Artifact	Adversaries succeed by presenting forged, cloned, or altered identity artifacts (digital documents, tokens, ...) that pass verification and are treated as genuine.
R2	Stolen or Revoked Credential Misuse	Illicit use of valid-but-stolen or formerly revoked credentials to authenticate and regain access despite intended controls
R3	Account Takeover	Control of a legitimate account is seized, enabling the attacker to act as the subscriber or admin
R4	Authentication Protocol Downgrade/Misuse	Protocol weaknesses or negotiation gaps allow authentication at lower assurance or without true user presence
R5	Assertion Subversion	Integrity or context of identity assertions is compromised so relying parties accept misbound identities.
R6	Attribute / Entitlement Drift	Authorization posture silently changes through incorrect, stale, or poisoned attributes, roles, or group memberships
R7	Unauthorized Transaction / Action	Operations are initiated or approved without the legitimate user's informed consent
R8	Confidentiality Breach (Identity, Policy & Transaction Data)	Sensitive identity, policy, or transaction data is exposed to unauthorized parties in transit, at rest, or via interfaces
R9	Data Integrity Compromise	Identity, attribute, decision, or transaction records are altered without authorization, biasing outcomes
R10	Cryptography / Key-Management Failure	Weak algorithms, improper bindings, or compromised key material enable forgery, decryption, or cross-service replay
R11	Rogue Device / Service Impersonation	Attacker-controlled endpoints masquerade as trusted clients/readers/services
R12	Administrative Misuse & Configuration Error	Misuse or mistakes by privileged users degrade controls, reduce visibility, or create invisible backdoors
R13	Update & Supply-Chain Compromise	Trusted distribution channels or dependencies are subverted, inserting malicious changes under a veneer of legitimacy
R14	Logging / Auditability Gaps	Insufficient, mutable, or uncorrelated telemetry prevents reliable detection, investigation, or repudiation controls
R15	Service Disruption (Identity & Access-Control Services)	Identity, federation, policy, or enforcement services are degraded or unavailable, leading to denials or unsafe fallbacks
R16	Biometric Presentation Attack (PAD Evasion)	Physical attacks aiming to defeat presentation attack detection and matching, yielding false accept decisions at capture time
R17	Biometric Data Injection (Remote)	Digital synthetic or relayed biometric inputs are fed into the pipeline to impersonate a subject without live presence
R18	Policy Lifecycle Integrity	Central policies and their enforcement remain trustworthy end-to-end. Failures here cause large-scale mis-enforcement.

Quiz number 20

Do you know what are the assets present into the harmonised standard?

Assets

Assets	Definition	Examples
Identity proofs	Canonical identifiers for subjects and their identity records used across the ecosystem	Digital documents, tokens, etc.
Credentials & authenticators	Secrets, factors, and artifacts used to authenticate subjects	Passwords, OTP seeds, cryptographic keys, device credentials
Biometric traits	Captured/latent biometric samples/signals prior to feature extraction	Images, audio, sensor streams
Biometric references & templates	Derived biometric features/templates and any linked metadata used for matching and PAD	
Assertions & tokens	Signed/attested statements about identity, authentication, or attributes	SSO/federation assertions
Attributes	Authoritative attributes and their bindings to subjects	Roles, groups, rights
Policy artifacts	Access-control rules, decision logic, risk signals, obligations, and constraints	
Decisions	Authorization decisions and obligations	
Session state & bindings	Session identifiers, cookies, tokens, device bindings, and continuity data that tie actions to authenticated subjects	
Audit logs	Event records needed for forensics and non-repudiation	Admin/user actions, decisions, failures
Cryptographic keys & credentials	Private/public keys, certificates, key metadata for issuers, and verifiers	
Secure channels	Protected communications and device I/O paths that carry sensitive inputs/outputs	
Software, configurations & code source	Executable code, configurations, and provenance for identity	Images, updates
Lifecycle records	Enrolment/proofing artifacts, issuance/revocation histories, recovery/unlock records, and identity linking/unlinking histories	
Sensitive data stores	Databases, caches, and backups that persist any of the system's assets	Digital documents, tokens, etc.

Quiz number 21

Do you know what are the threats present into the harmonised standard?

Threats

Threat	Related Risk	Threat description
Artifact Forgery	R1	The attacker generates what appears to be a valid digital identity artifact (e.g. an identity credential, SSO assertion, authorization token) without going through the legitimate issuer and presents it to the relying party so it is consumed as authoritative.
Artifact Cloning and Parallel Use	R1	The attacker extracts the full logical content of a legitimately issued credential (e.g. digital identity, mobile wallet credential, etc.), replicates it into a second container or device under their own control, and uses that clone in parallel to the legitimate holder.
Binding Substitution	R1	The attacker modifies or substitutes the subject binding in the credential so that the credential is still “a valid credential” for a genuine subject, but the subject data is now cryptographically/biometrically/holder-wise bound to the attacker instead of the legitimate person.
Stored-Payload Manipulation & Replay	R1	The attacker edits high-value fields (entitlements, eligibility attributes, role, age status, etc.) inside a credential that was originally valid, then replays that tampered payload so the verifier consumes the attacker’s modified claims as truth.
Issuer Impersonation / Fake Issuer Metadata	R1	The attacker stands up or emulates what looks like a legitimate issuer (naming, identifiers, certificate chain presentation, metadata endpoints), and then “issues” credentials to themselves that appear structurally correct and reference a plausible authority, relying on weak trust-anchor validation at the verifier.
Stolen Secret Use	R2	Use harvested passwords, PINs, keys, or device-bound tokens to log in as the subject through standard interfaces
Credential Re-activation via Process Abuse	R2	The attacker regains use of credentials that were legitimately revoked or deprovisioned by abusing still-available operational or administrative processes that restore access without robust re-proofing.
Session Artifact Theft & use	R2	An attacker uses stolen bearer artifacts (e.g., session cookies, refresh tokens, service tickets) captured from endpoints, logs, or memory to authenticate as the subject through normal interfaces without needing the primary secret.
Lifecycle / Revocation Status Falsification	R2	The attacker tampers with or forges lifecycle metadata (issuance timestamp, expiry timestamp, revocation state, suspension flag) so that an identity artifact that should no longer be trusted is still accepted as active and valid.
Use of Lost Device	R2	The attacker gains control of a lost device that still contains an active credential for a subject and is able to use that credential to authenticate as that subject because local protections (biometric/PIN gate, attempt throttling, wipe-on-transfer, hardware binding) are missing or weak.
Recovery Hijack	R3	The attacker uses the account’s recovery / reset / unlock flows (e.g. “forgot password,” “reset PIN,” “rebind device”) and passes weak or replayable recovery checks to set new authenticators and designate themselves as the legitimate controller of the account.
MFA Enrolment Takeover	R3	The attacker tricks or exhausts the real user into approving one high-assurance authentication or enrolment event (e.g. through MFA push fatigue, social engineering, or a spoofed consent prompt) and immediately uses that foothold to register a new second factor, new authenticator app, or new phone number under attacker control.
Adversary-in-the-Middle Rebind	R3	The attacker uses an adversary-in-the-middle or reverse-proxy phishing setup to relay the victim’s entire login flow including password, MFA, step-up, and even biometric checks to the legitimate service in real time and gains authentication to the session
Out-of-Band Channel Seizure	R3	The attacker takes control of the account’s out-of-band verification channel (e.g. SIM swap to hijack SMS/voice OTPs, compromise of the recovery email inbox, compromise of the push-notification endpoint or signing device), then uses that channel to authorize resets, approve step-ups, and rewrite the account’s own recovery / contact / factor info.
Factor Downgrade	R4	The attacker forces or tricks the relying service into accepting a weaker authentication factor or flow than policy requires.
Authentication Downgrade	R4	Adversaries force the use of outdated or vulnerable system feature versions that lack support for modern security controls or device/channel binding, weakening the authentication process
Conditional Access / Policy Control Tampering	R4	The attacker alters or disables conditional access logic (risk-based enforcement, IP/location-based rules, device posture checks, region restrictions, step-up requirements) so that authentication succeeds when it should have been blocked or escalated.

Quiz number 22

Do you know what is the objective of the clause 6 of the harmonised standard?

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.

Quiz number 23

Do you know what is a market surveillance authority?

Market Surveillance authority

- Article 3 (33) ‘market surveillance authority’ means a market surveillance authority as defined in Article 3, point (4), of Regulation (EU) 2019/1020

- Article 13(13) Manufacturers shall keep the technical documentation and the EU declaration of conformity at the disposal of the market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.

Quiz number 24

Do you know the link between the clause 6 and the market surveillance authority?

Market surveillance authority (MSA) control

- Inputs and output elements of the clause 6 can be used as “evidence” during a MSA control
- See fine level defined into the CRA

Quiz number 25

Do you know the Assessment Preparation categories present into the clause 6?

Assessment Preparation categories

TAG	CATEGORY	PURPOSE	EXAMPLES
[PROD]	Product Characterisation	Define what the product is and how it is intended to be used (identity, intended purpose, use case, interfaces, protocols, operational environment).	Product ID/version/target; intended purpose(s); use-case description; users/roles; dependencies; supported interfaces; supported protocols; intended operating environment.
[SCOPE]	Product Composition & Boundaries	Define assessed scope and composition (included/excluded components and assessment boundaries).	Component list; included/excluded modules/features; deployment boundary assumptions; version/build identifiers.
[RA]	Risk & Applicability	Capture risk/threat applicability rationale for the declared use case and environment, including special applicability topics.	Risk assessment report; assets to be protected; threat applicability rationale; RDPS applicability/non-applicability and justification.
[TM]	Threat Coverage Matrix	Demonstrate coverage/traceability between threats, assets, and security functions (or requirements).	Threats × assets × security functions matrix; mapping table showing how threats are addressed.
[DESIGN]	Security Architecture & Security Functions	Explain how the security mechanisms work and what security functions are claimed.	Security architecture description; security boundary/trust model; list/description of security functions and enforcement points.
[CRYPTO]	Cryptographic Specification	Document cryptographic choices and profiles relevant to the product security claims.	Cryptographic specification (e.g., Annex K); algorithms/key sizes; certificate/key lifecycle assumptions; protocol security settings.
[SBOM]	Software Bill of Materials	Provide software composition transparency to support scope, vulnerability handling, and component verification.	SBOM (SPDX/CycloneDX); package/component versions; build provenance notes (if applicable).
[TEST-ENV]	Test Environment	Describe where the assessment runs (platform, versions, topology, dependencies).	Deployment model (single node/cluster); platform/OS version; network topology; supporting services (registry/directory/KMS) and versions.
[CFG]	Configuration	Record the relevant configuration settings that remain set during the assessment.	Enabled/disabled interfaces; selected security profile; policy mode (default-deny/RBAC); encryption settings; configured trust anchors.
[PRECOND]	Preconditions & Initial State	Specify what must be true just before executing assessment activities.	Admin and non-privileged accounts created; system initialised; required certificates/keys loaded; baseline state confirmed; services started and reachable.
[TOOLS]	Required Tools	List the tools used to execute steps and observe outcomes.	CLI/API client; packet capture tool; log collector; scanner/fuzzer; crypto verification tool; custom scripts.
[GUID]	Documentation References/Guidance	Point to authoritative documents used for setup/operation/claims without duplicating their content.	User/Admin/Install guides; datasheet/general description; API/interface specs; referenced standards/profiles; “Doc X, section Y” pointers.

Quiz number 26

Do you know the Assessment Evidence present into the clause 6?

Assessment Evidence

TAG	CATEGORY	PURPOSE	EXEMPLES
[LOG]	Execution Logs & Outputs	Show what was executed	CLI logs, packet captures
[CONFIG]	System Configuration	Show how system was configured	Config files, ACLs
[SCOPE]	Product Composition Evidence	Show included/excluded components	SBOM, component lists
[RA]	Risk/Threat Applicability	Justify selected threats	Threat matrix
[DESIGN]	Architecture & Implementation	Explain how mitigations work	Security architecture docs
[OBSERVATION]	Enforcement Evidence	Demonstrate control behavior	Audit traces, signature check logs
[PLT-CAP]	Platform Capabilities	Show dependent features	Firmware/CPU/security module capabilities
[DOC-REVIEW]	Product Documentation	Demonstrate that the product documentation accuracy	User Guide, Administrator Guide, Installation Guide

Quiz number 27

Do you know if it is possible to re-use some documents or evidences from other voluntary standards?

Evidence from other voluntary standards

- Yes, but the clause 6 shall be respected.
- Note the clause 5 requirements some evidence and re-use of evidence is important

Quiz number 28

Do you know the Remote Data Process Services principle?

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

Quiz number 29

Do you know the voluntary transversal CRA standards?

Reference to informative reference

Informative :

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

Quiz number 30

Do you feel now comfortable to apply this harmonised standard to your important product class I ?

Collective answer in the chat

Quiz number 31

JOIN OUR WORK!

Accelerating towards completion:

- Field experts welcome to join via national standardization bodies

Q&A

Thank you!

Stefane Mouille