For a Rapporteurs joining the STAN4CR project to accelerate the standardisation supporting the Regulation 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

Starting date: 2024-12-02

Deadline for tenders: 2025-01-06
(= publication date + 35 calendar days)

I Introduction

I.1 General

The Cyber Resilience Act (CRA) aims to address the increasing cybersecurity threats faced by hardware and software products by setting essential cybersecurity requirements for manufacturers, with stricter assessments for important and critical products. The European Commission has issued a draft standardisation request to the ESOs for the development of several deliverables to support the implementation of the CRA.

The approach under the draft standardisation request includes the development of horizontal standards for a generic framework and vertical standards tailored to specific product risks. The cross-border nature of cyber threats needs EU-level action to ensure a competitive single market and boost trust in digital products. Standards will facilitate compliance, particularly for small and medium-sized enterprises. Timely development and availability of these standards is crucial for effective implementation.

The STAN4CR project aims to support and accelerate the standardization efforts within the EU, fostering collaboration and coherence in the rapidly evolving cyber security landscape, aiming to prevent security incidents and minimise the impacts of such incidents, including in relation to the health and safety of users.

European standardization efforts will be dedicated to developing the necessary horizontal and vertical (product specific) standards:

- The WG-9 within the CEN-CENELEC Joint Technical Committee 13 (CEN-CLC/JTC 13) “Cybersecurity and Data Protection” will be dedicated to the deliverables linked to the horizontal standards.
- The vertical standards will be developed in different technical committees in specific working groups within CEN, CENELEC and/or ETSI, depending on the scope.

The goal of this project is to facilitate a seamless and inclusive standardization process, while ensuring **appropriate coordination and alignment across both horizontal and vertical standards**. Maintaining cohesion between various workstreams **and engaging in comprehensive stakeholder consultations** will be key for the project’s success. These consultations aim to broaden stakeholder participation, gather diverse perspectives, and enrich the standardization discussions and development process. The project also seeks to raise public awareness of standardization activities and promote greater dissemination and engagement with relevant stakeholders, fostering broader involvement and helping achieve the project's objectives.

The timely development of standards will benefit industries, policymakers, and society at large by providing a solid foundation for the integration of state of art standards into everyday applications of many digital products placed in the EU market. Furthermore, the developments of standards to support the CRA will contribute to the resilience and competitiveness of the EU Single Market by enhancing cybersecurity measures, promoting innovation, and fostering trust among consumers and businesses alike.

To address the stated objectives and aligning with the proposal outlined in the call, the project STAN4CR is envisioned to be structured around three primary needs and objectives:

- timely delivery of the CRA standards
- providing administrative support,
- engaging stakeholders through outreach efforts.

The objective of this Open Call for Tender is selecting Rapporteurs to join the development of vertical standards within the CEN/TC 224 and in collaboration with other technical committees to cover standardization work in support of the *Regulation 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity* *requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).*

Table 1 Deliverables associated to this Open call for Tender

Deliverable	Allocation of the work	Target date of availability of the standards
European standard(s) on essential cybersecurity requirements for Hardware Devices with Security Boxes	The work will start in the CEN/TC 224, with the Rapporteur leading the expert group in WG 17.	2024-10-30
European standard(s) on essential cybersecurity requirements for smartcards or similar devices, including secure elements	The work will start in the CLC/TC 47X working on smartcards and be complemented by the experts lead by the Rapporteur in WG 17, to develop the application part.	2024-10-30

The 'Rapporteur' will be responsible for the execution of the project which involves the following tasks:

- Leadership and coordination of the project team.
- Drafting of the project standardisation documents at the different stages for comments of the involved technical bodies.
- Active contribution to comment solving, including the production of proposals of answers to the comments of the involved technical bodies.
- Attendance to the meetings of the technical bodies and all to relevant coordination meetings, including those corresponding to dissemination activities.
- Liaising with each other under coordination of the Convenor of the coordinating working group,
- Reporting to the coordinating Convenor and working group.
- Contributing to stakeholder outreach and engagement by producing dissemination and outreach material to supporting the development of workshops.
- Attend in person and present during stakeholder engagement activities.
- Lead deep dive sessions with stakeholders.

The Rapporteurs will be responsible for providing CEN-CENELEC with the respective progress reports along the project and the dissemination material to support the dissemination events and stakeholder engagement activities.

I.2 Context

The CRA stands as pivotal legislation aimed at tackling the escalating cybersecurity challenges confronting hardware and software products during their complete lifecycle and covering the value chain. It establishes crucial cybersecurity requirements for manufacturers placing products in the EU market, particularly emphasizing stringent assessments for important and critical products. The timely formulation of standards under the CRA not only serves the interests of industries, policymakers, and society at large but also furnishes a robust framework for the seamless integration of cutting-edge standards into the everyday functionality of numerous digital products. Moreover, the advancement of standards to uphold the CRA promises to fortify the resilience and competitiveness of the EU Single Market by bolstering cyber defence measures.

The project will be developed in close cooperation with the European Commission and directly related to the Standardisation Request to support the CRA. During the standard drafting process, all relevant documents will be shared via email and a centralized collaboration platform. The project results will be promoted on different channels such as on NC's webpages, CEN-CENELEC's and a final dissemination event.

II Objectives

The objective of the Rapporteurs under this call is to lead the project teams in charge of the development of European standards in support of the deliverables needed detailed under lines 39 and 41 of the draft standardization request, while ensuring **timely and appropriate coordination and alignment across both horizontal and vertical standards**. The Project Team will be comprised of the selected Rapporteur and the experts of the CEN/TC 224 WG 17.

III Execution

III.1 General tasks of the Vertical Rapporteurs

The Project Team Leader will be responsible for the execution of the project which involves the following tasks:

- **Leadership and coordination of the project team.**
- Drafting of the project standardisation documents at the different stages for comments of the involved technical bodies.
- Active contribution to comment solving, including the production of proposals of answers to the comments of the involved technical bodies.
- Amendment of the subsequent drafts according to the answers agreed by the technical bodies.
- Attendance to the meetings of the technical bodies **and all to relevant coordination meetings, including those corresponding to dissemination activities.**
- Liaising with each other under coordination of the Convenor of the coordinating working group,
- Reporting to the coordinating Convenor and working group.
- Contributing to stakeholder outreach and engagement by producing dissemination and outreach material to supporting the development of workshops.
- Attend in person and present during stakeholder engagement activities.
- Lead deep dive sessions with stakeholders.

III.2 Types of Vertical Rapporteurs

Two types of Rapporteurs are to be selected to join the STAN4CR project in this Open call for Tender to work on the deliverables listed in the above Table 1 of this Call for Tender. Applicants must specify in the application form the topic they are applying for:

- **Rapporteur 1, joining Project Team 1:** 'European standard(s) on essential cybersecurity requirements for Hardware Devices with Security Boxes'

- **Rapporteur 2, joining Project Team 2:** 'European standard(s) on essential cybersecurity requirements for smartcards or similar devices, including secure elements' (Collaboration work with CLC/TC 47X)

III.3 Timeframe

The Grant Agreement with the EC and EISMEA is in the process of being concluded. However, it is estimated that the project will have an effective start date of 2024-10-01 with the possibility to consider retroactive costs.

Table 2 shows the draft planning of STAN4CR for the vertical projects.

Table 2. Draft planning of STAN4CR, vertical projects

Month	Estimated date	Task	Permanent activities
1	December 2024 (start)	Launch public call for tender: Project Team experts (35 days)	Production of dissemination material and coordination with stakeholder events. Coordination and alignment with vertical workstreams and deliverables.
2-3	January 2025	Selection process of Rapporteurs	
2-3	January 2025	CEN/TC 224 WG 17 Virtual meeting: present Project Team experts and onboarding of experts	
3 to 7	January to May 2025	Project Team works on 1st draft(s)	
7	May 2025	CEN/TC 224 WG 17 meeting presentation of 1st draft and coordination with the horizontal standards and dissemination events and deep dives	
8	June 2025	Mature draft ready for quality check and consideration of stakeholder feedback.	
9	July 2025	Draft ready for submission to HAS assessment	
14	November 2025	Dispatch of ENQ draft	
16 to 20	February to June 2026	CEN/TC 224 WG 17 PT works on comments	
16	June 2026	Dispatch of FV draft	
24	End October 2026	Acceptance of the standard, Date of Availability (DAV), publication by ESO’s	

IV Financial support

The European Commission and EFTA have decided to provide financial support to the standardization work. The financial support from the European Commission and EFTA is based on the SMP 'Single Market Programme Regulation' (including its Financing Decision) and the MGA (Multi or mono beneficiary(ies) Grant Agreement). Unless specified otherwise, costs of external subcontractors are generally funded at 100%, with approx. 95% being borne by EC and 5% by EFTA. Costs have to qualify as eligible as defined in GA N° 101196779 and also in compliance with EC Financial Regulation, and be justified. The payment is usually divided into several instalments after completion of defined milestones and approval of the interim/final reports and the justification of costs. The subcontractors shall fulfil the conditions of the GA N° 101196779 including those relating to liability, ownership of results, confidentiality, conflict of interests, publicity, evaluation, assignment, checks and audits.

The subcontractors' costs shall be justified with copies of the relevant invoices. All relevant evidence shall be kept in view of future payments (reports, work, drafts and deliverables, contracts & invoices, time sheets, tickets, boarding cards, hotel invoices, attendance lists with signatures, meeting agendas & reports, invoices for any consumables, purchase orders, etc…).

Costs incurred before the start date of the STAN4CR project (2024-10-01) will not be considered as eligible for EU financial support.

IMPORTANT: The travel and accommodation costs of the Rapporteurs to the face-to-face meetings of this project are not eligible costs, they are considered as covered by their daily rate.

V Selection criteria

V.1 Selection criteria for the Rapporteurs

The applicants shall comply with the following general requirements:

- Deep knowledge of the European Standardisation system, with a focus on CEN and CENELEC.
- Ability to co-ordinate and lead a team of experts.
- Ability to ensure the integration and consolidation of all contents provided by the Project Team (PT) experts.
- Management skills such as coordinating a group of experts and subcontractors (e.g. technical project leaders), promoting consensus, convening meetings, ensuring the circulation of relevant documents, early recognition, and solution of problems (e.g. concerning time and content of the deliverables).
- Reporting by correspondence or at meetings by addressing the relevant points.
- Ability to timely produce reports when requested and when relevant.
- Proven technical background and a relevant degree in a technical field.
- Ability to supply deliverables at specified target dates.
- Ability to contribute as content provider for the requested deliverable/s in one of the three projects they are applying for (please see below the description of the Rapporteurs).
- Wide experience in standardization processes, creation of standardisation documents and consensus building activities in European and other standardization environments (national and international).
- Strong knowledge of the Cyber Resilience Act, the EU Cybersecurity Strategy and other relevant European legislation, such as the NIS2 Directive and the Cybersecurity Act.
- Knowledge of European and international cybersecurity requirements applicable, under the approach of the Cyber Resilience Act, considering the full lifecycle of connected devices and software products, including vulnerability handling.
- Knowledge of the New Legislative Framework and its implications for standards drafting.
- Understanding of the processes of conformity assessment.
- Communication skills and proficiency in English.

And with the specific knowledge and experience related to the project they intend to join:

Rapporteur 1, joining Project Team 1: 'European standard(s) on essential cybersecurity requirements for Hardware Devices with Security Boxes'

- Deep knowledge of Security Boxes such as used to protect payment terminals, tachograph vehicle units, smart meters, taxi meters, access control terminals, or Hardware Security Modules.

- Knowledge of typical cybersecurity threats, design requirements and assessment methodologies for Hardware Devices with Security Boxes.

- Experience with SOG-IS' Technical Domain for "Hardware Devices with Security Boxes" as a developer, tester or certifier

Rapporteur 2, joining Project Team 2: 'European standard(s) on essential cybersecurity requirements for smartcards or similar devices, including secure elements' (Collaboration work with CLC/TC 47X)

- Broad knowledge of applications running on embedded systems such as smart cards, system-on-chips and similar devices.

- Deep knowledge of application layer security of at least on vertical industrial.

- Knowledge of typical application layer security, including threats, design requirements and assessment methodologies for embedded applications.

- Experience with SOG-IS' Technical Domain for "Smart Cards and Similar Devices" as a developer, tester or certifier.

VI Award criteria

VI.1 Award criteria for the Project Team Leader

The selection of the most suitable candidate will be made on the basis of the following criteria:

a) Documented experience (maximum 60 points):

- Deep knowledge of the European Standardisation system, with a focus on CEN and CENELEC.
- Ability to co-ordinate and lead a team of experts.
- Ability to ensure the integration and consolidation of all contents provided by the Project Team (PT) experts.
- Management skills such as coordinating a group of experts and subcontractors (e.g. technical project leaders), promoting consensus, convening meetings, ensuring the circulation of relevant documents, early recognition, and solution of problems (e.g. concerning time and content of the deliverables).
- Ability to timely produce reports when requested and when relevant.
- Proven experience and a relevant degree in a technical field for the role the intend to apply for (see descriptions Rapporteurs 1 and 2).
- Ability to supply deliverables at specified target dates.
- Ability to contribute as content provider for the requested deliverable/s in one of the three pillars they are applying for (see descriptions Rapporteurs 1 and 2).
- Wide experience in standardization processes, creation of standardisation documents and consensus building activities in European and other standardization environments (national and international).
- Strong knowledge of the Cyber Resilience Act, the EU Cybersecurity Strategy and other relevant European legislation, such as the NIS2 Directive and the Cybersecurity Act.
- Knowledge of European and international cybersecurity requirements applicable, under the approach of the Cyber Resilience Act, considering the full lifecycle of connected devices and software products, including vulnerability handling.
- Knowledge of the New Legislative Framework and its implications for standards drafting.
- Understanding of the processes of conformity assessment.
- Communication skills and proficiency in English.

b) Specific knowledge, technical background and experience related to the project they intend to join (see descriptions Rapporteurs 1 and 2) (maximum 20 points)

c) Expected ability to work well with the existing working group (maximum 10 points)

d) Price (maximum 10 points)

The candidate who will reach the highest score will be considered as the best value for money offer and hence should be the candidate selected to perform the expected activities (unless force majeure).

VII Eligibility criteria

The following candidates will be excluded:

- Candidates who were the subject of a non-likely judgment of recourse for a professional infringement
- Candidates who are in an irregular tax situation or in an irregular special taxation situation
- Candidates who provide incomplete or erroneous information.
- Candidates who submit their application after the submission deadline.
- Candidates with any conflict of interest.

VIII Selection Procedure

Selection procedure Applicants will be selected by a selection committee, which is composed of: − the convenor of CEN/TC 224 WG 17− the secretary of CEN/TC 224; − a representative from the CEN -CENELEC Management Centre.

Applications will be reviewed against the criteria found in the project plan and the skills mentioned in the previous section (weighting 60%). The technical background in the relevant fields of cybersecurity will be particularly valued (weighting 20%). The expected ‘chemistry’ within the project team will also be considered (weighting 10%). Additionally, the selection will be based on the principle of best value for money, considering the day rate of the expert and the number of days the expert requires to execute the work (weighting 10%).

The report of the selection committee on the selection of the experts will be submitted to the European Commission and EISMEA prior to the contracting of the experts.

IX Tenders

Tenders shall be sent to Lucia Lanfri (llanfri@cencenelec.eu), Project Manager at CEN-CENELEC Management, as soon as possible, **to be received at the latest by 2025-01-06**.

The tender shall be in English and contain:

- Application form in the format given in Annex B.
- Curriculum Vitae of each relevant person participating in the project, demonstrating the necessary expertise for the ‘Advertised position’. Applicants shall specify the type of Rapporteur they apply for;
- A schedule and a description of the execution of the tasks which will be carried out in the project as such;
- A table in the format given in Annex A with detailed information on the costs;
- Any further documents to prove the qualification required in the above Clauses on Selection and Award criteria;
- A signed declaration (see Annex B), by which the candidate(s) certifies not to be subject to one of the exclusion criteria as described in Clause “Eligibility criteria” and the veracity of the adjoining documents.

IMPORTANT: The Grant Agreement with the EC and EISMEA is in the process of being concluded. The selection proceeding is conditioned by the signature of the Grant Agreements with the EC/EISMEA. Not signing the contract would imply the cancelation of the selection procedure.

Please note that, to ensure equal treatment of all tenders, it is not possible to modify offers after their submission in relation to the technical and financial proposals. Therefore, incompleteness in this section can only result in negative impact for the evaluation of award criteria. Please note also that proposals deviating from the technical specifications may be rejected for non-conformity.

Candidates may apply for more than one role. In case of multiple applications candidates shall state their priorities **and shall disclose if they are receiving funding for any other EU funded project such as Cyberstand.eu or any other initiative.**

Potential candidates may come from the public sector, universities and from the private industry, always indicating their affiliation. It is essential that the qualifications and experience of the individual fulfilling the tasks are properly described.

For any questions concerning the information provided in this call for tender or if further clarification or additional information is needed, please contact:

Ms Lucia Lanfri
Project Manager at CEN-CENELEC Management Centre
llanfri@cencenelec.eu
Postal address: Rue de la Science 23, 1040 Brussels, Belgium

If additional information related to this call for tender is required, whether due to queries or other reasons, it will be published on the website of CEN-CENELEC.

Please send your application to:

CEN-CENELEC Management Centre
Ms Lucia Lanfri
llanfri@cencenelec.eu
Postal address: Rue de la Science 23, 1040 Brussels, Belgium

Annex A

Table with detailed information on the costs

The following table shall be used in the tender to give detailed information on the costs regarding the work of 'Advertised position'.

Applicants are asked to propose an all-inclusive daily rate which would include travel costs.

Organisation / Staff level	Daily rate (€)	Number of man-days	**Total (€)**	Travel budget	Others (Supplies, Consumables)	**Total cost (€)**
Rapporteur	0,00	0	**0,00**	included	included	**0,00**

IMPORTANT: The travel costs of the Rapporteurs to the face-to-face meetings of this project are not eligible costs, they are considered as covered by their daily rate.

Annex B

Application to a Call for Tender in compliance with SMP Single Market Programme Regulation (and its financing decision) & MGA (Mono or Multi beneficiary(ies) Grant Agreement)

A- Contact details of the Expert

Name:
Position:
Company:
Phone:
Email address:
Country of residence:
Personal website (if any)

B- Information about the organisation/s the expert is working (name, website, contact person, phone, email)

C- Curriculum Vitae (maximum 4 A4 pages)

D- Please specify for which position you are applying:

☐ Rapporteur 1, joining Project Team 1: ‘European standard(s) on essential cybersecurity requirements for Hardware Devices with Security Boxes’
☐ Rapporteur 2, joining Project Team 2: ‘European standard(s) on essential cybersecurity requirements for smartcards or similar devices, including secure elements’ (Collaboration work with CLC/TC 47X)

In case of multiple applications, please list your priorities.

…………………

E- Rapporteur

Skills and expertise	**Yes/No**	**Short description of the evidence of the required skills and expertise for the role you are applying for**
Ability to co-ordinate and lead a team of experts.		
Ability to ensure the integration and consolidation of all contents provided by the Project Team (PT) experts.		
Management skills such as coordinating a group of experts and subcontractors (e.g. technical project leaders), promoting consensus, convening meetings, ensuring the circulation of relevant documents, early recognition and solution of problems (e.g. concerning time and content of the deliverables).		
Reporting by correspondence or at meetings by addressing the relevant points.		
Ability to timely produce reports when requested and when relevant.		
Proven experience and a relevant degree in a technical field for the role the intend to apply for (see descriptions Rapporteurs 1 and 2).		
Ability to contribute as content provider for the requested deliverable/s for the project they are applying for.		
Deep knowledge of the European Standardisation system, with a focus on CEN and CENELEC.		
Wide experience in standardization processes, creation of standardisation documents and consensus building activities in European and other standardization environments (national and international).		
Strong knowledge of the Cyber Resilience Act, the EU Cybersecurity Strategy and other relevant European legislation, such as the NIS2 Directive and the Cybersecurity Act.		
Knowledge of European and international cybersecurity requirements applicable, under the approach of the Cyber Resilience Act,		

considering the full lifecycle of connected devices and software products, including vulnerability handling.		
Knowledge of the New Legislative Framework and its implications for standards drafting		
Understanding of the processes of conformity assessment.		
Communication skills and proficiency in English.		
Communication skills and proficiency in English.		
Rapporteur 1, joining Project Team 1: - Deep knowledge of Security Boxes such as used to protect payment terminals, tachograph vehicle units, smart meters, taxi meters, access control terminals, or Hardware Security Modules. - Knowledge of typical cybersecurity threats, design requirements and assessment methodologies for Hardware Devices with Security Boxes. - Experience with SOG-IS' Technical Domain for "Hardware Devices with Security Boxes" as a developer, tester or certifier.		
Rapporteur 2, joining Project Team 2: - Broad knowledge of applications running on embedded systems such as smart cards, system-on-chips and similar devices. - Deep knowledge of application layer security of at least on vertical industrial. - Knowledge of typical application layer security, including threats, design requirements and assessment methodologies for embedded applications. - Experience with SOG-IS' Technical Domain for "Smart Cards and Similar Devices" as a developer, tester or certifier.		

F- Information on the costs of the experts

F.1 - Rapporteur

- Daily rates:
- Number of man-days:

Total costs:

IMPORTANT: The travel costs of the Rapporteurs to the face-to-face meetings related to this project are not eligible costs, they are considered as covered by their daily rate.

G- Information on the costs of the experts

Description of the offer (answer to the call for tender)

I certify that all documents provided are veracious and in conformity with reality and certify not to be in any situation described below:

a) subject of a non-likely judgment of recourse for a professional infringement
b) to be in an irregular tax situation or in an irregular special taxation situation
c) to provide with incomplete or erroneous information

I also declare that I have no conflict of interest by submitting the present offer.

Signed:

On behalf of :(print name here)

Date: