EUROSMART
The Voice of the Digital Security Industry

CSA 2 - Maintaining Cybersecurity is not Standardisation:

ISACs as Trusted Communities for Cybersecurity Certification Maintenance

October 2026

About Eurosmart

Eurosmart is a European not for profit organisation dedicated to advancing the digital security industry through innovation, standardisation and certification, and advocacy. With a rich history spanning decades, Eurosmart serves as a trusted voice in the field, representing a diverse range of stakeholders. Its members include manufacturers of secure elements, semiconductors, smart cards, systems-on-chip, high-security hardware and terminals; providers of biometric technologies, secure software and cloud services; system integrators; application developers; and issuers. The membership also encompasses security evaluation laboratories, consulting firms, research organisations and industry associations.

Committed to fostering a secure and trustworthy digital environment, Eurosmart engages in proactive initiatives to promote the adoption of robust security solutions and standards. By leveraging its expertise and extensive network, Eurosmart plays a pivotal role in shaping the future of cybersecurity and digital transformation across Europe and beyond.

Executive summary

Cybersecurity certification requires expertise beyond the ESO remit

Eurosmart calls for the removal of the "ESO-first" approach in the draft ITRE report on the Cybersecurity Act revision. European standardisation organisations (ESOs) develop common requirements for security, functionality and interoperability. Harmonised standards help manufacturers demonstrate conformity with the legal requirements they cover. The ongoing maintenance of a cybersecurity certification scheme falls outside that standardisation remit. Making ENISA's ability to issue a technical specification conditional on the availability of a suitable European standard would put the maintenance of certification schemes on the wrong footing.

Security assurance is the purpose of certification

A cybersecurity certification scheme exists to provide assurance about the security properties of a product, component or service within a defined scope and at a stated assurance level. Certification evidence can support a demonstration of regulatory conformity where the scope of the evaluation covers the relevant legal requirement. Maintaining that assurance requires specialists who can assess whether evaluation methods still reflect current threats and whether laboratories apply them consistently. A standard can remain valid while the methods used to evaluate its requirements need to change.

ISACs already provide specialist expertise for scheme maintenance

That expertise already exists. The EUCC ISAC shows how technical groups can bring together evaluation laboratories, certification bodies, manufacturers and public authorities to compare findings from actual evaluations and develop proposals for scheme maintenance. When laboratories interpret the same requirement differently, the relevant group can examine the cases and propose a common interpretation. It can also review sensitive findings in confidence and advise ENISA when an evaluation method needs to change. Other schemes should be able to draw on existing specialist communities or develop their own as the need arises.

NCCAs are best placed to support consistent application across Member States

Member State expertise is essential to consistent application across the Union. National cybersecurity certification authorities (NCCAs) are best placed to identify differences in how schemes are applied because they oversee certification practice in their Member States. They should have a formal role in bringing those differences to the attention of ENISA and the European Cybersecurity Certification Group (ECCG) and reviewing whether proposed changes can be applied consistently. The technical groups can help establish what needs to change. The NCCAs can assess how that change will work in practice across Member States.

ENISA should retain responsibility for technical specifications

ENISA, supported by the ECCG, should decide through the scheme's maintenance process when to issue, revise or withdraw a technical specification. The citation of a European standard should trigger a review where relevant, with ENISA determining whether laboratories still need the specification to apply the scheme consistently. Under Article 75, each maintenance strategy should define how NCCAs contribute and identify the ISAC or equivalent trusted technical community that will support the scheme. This would give practical effect to the role for ISACs recognised in Recital 88 of the Commission proposal

Table of Contents

1. Keep the three legal instruments distinct: certification is not standardisation 5
2. Keep cybersecurity maintenance continuous and threat driven 5
3. Reject the ESO first model for cybersecurity scheme maintenance 6
4. Make operational evidence the foundation of every maintenance strategy 6
5. Keep ENISA accountable and give NCCAs and certification bodies a formal role 7
6. Recognise ISACs as permanent trusted maintenance communities 7
7. Keep cryptographic assurance under Member State governance and operational review 8
8. Protect sensitive knowledge while preserving international participation 9
9. Require every maintenance strategy to identify its trusted community 9
10. Delete the “ESO-first” amendments 10
11. Eurosmart calls for five safeguards 11
12. Adopt the amendments as one coherent package 11

1. Keep the three legal instruments distinct: certification is not standardisation

The ITRE approach conflates three instruments with different legal functions. A harmonised standard translates essential legal requirements into common technical specifications, provides a presumption of conformity within its cited scope and facilitates market access and the free movement of products and services in the internal market. A common specification is a regulatory fallback used where the standardisation system has not delivered an appropriate result in time.

This is precisely what distinguishes a harmonised standard from a technical specification understood as **a certification scheme maintenance document: the latter keeps cybersecurity evaluation methods operational, up to date and aligned with the evolving state of the art; it does not establish a general route to market access.**

Their possible technical overlap does not make their legal purpose, governance or lifecycle interchangeable.

A product may incorporate a component certified under EUCC. Evidence from that evaluation may help the manufacturer demonstrate compliance with specific Cyber Resilience Act requirements that fall within the evaluated scope. The manufacturer still needs to assess how the component is integrated and address the requirements that the evaluation did not cover. Clear rules on which evidence can be reused would help manufacturers avoid repeating work already carried out during certification.

Instrument	Function	Legal and operational characteristics
European standard	A consensus-based technical document for common and repeated use, developed by a standardisation organisation.	Normally public. A harmonised standard may support a presumption of conformity where Union legislation gives it that effect.
Common specification	A regulatory fallback adopted by the Commission where the standardisation system has not delivered an appropriate result in time.	May temporarily support a presumption of conformity and may be withdrawn when a suitable standard becomes available.
Technical specification **CSA2 maintenance document**	An operational instrument used to prepare, interpret, implement or maintain a certification scheme.	Must evolve with threats and evaluation experience. It may be authoritative, restricted and long-lived; it is not inherently temporary.

2. Keep cybersecurity maintenance continuous and threat driven

A certification scheme must remain aligned with the threat landscape and with experience gained from real evaluations. Maintenance includes updating evaluation methodologies, technical interpretations, attack-potential ratings, attack methods and scenarios, technical-domain rules, vulnerability-handling and mitigation measures. Some outputs can be public.

Others contain attack paths, exploitation techniques, non-public vulnerabilities or detailed evaluation methods and require controlled distribution.

EUCC illustrates the issue. Its operation depends not only on ISO standards but also on evolving interpretations, attack-potential calculations, technical-domain knowledge, laboratory practice and vulnerability information. The EUCC ISAC provides the trusted public-private environment needed to address these challenges. Its work is continuous, sometimes urgent and not always compatible with unrestricted circulation.

If every update had to wait for an ESO process, or if a cited standard automatically displaced ENISA documentation, urgent security changes could be delayed, and existing certificates could face avoidable legal and operational disruption.

3. Reject the ESO first model for cybersecurity scheme maintenance

Articles 18 and 77 of the ITRE draft report apply the logic of a temporary common specification to ENISA technical specifications. ENISA could act only where no suitable European standard exists or where an ESO process has failed. The Commission would then request an ESO to develop a standard covering the same requirements, and the ENISA specification would cease to apply to new certifications after citation of that standard.

That sequence may be coherent for a regulatory fallback intended to be replaced by a harmonised standard. It may support conformity assessment for market access, but it is unsuitable for scheme maintenance.

European and international standards may inform scheme maintenance, but they must not automatically replace ENISA technical specifications or maintenance documents. ENISA should determine their relevance through the Article 75 maintenance process, with input from the ECCG, NCCAs, conformity assessment bodies and the relevant scheme-specific technical community.

4. Make operational evidence the foundation of every maintenance strategy

The maintenance strategy should organise a repeatable lifecycle. **It should combine strong operational input with clear accountability and a fast route for urgent action.**

The legal anchor is Article 75(1) of the Commission proposal: each European cybersecurity certification scheme must establish a maintenance strategy covering the expected maintenance activities, the standards or technical specifications referenced by the scheme and interaction with relevant stakeholders. Article 75(2) keeps responsibility for scheme maintenance with ENISA, supported by the ECCG, while Article 75(3) provides the basis for structured stakeholder involvement. **The maintenance strategy should therefore identify the trusted technical environment through which the evidence required for ENISA's technical specifications is assembled and assessed.**

NCCAs, conformity assessment bodies, vendors and scheme users are the principal sources of operational evidence for maintenance. NCCAs bring supervisory findings, peer-review results,

information on consistent national implementation, capacity constraints and the regulatory impact of transitions. Certification bodies and laboratories bring direct evidence from evaluations: recurring interpretation issues, limits in evaluation methodologies, attack-potential calibration, vulnerability handling and assessment bottlenecks. Vendors contribute product and service expertise, vulnerability and update experience, implementation constraints and evidence on the treatment of existing certificates. Scheme users contribute deployment experience, operational risks, procurement needs and evidence on whether scheme requirements and transitions remain usable in real environments. Their input should be continuous, structured and scheme-specific.

The relevant ISAC or equivalent trusted environment should consolidate this evidence and facilitate exchanges with ENISA and public authorities in support of scheme maintenance.

The maintenance strategy should specify how the trusted community submits technical findings to ENISA, how sensitive evidence is handled and who can refer an urgent issue to ENISA. For example, where laboratories interpret the same requirement differently, the ISAC could compare the cases and submit a proposed interpretation for ENISA's review.

5. Keep ENISA accountable and give NCCAs and certification bodies a formal role

ENISA should remain responsible for deciding whether maintenance action is required and for adopting the resulting interpretation, methodology or technical specification. It should do so on the basis of structured operational evidence from NCCAs, certification bodies, laboratories, vendors and scheme users.

- **The ECCG and NCCAs** should provide institutional and supervisory review.
- **Within an ISAC or equivalent trusted environment**, certification bodies and laboratories should assess evaluation feasibility and reproducibility; vendors should assess implementation, vulnerability-handling and product-lifecycle effects; and scheme users should assess deployment, procurement and operational effects. Participation must preserve impartiality, confidentiality and conflict-of-interest safeguards.

6. Recognise ISACs as permanent trusted maintenance communities

An ISAC is a trusted environment that brings public and private actors together around a scheme. Within that environment, they can combine supervisory and evaluation evidence with product-lifecycle and deployment experience, consolidate difficulties encountered in evaluation and use, develop shared interpretations and contribute operational evidence on methodologies, attack-potential ratings, vulnerabilities and attack catalogues. ENISA can then use this evidence to adopt and maintain the technical specifications required for the scheme.

This trusted model is already recognised and promoted by ENISA. **ENISA describes ISACs as central resources for gathering and analysing cyber-threat information and enabling two-way information sharing between the private and public sectors and provides an ISAC-in-a-Box toolkit to support their establishment and operation.** The same logic underpins the voluntary cybersecurity information-sharing arrangements encouraged by Article 29 NIS2. It is

particularly relevant in sensitive environments, where participants must exchange vulnerabilities, incidents, attack techniques and operational lessons within a controlled community rather than through an unrestricted public process.

The Commission proposal itself recognises this model in Recital 88, which states that technical contributions to scheme maintenance may come from ISACs. That recognition should have an operative consequence: Articles 75 and 77 should require the maintenance strategy to identify the relevant trusted community and enable ENISA to use its consolidated technical contributions when developing and updating scheme specifications.

The EUCC ISAC provides the practical model. It is today the primary external contributor to maintenance of the EUCC scheme, operating through a liaison agreement and in accordance with the stakeholder policy established by the European Commission. This framework gives the ECCG subgroup for EUCC maintenance, ENISA and the Commission a structured channel for receiving consolidated technical contributions from NCCAs, certification bodies, laboratories, vendors, scheme users and technical experts. Its value lies in continuity, recognised competence, controlled participation and the ability to handle sensitive operational information.

Under Article 75(1), the maintenance strategy should identify the relevant ISAC and its participants, including NCCAs, certification bodies, laboratories, vendors and scheme users. Where no suitable ISAC exists, an established stakeholder organisation may provide an equivalent trusted environment offering the same expertise, continuity and safeguards. Consistent with the NIS2 approach, the development of ISACs should be encouraged and supported as part of the maintenance ecosystem.

7. Keep cryptographic assurance under Member State governance and operational review

Cryptography is a foundational component of cybersecurity assurance. Its reliability depends not only on published standards, but also on the continuous assessment of algorithms, parameters, implementation techniques, attack methods and migration requirements. Developments in cryptanalysis, implementation attacks and post-quantum cryptography may require coordinated updates that cannot wait for a full standardisation cycle.

The EUCC Agreed Cryptographic Mechanisms provide a concrete governance model. The ACM is maintained by the ECCG subgroup on cryptography, composed of Member State representatives, and supports developers and evaluators in determining which cryptographic mechanisms should preferably be used for EUCC certification. This allows cryptographic requirements to remain aligned with the evolving state of the art and with European security needs.

Member State governance must be supported by evidence from actual evaluations. Certification bodies and laboratories should report recurring implementation weaknesses, interpretation difficulties, attack techniques, methodological limitations and the effects of changes on ongoing evaluations and existing certificates. Vendors should contribute implementation, update and crypto-agility constraints, while scheme users should contribute evidence on deployment conditions, migration feasibility and residual risk. The EUCC ISAC or an equivalent trusted community can consolidate these contributions for the ECCG and ENISA.

This allocation preserves institutional accountability: the ECCG and NCCAs determine the European security position; ENISA maintains the authoritative scheme documentation; and

certification bodies and laboratories provide evaluation evidence without acquiring decision-making authority over the requirements they apply. The ACM therefore demonstrates why an ESO-first model is inappropriate. A later standard may inform the ACM and the EUCC scheme, but it should not automatically replace the cryptographic guidance maintained by the Member States, alter the assurance claimed by a certificate or determine the transition applicable to certified products.

8. Protect sensitive knowledge while preserving international participation

Openness is essential to the development of public standards. However, it is not appropriate for all cybersecurity material, particularly detailed attack methods, exploitation techniques, attack-potential ratings and non-public vulnerability information. Ordinary ESO participation and publication arrangements are not designed to provide the controlled environment required for such sensitive information.

ISACs provide a trusted framework in which qualified participants exchange sensitive information under clear, predictable and enforceable rules on eligibility, confidentiality, conflicts of interest and need-to-know access. **The EUCC ISAC illustrates the appropriate balance: European governance and control combined with the full participation of qualified international stakeholders.** European digital sovereignty should not mean excluding international expertise but ensuring that access to sensitive material and decisions affecting European high-assurance certification remain governed by European rules and interests.

Access rules should be proportionate to the sensitivity of each document. The objective is not to restrict technical cooperation or exclude relevant international expertise. It is to ensure that information capable of facilitating attacks is accessible only to trusted participants who need it for scheme development, evaluation, certification, supervision or maintenance. This controlled but internationally open model protects sensitive methodologies while reducing the risk that actors subject to undue third-country influence obtain privileged access to the technical foundations of European high-assurance certification.

9. Require every maintenance strategy to identify its trusted community

A generic reference to stakeholder involvement is insufficient. Article 75(1) requires each scheme to establish a maintenance strategy. That strategy should identify the ISAC or equivalent trusted environment that brings together the NCCAs, certification bodies, laboratories, vendors, scheme users and technical experts supporting the scheme. Existing and effective structures should be preserved rather than duplicated by temporary groups.

The maintenance strategy should specify:

- the scheme-specific ISAC or equivalent trusted environment and its technical remit;
- the participating categories brought together within it, including NCCAs, certification bodies, laboratories, vendors, scheme users, researchers and other trusted technical contributors;
- the allocation of responsibilities between ENISA, the ECCG maintenance sub-group, NCCAs and the technical community;

- access eligibility, need-to-know rules, confidentiality obligations, conflict-of-interest controls and secure handling arrangements;
- the distinction between public scheme documents and restricted authoritative maintenance documents;
- contribution records, version control, change classification, review periods and transition between versions;
- intermediate consultation steps for broader stakeholder input before material documents are finalised; and
- an urgent procedure allowing ENISA to act immediately, followed by notification and ex post review.

Ad hoc groups should remain available where no mature stakeholder ecosystem exists or where a time-limited specialist task requires additional expertise. They should complement, not displace, permanent technical communities.

10. Delete the "ESO-first" amendments

The ITRE draft report contains a structural contradiction. It keeps ENISA responsible for maintenance while making key ENISA technical tools subsidiary to ESO processes. Eurosmart supports standards-based schemes but rejects any automatic hierarchy that subordinates scheme maintenance to standardisation.

Provision	Problem	Eurosmart position
Article 18(1) ITRE amendment 46	ENISA may act only where no harmonised standard exists and after an ESO request has failed or proved inadequate.	Delete the ITRE amendment and retain the Commission proposal. ENISA action must not depend on an ESO gateway.
Article 77(1) ITRE amendments 74 to 76	ENISA technical specifications become conditional on the absence or inadequacy of European standards.	Reject the condition. Standards should be used where technically relevant, while ENISA remains responsible for scheme documentation.
Article 77(1a) ITRE amendments 74 to 76	The Commission must request an ESO standard and the ENISA specification ceases to apply to new certifications within twelve months after citation.	Delete. A later standard should be assessed by ENISA with the ECCG, NCCAs and the relevant technical community; it must not trigger automatic cessation.
Article 75 ITRE maintenance provisions	Article 75(1) requires a maintenance strategy and ENISA remains responsible, but the trusted environment needed to organise operational input is not sufficiently defined.	Require the maintenance strategy to identify the ISAC or equivalent trusted environment that brings together NCCAs, CBs, laboratories, vendors, scheme users and technical experts and supplies evidence for ENISA technical specifications.
Article 74(2) scheme preparation	The ECCG and stakeholder consultation are recognised, but the lifecycle role of NCCAs and operational experts needs greater precision.	Require a reasoned ECCG opinion and systematic NCCA evidence while preserving ENISA-led technical work with qualified communities.

11. Eurosmart calls for five safeguards

Eurosmart recommends a maintenance model built on five principles:

1. **ENISA accountability and agility.** ENISA should remain responsible for technical maintenance, versioning and urgent action. Its ability to draft and maintain technical specifications must not depend on a prior ESO request or failure finding.
2. **A permanent trusted maintenance community.** Each maintenance strategy should identify a scheme-specific ISAC, or an equivalent trusted environment with recognised expertise. For EUCC, the EUCC ISAC should be recognised as the primary technical maintenance community.
3. **Structured operational evidence.** The maintenance community should bring together the ECCG, NCCAs, certification bodies, laboratories, vendors, scheme users and technical experts. Their respective roles, access rights and safeguards should be defined, while preserving ENISA's decision-making responsibility and the impartiality of conformity assessment bodies. The ACM illustrates why Member State cryptographic governance must be informed by continuous evidence from certification bodies and evaluation laboratories.
4. **Controlled access with international participation.** Public documents should remain open. Sensitive attack methods, vulnerabilities and evaluation material should be shared under proportionate European governance and need-to-know rules, while allowing full participation by qualified international stakeholders.
5. **Standards as input, not as a maintenance gateway.** ESOs should remain liaison partners and sources of relevant standards and technical input. A later standard should be assessed on its merits; it should not automatically replace an ENISA maintenance document or disrupt existing certificates.

12. Adopt the amendments as one coherent package

These principles should be implemented as one coherent amendment package. The detailed drafting is set out in Annex I of the Eurosmart CSA2 ITRE Position Paper Draft v0.32:

- **Article 18(1):** delete the ESO-first restriction and retain ENISA's autonomous ability to draft technical specifications and guidance.
- **Article 74(2):** require structured ECCG and NCCA input during scheme development, including a reasoned and time-bound view on supervisory feasibility, capacity and transition, without displacing ENISA-led technical work.
- **Article 75(1) to 75(5):** require the maintenance strategy to identify the permanent ISAC or equivalent trusted environment, its participating NCCAs, certification bodies, laboratories, vendors, scheme users and technical experts, and the applicable roles, access conditions, confidentiality rules and consultation steps.
- **Article 77(1) and 77(1a):** preserve ENISA-led technical specifications, remove the ESO-first condition and delete automatic cessation or replacement when a European standard is cited.
- **Article 77(4) and new paragraphs 4a to 4d:** establish rules for authoritative documentation, restricted material, ECCG and NCCA consultation, versioning, transition, treatment of existing certificates and urgent ENISA action followed by ex post review.

- **Article 89(3):** ensure that peer review covers the scheme-specific technical expertise and operational capacity of NCCAs, certification bodies, laboratories and other conformity assessment bodies.
- **Article 53(3):** ensure traceability of maintenance decisions and stakeholder contributions while protecting sensitive or restricted information.

Join Eurosmart shaping digital security standards and legislations

Eurosmart extends a warm invitation to all interested parties to join us in our pivotal mission to influence, promote, and advise on legislative frameworks concerning digital security standards and certifications. As we advocate for robust regulatory measures, the support of industry partners is paramount to our success. Whether your operations are within Europe or beyond, your collaboration is vital in bolstering our collective efforts towards fostering a secure digital environment.

Membership with Eurosmart offers the opportunity to contribute to impactful initiatives, providing access to an esteemed network of professionals, exclusive resources, and strategic partnerships. By aligning with Eurosmart, members gain a platform to actively participate in discussions, shape policies, and drive positive change in the realm of cybersecurity standards.

In navigating the complexities of evolving regulations, your partnership plays a pivotal role in advancing our shared objectives. Together, let us uphold the best regulatory and technical approaches, ensuring a safer digital future for all.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com