Question Report

Disclaimer: the answers to these questions reflect the best understanding of the topic from our experts, they do not represent the official position of CEN and CENELEC nor the European Commission.

1,"Traditional terminal testing is hardware centric. However, the CRA also has requirements related to the remote data processing solution. How is this being handled in the draft standard for hardware devices with security boxes?"

For the moment RDPS has not been addressed. The HWSB can be connected to external systems such as remote management, secure update or servers that process the data coming from the HWSB. A cross-vertical group is currently working on the way to decide which services qualify for RDPS.

2,Does a security box correspond to a zone according to IEC 62443-3-2?,

Hello! Might be interesting to check our past webinar dedicated to the work being done to update the EN IEC 62443-4-1 and -2-4 https://www.cencenelec.eu/news-events/events/2025/2025-09-09-en-iec-62443-to-cra/. Check the recording and presentation that are available on that page. I hope this helps!

3,"How can the results of a CC evaluation be reused for the CRA assessment, e.g. in modules B+C ?"
Evidences used for CC evaluation can be reused.

4,"If a Programmable Logic Controller (PLC) integrates physical chassis tamper resistance and detection mechanisms (per IEC 62443-4-2), and that PLC integrates secure communications and encryption of data at rest, and those encryption mechanisms are supported by an integrated TPM, does this PLC now fall under the definition of ""Hardware Device with Security Box""?"

As described this PLC could qualify as a HWSB. However, PLC main function is to control complex automated processes.

5,Does the standard contain a definition of “sensitive data”?
Data could be two categories.

- Activation data and secrets of the product owner.
- User data (transaction, metering data, ….) associated to the end usage.

To be discussed during the deep dive session.

6,"Do Intrusion and Fire control panels which include tamper enclosure protection & digital elements fall under this product category? There is an ongoing discussion with EU commission & industry, what is the angle of this working group?
To be discussed during the deep dive session.

7,"how CRA and the Machine Regulation MR do works for machine? , Are they mutually exclusive or doubling the need to proof compliance?"

"Hello! Here there's a Q&A 'from the EC, where the interplay with Machinery is described. https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation

8,"The horizontal standard for the SDL has an explicit mention on the need for integrating security by design, including not relying on security through obscurity. How will this vertical standard ensure alignment to the EN 40000-1-2 horizontal standard, specifically in not propagating the security through obscurity perspective embedded in the attack potential computations that are traditionally used in CC? In addition, besides alignment with the horizontal standards, exclusion of a reliance on security through obscurity is critical because the standardisation request includes a clear requirement to integrate the concerns of open source. The standard must not give closed-source solutions free brownie points in the attack potential computation (unlike the EUCC scheme state-of-the-art document on application of attack potential to HWSB), not should open-source vs closed-source be a factor in vulnerability handling timelines (unlike the EUCC scheme guidelines on vulnerability management and disclosure)."

CRA provides transparency about the product security functionalities and its intended use. If you refer to the knowledge of the TOE used in the attack quotations, I would say 3 things:

1) This way of establishing attack quotation is already part of several well-established schemes (not only CC).
2) I am not aware that it is the role of CRA to privilege open/closed source product. And if it was the case this would apply to all the CRA verticals.
3) It is far from free if you consider all the protections needed to protect the TOE.

9,"How will the vertical standards – and the HWSB standard in specific – ensure alignment with the post-quantum transition roadmap from the NIS Cooperation Group, especially on the point of PQC-safe roots of trust?"

For crypto algorithms we refer to an Annex K that will apply to all the CRA verticals explains how to deal with the selection and with agility.

10,"This definition of hardware security boxes seems to be very broad. How to know whether a product falls into this category? For example are EV charging stations HWSBs? They have a lot of sensitive data, crypto, payment, etc.pp"

Hello! The most important is that if the EV charging station includes a direct or indirect logical or physical data connection to a device or network it falls under the CRA. One can comply to the CRA in many ways, the standard being presented by Claire covers what was mentioned in the presentation. You will do a risk assessment for your EV station and see what essential requirements are applicable to this product. You will have to ensure to put all the mitigations and testings in place to cover for that. When a harmonized standard is not enough for this, the manufacturer can find complementary ways to cover for what is missing.

We will come back on this question during the deep dive session.

11,"Thanks for the valuable information. Article 2(4) of the Cyber Resilience Act (CRA) states that the Regulation does not apply to equipment falling within the scope of Directive 2014/90/EU (Marine Equipment Directive – MED).

However, IACS E27 introduces mandatory cyber security requirements for all equipment installed on board ships, including systems and components that are not classified as marine equipment under Directive 2014/90/EU.

In this context, does the Cyber Resilience Act apply to shipboard equipment that is not covered by Directive 2014/90/EU but is nevertheless installed on board ships and subject to IACS E27 cyber security requirements?"

"Hello! Extracted from the Q&A published by the EC: Equipment that falls within the scope of Directive (EU) 2014/90 is listed in the annex to Commission Implementing Regulation (EU) 2025/1533 as regards design, construction and performance requirements and testing standards for marine equipment. However, where components are intended for integration into equipment within the scope of Directive (EU) 2014/90 but those components do not fall within the scope of that Directive, those components may be covered by the CRA (if they are products with digital elements and made available on the market). https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation"

12,Can you please share the slides after the webinar?
Hello! Yes, the slides and recording will be posted here

13,do these requirements must be applied just for HWSB products or do they are general for CRA?,
This specific selection applies to the HWSB. We try as much as possible to describe the similar security functions in the same way via cross vertical specifications.

14,"You showed in the Requirements-examples a reference to the CC assurance components, and also in the assessment example. How does it fit together?"
Each risk profile is associated to a selection of security functional requirements and assurance requirements. The assurance evidences are assessed on their own when appropriate and are used to assess the functional requirements.

15,Can you elaborate in the extended components for the CRA needs?
Extended components have been designed by Enisa to cover aspects of the CRA that were not covered explicitly by the current catalogue. You can find them here https://certification.enisa.europa.eu/publications/cyber-resilience-act-implementation-eucc-and-its-applicable-technical-elements_en

16,"Thanks for the presentation! I have a question regarding the Use Cases (page 21). Could you please develop about future use cases (UC6, etc.)? Do you envision Intrusion and Access Systems falling under this category? Many thanks!"
Yes it is planned.

17,Have you already made a public draft of the standards?
"Only the EN 40000-1-2 and EN 40000-1-3 have entered in what is known as public enquiry. This is the first moment when the standards are publicly available, and can be accessed through our member's portals. Over the next weeks we will launch the ENQ of lines 28-29, 37-39 and 41a and b (refer to www.stan4cra.eu for checking all the topics of the different lines of the SReq

18,Note: [16] ist about Smart meters and not Smart Meter Gateways. The German SMGW-PP ist BSI-CC-PP-0073
Hot topic, will be discussed during the deep dive.

19,is it possible to share the Q&As with us...?,Paul Yu,Paul.Chung.yu@intertek.com,
Yes, we will try to publish the answered questions in the website

20,"Paul, you can copy/paste the Q&A"

21,"Hi maybe as a feedback would be nice to consider a guideline based evaluation for CRA, I think this is much more efficient and concrete than CC / EUCC evaluations, and any links to certification have very specific terminology which shouldn't be known by anyone not working with it.
"Hello! The European Commission (EC) sometimes releases guidelines, and they are in is the best place for developing this kind of documents. Perhaps this could come in the future as a part of the CRA Expert Group (EG) set by the EC. If your company is having a seat at the EG, could be mentioned there

22,"On the slide with the Product Requirements you mentioned that certain requirements are already covered by the implemented Security Box.
When we talk about certification of the product: Did you address the end of the certification of the Secure Box as part of the product and the consequence to the certification of the product?"
Not sure to understand the question.

23,Thank you for the interesting session :)