

European Standardization Organizations

CRA Standards Unlocked: Navigating smartcards and similar devices & secure element compliance under the Cyber Resilience Act

*We start at
10:00 CET*

Webinar moderator



Els SOMERS

Project Manager

Public Relations

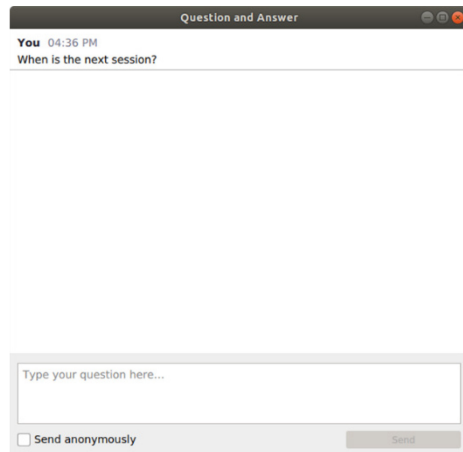
CEN-CENELEC

esomers@cencenelec.eu

Get the most out of the webinar today



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



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

► Introduction

- CRA standards and the standardization request
- What is a harmonized standard?
- Technical work
- Funding opportunities

► Presentation on Smart card and similar devices: focus on the application layer (Rapporteur Ivan Plajh)

Your speakers today



Lucia LANFRI

Project Manager Electrotechnology
Standardization & Digital Solutions



Ivan PLAJO

Rapporteur CEN TC 224
WG 17, work item #41b
CRA standardization
request

- ▶ A **Standardization Request (SReq)** is a formal document issued by the European Commission (EC) to European Standardization Organizations (ESOs)—namely CEN, CENELEC, and ETSI—asking them to **develop, revise, or update harmonized standards** to support **EU policies or legislation**.
- ▶ M/606 “CRA” : [eNorm Platform](#)
- ▶ This request was accepted by CEN, CENELEC and ETSI

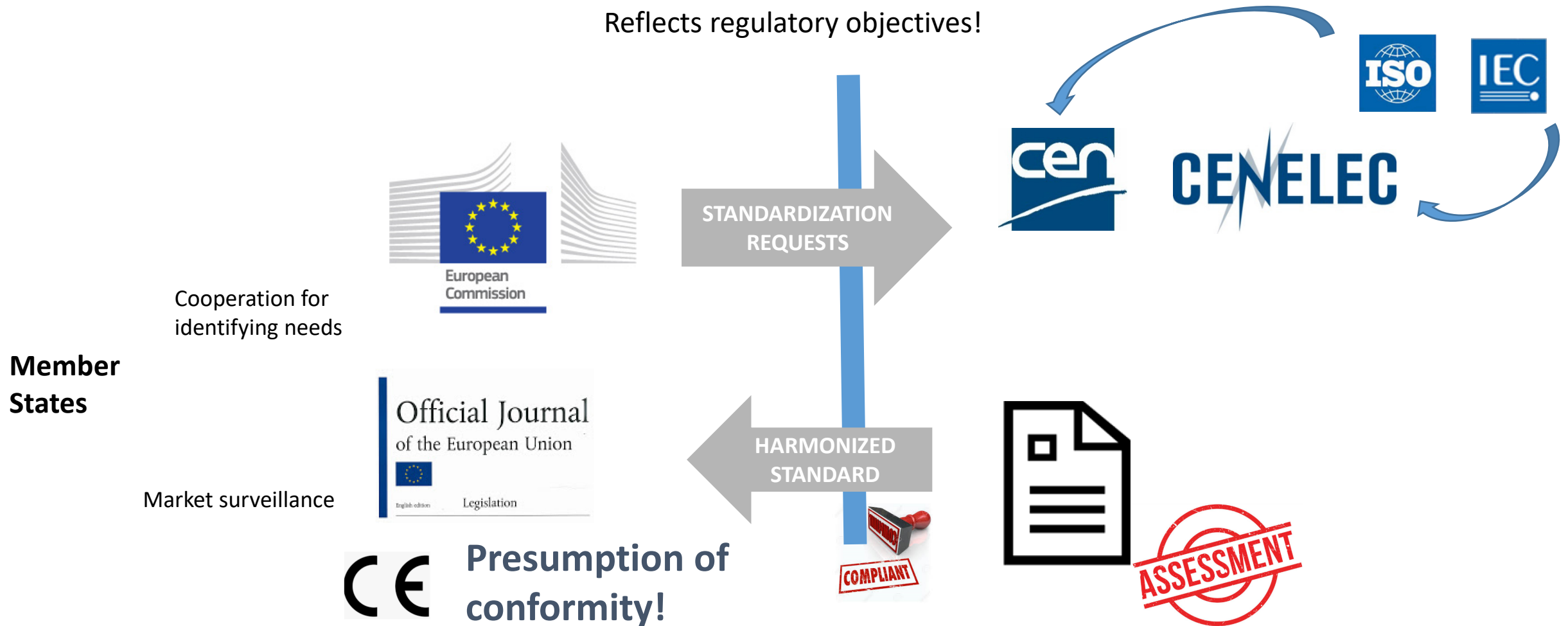
What is a harmonized standard?



- ▶ 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.

Regulation 1025/2012 – Assessment, citation and Presumption of conformity

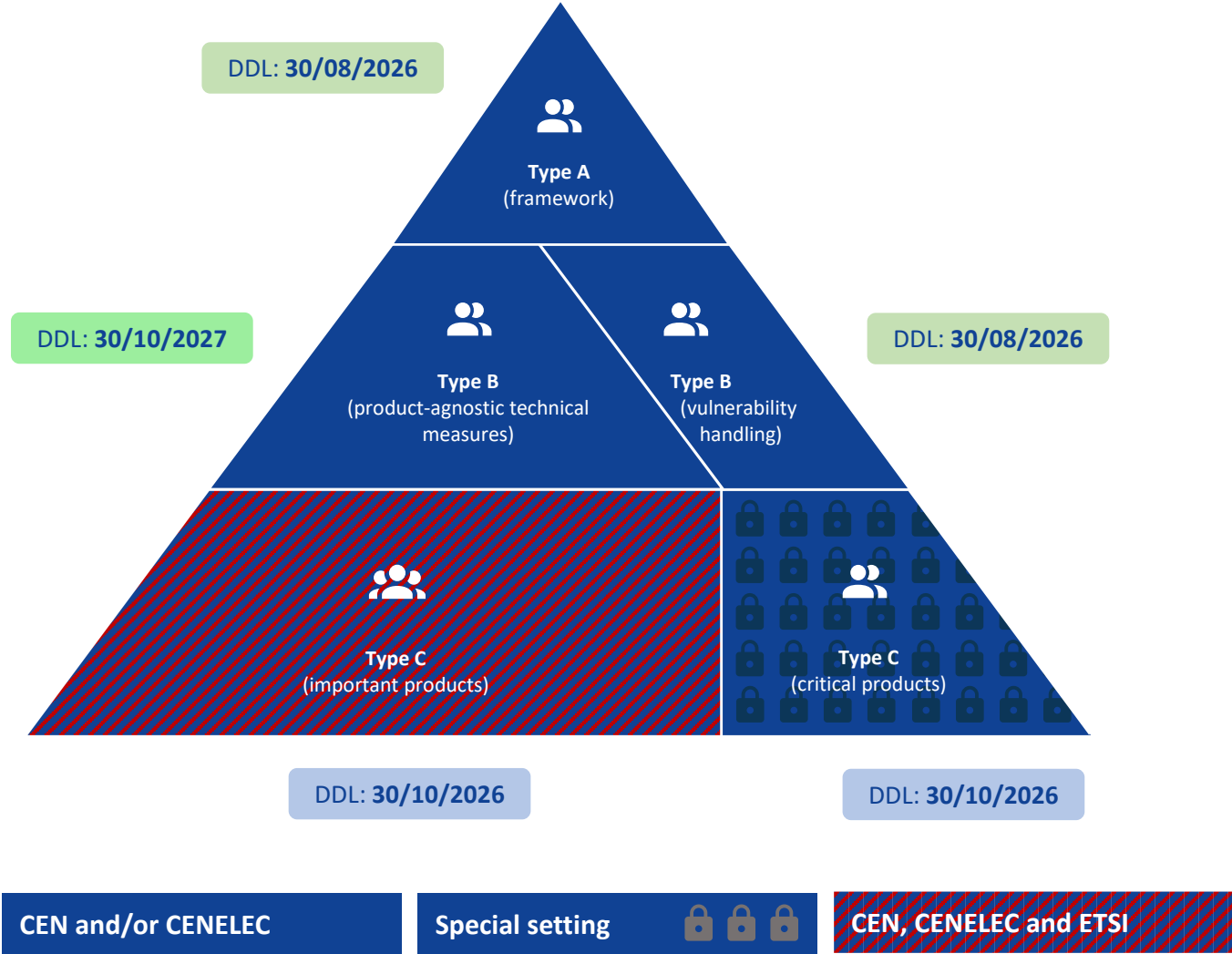
Reflects regulatory objectives!



CRA Harmonized standards

- ▶ Standards requested and work programme
- ▶ What are the timelines?
- ▶ How is the work organized?
- ▶ How to participate?

CRA SReq - deliverables requested



- ▶ 41 topics, 3 'types' of deliverables:
 - ▶ Category "A": horizontal framework
 - ▶ Only CEN and CENELEC
 - ▶ Topic #1 (JTC 13 WG9)
 - ▶ deadline 2026-08-30
 - ▶ Category "B": product-agnostic technical measures & vulnerability handling
 - ▶ Only CEN and CENELEC
 - ▶ Topic #2-15 (JTC 13 WG9)
 - ▶ Deadline 2027-10-30 (except for line 15 - vulnerability handling - 2026-08-30)
 - ▶ Category "C": Important and critical products
 - ▶ CEN, CENELEC **and ETSI**
 - ▶ Topic #16-38
 - ▶ deadline 2026-10-30
 - ▶ Only CEN and CENELEC
 - ▶ Topic #39-41
 - ▶ **Critical products**
 - ▶ deadline 2026-10-30

Correlation between the requested standards on M/606 and the technical committees at CEN, CENELEC and ETSI

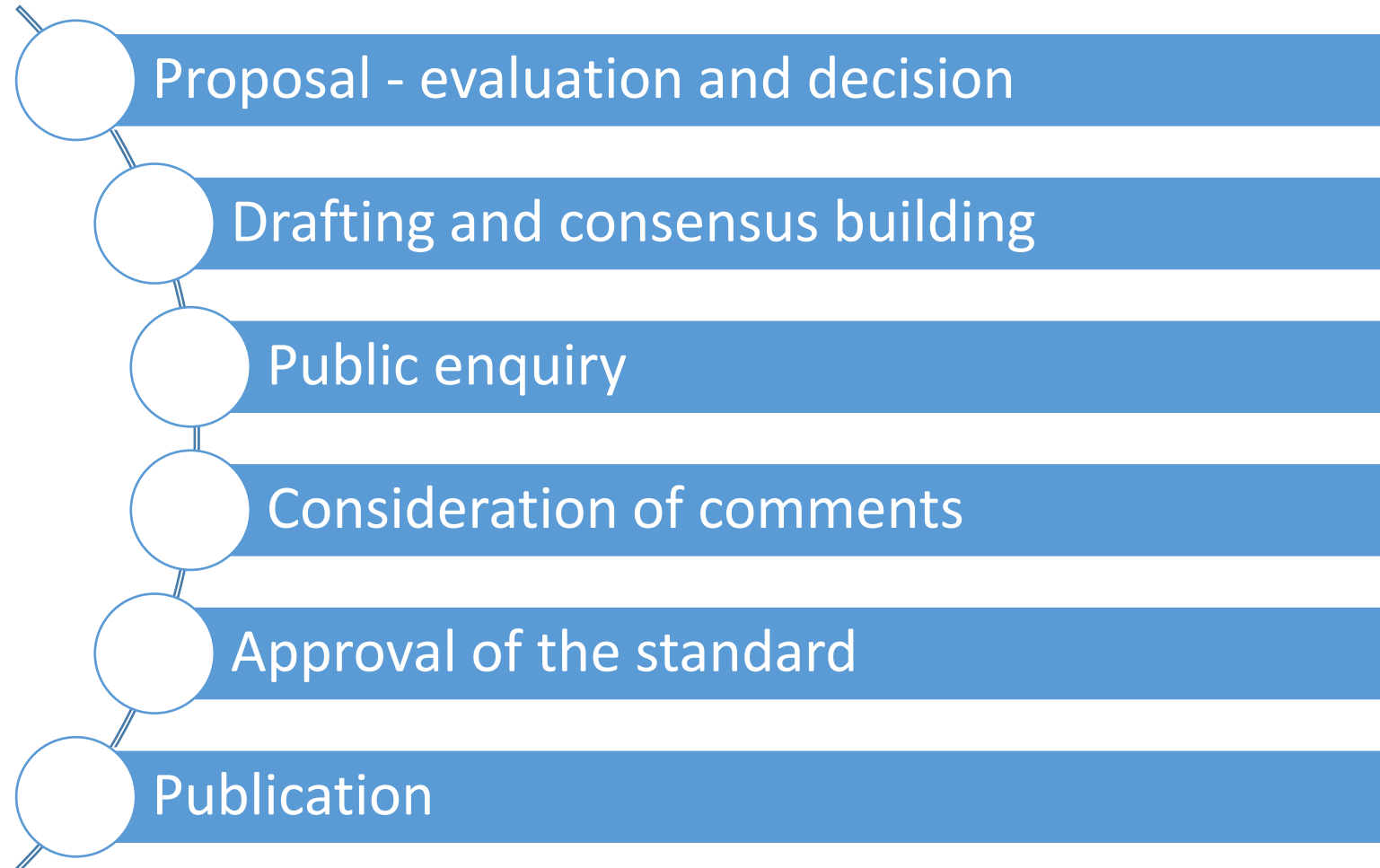


ANNEX I
List of new European Standards to be drafted

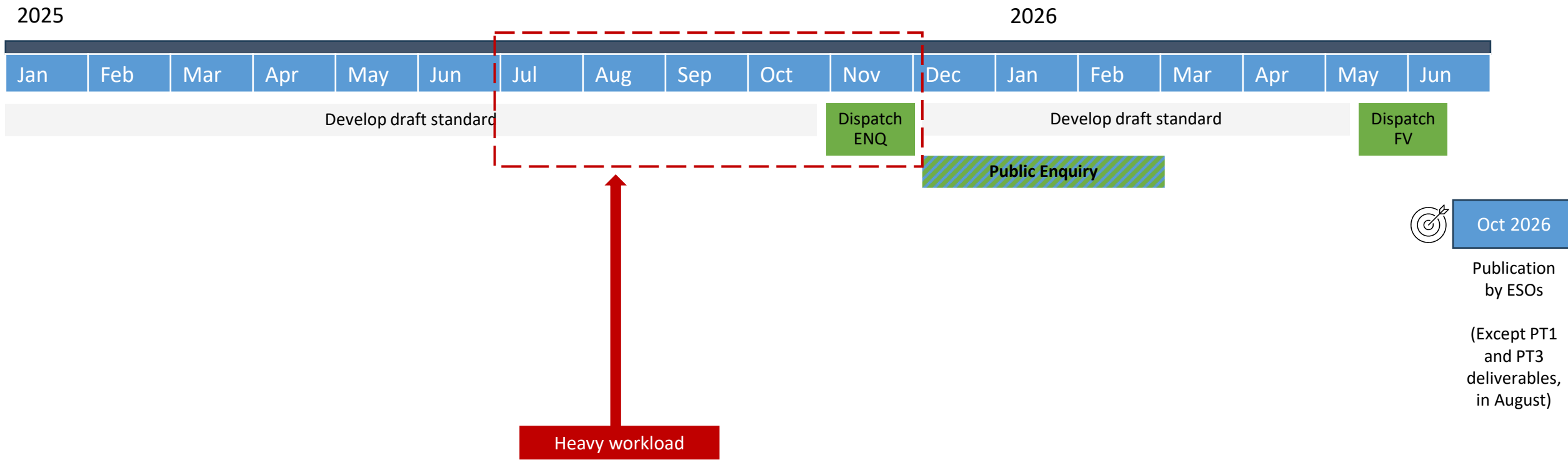
Reference information		Deadline for the adoption by the ESOs
Horizontal standards for security requirements relating to the properties of products with digital elements		
1.	European standard(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks	30/08/2026
2.	European standard(s) on making products with digital elements available on the market without known exploitable vulnerabilities	30/10/2027
3.	European standard(s) on making products with digital elements available on the market with a secure by default configuration	30/10/2027
4.	European standard(s) on ensuring that vulnerabilities in products with digital elements can be addressed through security updates	30/10/2027
5.	European standard(s) on ensuring protection of products with digital elements from unauthorised access and reporting on possible unauthorised access	30/10/2027
6.	European standard(s) on protecting the confidentiality of data stored, transmitted or otherwise processed by a product with digital elements	30/10/2027
7.	European standard(s) on protecting the	30/10/2027

M/606	Technical Committee(s)				
Topics M606 - Annex I	TC ref.	TC title	Standard title	Last realized stage	Deadline for adoption
Line 1: European standard(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks					
1	CEN-CLC/JTC 13 WG 9	Cybersecurity and Data Protection	Cybersecurity requirements for products with digital elements – Principles for cyber resilience	10.99 - NWI - New Work Item adopted	2026/08/30
Lines 2-14 - European standard(s) CRA essential requirements					
2 to 14	CEN-CLC/JTC 13 WG 9	Cybersecurity and Data Protection	Cybersecurity requirements for products with digital elements – Generic Security Requirements	10.99 - NWI - New Work Item adopted	2027/10/30
Line 15: European standard(s) on vulnerability handling for products with digital elements					
15	CEN-CLC/JTC 13 WG 9	Cybersecurity and Data Protection	Cybersecurity requirements for products with digital elements – Vulnerability Handling	10.99 - NWI - New Work Item adopted	2026/08/30
Line 16: European standard(s) on essential cybersecurity requirements for identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers					
16	CEN/TC 224 WG 17	Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment	Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers : criteria to fulfill with the essential requirements from regulation 2024/2487 (CRA)	TC decision taken	2026/10/30
Line 17: European standard(s) on essential cybersecurity requirements for standalone and embedded browsers					
17a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for embedded browsers	PWI - Proposed Work Item created	2026/10/30
17b	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for standalone browsers	PWI - Proposed Work Item created	2026/10/30
Line 18: European standard(s) on essential cybersecurity requirements for password managers					
18	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for password managers	PWI - Proposed Work Item created	2026/10/30
Line 19: European standard(s) on essential cybersecurity requirements for software that searches for, removes, or quarantines malicious software					
19	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for software that searches for, removes, or quarantines malicious software	PWI - Proposed Work Item created	2026/10/30
Line 20: European standard(s) on essential cybersecurity requirements for products with digital elements with the function of virtual private network (VPN)					
20a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for products with digital elements with the function of virtual private network (VPN)	PWI - Proposed Work Item created	2026/10/30
20b	CLC/TC 65X WG 3	Industrial-process measurement, control and automation	Security Profile for products with digital elements with the function of virtual private network (VPN)	00.60 - PWI - Preliminary Work Item created	2026/10/30
Line 21: European standard(s) on essential cybersecurity requirements for network management systems					
21a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for network management systems	PWI - Proposed Work Item created	2026/10/30
21b	CLC/TC 65X WG 3	Industrial-process measurement, control and automation	Security Profile for network management systems (based on IEC 62443)	00.60 - PWI - Preliminary Work Item created	2026/10/30
Line 22: European standard(s) on essential cybersecurity requirements for Security information and event management (SIEM) systems					
22a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for Security information and event management (SIEM) systems	PWI - Proposed Work Item created	2026/10/30
22b	CLC/TC 65X WG 3	Industrial-process measurement, control and automation	Security Profile for security information and event management (SIEM) systems (based on IEC 62443)	00.60 - PWI - Preliminary Work Item created	2026/10/30
Line 23: European standard(s) on essential cybersecurity requirements for boot managers					
23	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for boot managers	PWI - Proposed Work Item created	2026/10/30

How are standards made?

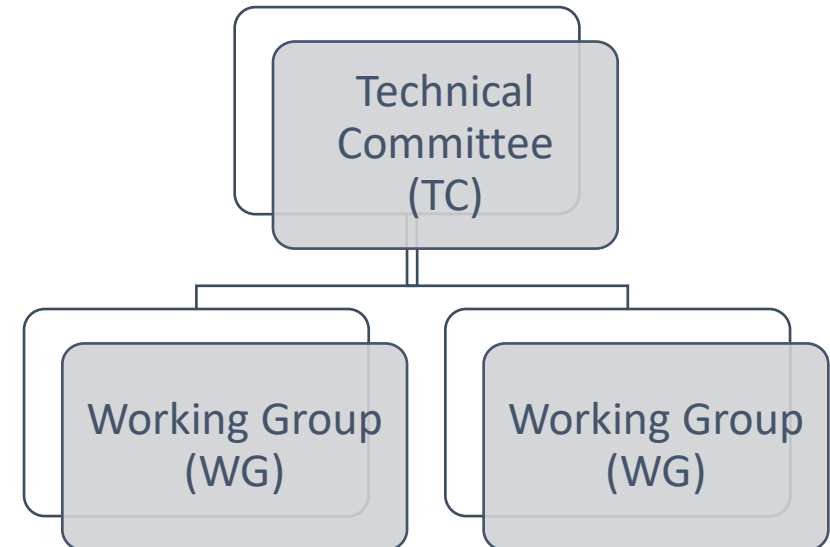


High level expected timeline



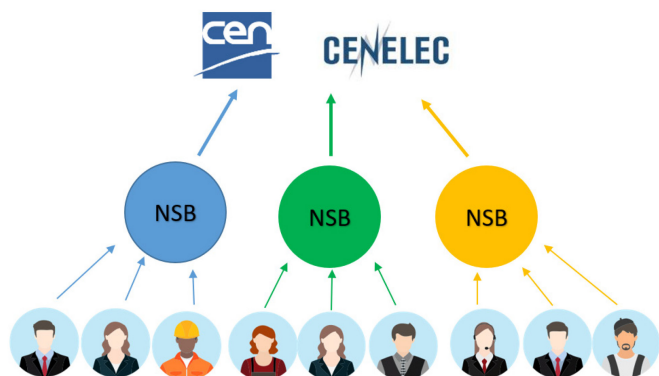
How is the work organized?

- ▶ The standards are developed in Technical Committees (TC)
- ▶ Each TC has Working Groups (WGs)
- ▶ Each WG has a dedicated scope



How to participate?

- CEN and CENELEC Members in 34 countries
- Participation can take place via the national members



Funding opportunity





CYBERSTAND.eu

Apply for Funding to Develop Standards for the Cyber Resilience Act

ENCOURAGED APPLICATIONS

Contributions on harmonised standards to support deliverables in CEN/CENELEC - ETSI Work Programme

8th SSP

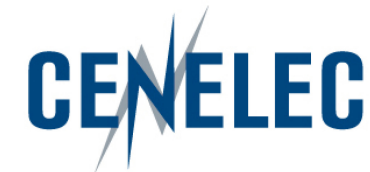
OPEN 23rd Jun

CLOSE 19th Sep **17:00 CEST**

APPLY NOW!



 Co-funded by the European Union



European Standardization Organizations

Thank you for your participation!

Upcoming webinars/events

2025-09-23 - [Workshop 'Cyber Resilience Act and Horizontal Standards'](#) (hybrid/Madrid)

CRA standards unlocked: [CRA Standards Unlocked – new webinar series launched - CEN-CENELEC](#)