Webinar of 2025-10-13

Webinar 'CRA Standards Unlocked: Deep dive session on the draft standard focusing on the application layer of smartcards, similar devices & secure element compliance under the Cyber Resilience Act'

1	Is the use of hardware-based secure storage such as a Trusted Platform Module (TPM) mandatory for protecting encryption and decryption keys, or is a software-based solution sufficient to meet the essential cybersecurity requirements?	This question is not strictly related to the deep-dive webinar topic, which was about applications on a Secure Elements, smart cards, similar devices. Furthermore, precise answer cannot be given without knowing details about the product or a use case or overall security requirements and if the product is in a default, important (1 & 2) or critical category. Generally, protecting keys with TPMs, different forms of the Secure Elements (SE, such as integrated or embedded), Trusted Execution Environment (TEE), Secure Encalves, Strong Boxes, or even by specific techniques how to write FW/SW on a microprocessor or microcontroller that may not be equipped with any of these - is a meaningful measure. Depending on the use case, CRA category and additional security requirements - one or multiple may be required.
2	What is the authoritative source for agreed cryptographic algorithms?	This question is not strictly related to the deep-dive webinar topic, which was about applications on a Secure Elements, smart cards, similar devices. The source for the Agreed Cryptographic Mechanisms is here: https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en While it is unclear what is meant with 'authoritative source', it is clear that these guidelines, which are supporting the EUCC scheme, come from ENISA / European Cyber Security Certification Group, Sub-group on Cryptography.
3	Good afternoon, i work for a company that produces industrial floor cleaning machines and	No, this kind of a machine cannot be considered as a Secure Element - but it can have none, one,

	one of them is a self-driving robot. At the moment all the data collected by the sensors are elaborated locally on the machine computer but in the future, there will also be the possibility to exploit a cloud-based elaboration method for bigger maps. The data inside the machine are encrypted and only the manufacturer can access them. There are currently no authentication methods on this platform. Given the premises can this kind of machine be considered an SE and if not, what are the key steps to make it CRA compliant	or more secure elements embedded. The Secure Element consists of at least one application and an underlying platform that consists of two further components: Secure IC and execution environment. These Secure ICs are rarely bigger than a couple of square millimetres and their intended purpose is not comparable to one exposed in the question.
4	Thanks for your good overview. As we share the #41 (smartcards/similar devices, secure elements) between TC224 and TC47X. As critical products need to go for 3rd party assessment, do you foresee any other option for assessment with the hENs of TC224 for #41?	Third party assessment is to happen if a manufacturer of an application on the Secure Element decides to use this harmonized standard, or their own process. The special case - achieving the presumption of conformity along with EUCC assessment and certification - does not void the third-party assessment of the CRA essential requirements - they need to be either already present or added to Security Target or Protection Profile. Basically, any of these 3 options (CRA assessment via harmonized standard, manufacturers own request, EUCC Security Target / Protection Profile) requires 3rd party effort.
5	The CRA states that the product should be vulnerability free. What does this exactly mean, all Vulnerabilities (also low risk) or only exploitable vulnerabilities?	Within the CRA regulation: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng#tit_1 There is no explicit request or a formulation that a product should be vulnerability free. The Annex I, Part II is rather precise about vulnerability handling.
6	What is the difference between the application of Art. 8 (1) and Art. 27 (9) with respect to the obligation to use a EU cybersecurity certificate?	The question is generic and may be applicable to more than just an application on a secure element. Following should not be considered as a correct legal interpretation of the CRA regulation - it is merely my, maybe oversimplified interpretation of what I read from these two articles: Per Art. 8(1) the Commission may adopt delegated acts which would force mandatory certification for certain critical product categories

		(Annex IV). The mandatory enforcement may be interpreted from the "...are to be required to obtain a European cybersecurity certificate at assurance level at least 'substantial..." formulation. Per Art. 27(9) the Commission may adopt delegated acts by which, the manufacturer who would choose to use a certification scheme, could get the certificate, which would remove the need for certain third-party conformity assessments. This Article/clause sounds somewhat similar to Art.8 (1) but it covers more products (beyond Annex IV) and it also seem to be less mandatory - which may be concluded from interpreting the "...that can be used..." part of the 27(9)
7	How to handle public-facing audio/video streams (broadcasts): Do they require encryption in transit?	This question is not strictly related to the deep-dive webinar topic, which was about applications on a Secure Elements, smart cards, similar devices. Generally, this may depend on the use case and several other specifics.
8	For air gapped devices (e.g. non internet facing applications), how automated security updates can work?	Logically, fully air-gapped devices cannot be automatically updated, this is why CRA Regulations Annex 1(2)(c) uses 'where applicable' formulation.
9	Is CRA also or will mandate maintaining Cryptographic- Bill-of-Materials (CBOM) and AIBOM ?	Yes, per Annex I, Part II, (1), SBOM is required.
10	In the CRA, a SE is classified as a critical product (Annex IV). "How to demonstrate conformity? Critical products require a certification following a European cybersecurity certification scheme (Article 32(4) CRA)." [BSI TR-03183 section 3.8.4]. In the presentation (slide 10), the Assessment according to this standard is the first path to CRA compliance and, on slide 58, it's clearly written: ""CRA compliance does not mandate any type of security evaluation & certification. Would you clarify what seems to me to be a contradiction, please?	For an application on a Secure Element, CRA conformity can be achieved via security assessment, which is not the same as evaluation & certification. There are two types of a security assessment: - by this harmonized standard - by manufacturers own specification The third way would be - to perform EUCC security evaluation and certification; this requires the coverage of the responses to CRA essential requirements, which may cover the scope beyond the ToE (Target of

		Evaluation) that is needed for the EUCC evaluation and certification.
11	In IEC 62443-3-3, we have system (interconnected devices as an example). Does CRA applies to individual products within the system or at the system? Different components (individual products) inside the system can have different product lifecycle such as their cybersecurity lifecycle support. In this case, how can we address the security posture of the entire system in a sustainable way? Does system level mitigations accepted, or remediation is the only accepted solution in CRA?	While a manufacturer of a composed product (in this context - a product with digital elements that embodies one or multiple other digital product with digital elements) must ensure CRA compliance for the entire product, singular and precise answer may not be possible - as there are multiple options, some of which are related to the explanation what placement on the EU market means and what are the specifics of the value chain behind his product - but also if the foreseeable use finds place in areas that are covered with other regulations or directives (such as Automotive, Maritime, Aviation, ...)
12	Will CRA also specify a transition timeline from conventional cryptography to Post Quantum Cryptography (PQC) ?	The CRA Regulation is not covering any specific type of cryptography or algorithms. Other documents may be relevant for that context.
13	Maybe adding to the other question: if the lifetime of an SE or a product with embedded SE would extend into the potential "quantum age", would it be fair to assume that the risk assessment has to include a QC-based attack and also measures how to mitigate this?	This is a good extension! The CRA regulation itself does not provision for such assumption. A manufacturer of an application on the Secure Element (which was in scope of this webinar) would need to decide and provide evidence weather the quantum cryptolytics is a threat or not, from current point-in-time perspective. If the quantum cryptolyitics becomes the threat during the lifecycle of the application on the SE or within the period defined by the CRA regulation - the manufacturer cannot avoid the responsibility to act and handle vulnerabilities when quantum or any other threat that was not relevant at the moment of the placement in the market - becomes relevant. Factually, the resilience isn't to be proven at the one moment in the time of the life cycle - it shall be maintained throughout the entire life-cycle / period defined within the regulation.

Note: The questions and answers compiled in this Q&A report were not proof-read by DG CONNECT. The report is presented for reference purposes only, and no review or input from DG CONNECT was sought or provided prior to publication.