

Using EUCC certificates to demonstrate CRA conformity:

Recommendations for the Delegated Act under Article 27(9) of the Cyber Resilience Act

September 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.

Coreposition

A valid EUCC certificate should provide a presumption of conformity only for the CRA requirements and product scope that it demonstrably covers. When additional evidence are required to comply with the CRA (e.g.: gap between the evaluated product and the product place on the market) relevant EUCC supporting evidence should be reusable within another applicable CRA conformity-assessment route. Bridging EUCC certification and CRA conformity should leverage existing Protection Profiles where they demonstrably cover the relevant requirements. Protection Profiles should update when feasible but not be expanded automatically or wholesale merely to reproduce the CRA, although proportionate updates should remain possible where technically justified. When required, reusing an EUCC certificate should remain the preferred route when it avoids duplicative evidence or a separate conformity assessment and does not create disproportionate burden for the industry. This approach shall also fit within the manufacturers' overall conformity assessment strategy.

Where an essential requirement is not covered by the certified scope of a valid EUCC certificate or its supporting evidence, whether the certificate was issued before or after the date of application of the Delegated Act the CRA notified body responsible under the applicable procedure should assess only the uncovered elements, using the relevant harmonised standards and the procedures under Modules B+C or H. The Delegated Act should require that body to recognize relevant EUCC evidence. As a transitional measure, valid existing EUCC and SOG-IS certificates should provide a presumption of conformity within their certified scope and for their remaining validity period. Their supporting evidence should remain reusable subject to validation of its scope, a proportionate gap analysis and any necessary additional assessment or remediation; this is not an exemption from CRA conformity assessment.

Table of Contents

Executive summary 4

1. The proposed EUCC CRA bridge..... 5

1.1. Map EUCC coverage to each CRA requirement..... 5

1.2. Preserve existing Protection Profiles and security targets 5

2. A light-touch and modular approach for requirements not covered by EUCC 6

3. Treatment of changes during the product lifecycle..... 9

3.1. Lessons from the QSCD experience..... 9

3.2. Way to solve this shortcoming: provide a risk-based continuity mechanism for CRA conformity ... 9

3.3. Approach to manage cases where the EUCC certificate status or risk changes..... 10

4. Roles and exchange of evidence..... 11

4.1. Clearly define the assessment roles 11

4.2. Define access criteria to EUCC evidence 12

4.3. Define the remaining assessment activities by the CRA Notified Body..... 12

5. Conclusions and recommendations for the Delegated Act..... 13

Executive summary

Eurosmart supports the use of EUCC certification to facilitate conformity assessment under the Cyber Resilience Act. The Delegated Act provided for in Article 27(9) should establish a practical bridge between the two frameworks. It should preserve CRA's and EUCC's respective scope, avoid unnecessary duplication and should not entail any extra burden for the industry.

Eurosmart recommends a modular approach:

1. **Leverage EUCC certification.** Any valid EUCC certificate, whether issued before or after the Delegated Act becomes applicable, should be recognised for the CRA requirements covered by its certified scope. The corresponding evaluation should not be duplicated.
2. **Complement EUCC where necessary.** Where an EUCC certificate does not cover all applicable CRA requirements, the manufacturer should be able to update the certification, use a complementary CRA assessment, or combine both approaches. The CRA notified body should assess only the requirements not covered by EUCC, under the applicable procedure, including Modules B+C or H.

Protection Profiles may need to be adapted for new or renewed certifications, as illustrated by the migration of PP-0084 and PP-0125. Such updates should be targeted, phased and carried out in an orderly manner, starting with component-level Protection Profiles where certification relies on composition. The timetable should take account of the number of profiles concerned, the capacity of industry and conformity assessment bodies, and certification lead times.

Updating a Protection Profile should not, however, be a prerequisite in every case. Where appropriate, an existing Protection Profile should remain usable, with the manufacturer relying on a complementary CRA assessment for requirements not covered by the resulting EUCC certificate.

3. **Ensure transition and continuity throughout the product lifecycle.** Valid EUCC and SOG-IS certificates issued before the Delegated Act becomes applicable should remain usable, within their certified scope, for their remaining period of validity. Existing evaluation evidence should also remain reusable, subject to validation and a proportionate gap analysis, including where the product changes or the certificate is renewed. Reassessment should focus on the impact of the change; a full reassessment should be required only where the certified scope or the relevant CRA requirements are materially affected.

The Delegated Act should also clarify the roles of the different actors and facilitate the secure exchange of evidence.

1. The proposed EUCC CRA bridge

The Delegated Act should use EUCC on a **requirement-by-requirement basis**. It should not require the EUCC framework to be automatically expanded to cover the whole CRA. The feasibility and value of updating Protection Profiles or security targets should nevertheless be assessed during EUCC migration or renewal. The Delegated Act should define how EUCC coverage is mapped to individual CRA requirements, how uncovered requirements are completed through Modules B+C or H, and how evidence is reassessed when certificate status or product risk changes.

The framework should distinguish between: (i) the transitional treatment of existing EUCC and SOG-IS certificates; (ii) the use of new or renewed EUCC certificates for CRA conformity; and (iii) the role of Protection Profiles and security targets as the technical basis for future evaluations. Protection Profiles should not be treated as certificates or as providing, by themselves, a presumption of conformity.

1.1. Map EUCC coverage to each CRA requirement

For each CRA essential cybersecurity requirement, the manufacturer should identify the EUCC certificate, security target, Protection Profile property or evaluation result that provides the relevant coverage and fits its conformity assessment strategy. For instance, some manufacturers may prefer (1) using EUCC evidence as input to a module H conformity assessment because their whole quality management system has been assessed, or (2) rely on prEN 40000-1-3¹ for the vulnerability handling as it uses the same process for all its products, be they EUCC certified or not. In order to identify the relevant coverage, the manufacturer could leverage on the analysis already provided by existing harmonized standards e.g. standards for “Smartcards or similar devices, including secure elements” as prepared by CENELEC/TC 47X. The Delegated Act should define a clear path for facilitating this correspondence so that manufacturers and CABs reach easier and predictable conclusions.

The Delegated Act should clarify how partial EUCC coverage can be combined with the applicable CRA conformity assessment procedure. Where an EUCC certificate or its supporting evaluation evidence covers only part of a CRA requirement, the assessment should focus on the remaining elements and avoid duplicating the work already performed.

1.2. Preserve existing Protection Profiles and security targets

Existing Protection Profiles and security targets have been prepared for types of products for which a high level of security is required. These Protection Profiles and security targets have been drafted from a sound cybersecurity analysis and therefore, by design, they already address all relevant threats and risks which may affect the corresponding product types. Hence, they already include by default all applicable security requirements related to the properties of products with digital elements (as defined in the CRA Annex I – Part I). Therefore, EUCC certificates based on them should provide a presumption of conformity only for the essential cybersecurity requirements and product scope that they demonstrably cover.

¹ prEN 40000-1-3 “Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling;” draft European Standard covering the vulnerability handling requirements as defined in CRA Annex I, Part II.

This does not exclude proportionate updates where they are technically justified: as illustrated by the ongoing migration of PP-0084 and PP-0125. Such updates should be targeted, proportionate and phased. Where certification relies on composition, updates should proceed in an orderly manner, starting with component-level Protection Profiles before addressing composite or higher-level products.

In such a case the feasibility of revising existing Protection Profiles and security targets to address relevant CRA requirements should be assessed case by case, including during the migration to EUCC and at renewal. Revisions should be required where they are technically justified and proportionate, but not solely to reproduce the complete CRA requirement set. A blanket expansion would be costly and lead to capacity problems of CAB and/or Industry, require substantial industry resources and divert technical efforts from innovation and the security challenges that certification is intended to address, especially given the number of Protection Profiles concerned.

Eurosmart recommends that the Delegated Act relies on the existing EUCC Protection Profiles and supporting evaluation evidence to the extent possible. Other CRA conformity assessment routes should be usable for requirements outside their scope and should remain the privileged pathway to ensure conformance.

2. A light-touch and modular approach for requirements not covered by EUCC

Eurosmart recommends a light-touch and pragmatic approach to bridge EUCC certification and CRA conformity to streamline as much as possible the CRA conformity activities from an EUCC certificate for manufacturers, while reducing at the maximum the burden. This approach should be based on the following principles:

- **Leveraging EUCC certificates for CRA conformity based on “regular” protection profiles without specific enhancements to cover all the set of CRA essential cybersecurity requirements;**
- **Reusing everything that could be reused from an EUCC certificate for CRA conformity, either the EUCC certificate as a whole, or EUCC certification evidence.** As such, manufacturers could easily leverage EUCC certificate to demonstrate CRA conformity;
- **Conformity assessment designed to be modular.** It should be possible for manufacturers to address the essential cybersecurity requirements not covered by the EUCC certificate with other conformity assessment routes.

This approach would substantially streamline CRA conformity activities for manufacturers. The Delegated Act should require the CRA notified body to recognize an existing EUCC certificate and its supporting evidence within the certified scope. Manufacturers could then (1) rely on that certificate for the relevant essential cybersecurity requirements and (2) address only the missing requirements through supplemental activities under Module B+C or Module H.

Where an EUCC certificate covers an essential cybersecurity requirement within the product scope and boundaries defined by its security target and, where applicable, its Protection Profile, the product should benefit from a presumption of conformity for that requirement. If the certified scope does not cover the whole product or one or more relevant requirements, the presumption should apply only to

the covered elements (partial presumption of conformity). The manufacturer should demonstrate conformity for the remaining elements through the applicable procedures under Modules B+C or H.

Likewise, relevant EUCC supporting evidence should be accepted in the applicable procedures under Modules B+C or H, subject to validation of its relevance and scope. Supporting evidence does not by itself create the same legal presumption as a valid certificate.

The Delegated Act should confirm that the manufacturer may rely on either the EUCC certificate or the supporting evidence used to obtain it as part of its CRA conformity activities, and that the competent CRA notified body must take that material into account within its demonstrated scope.

In addition, due to this approach, a manufacturer could combine:

- An EUCC certificate to demonstrate compliance with (all or part of) the applicable essential cybersecurity requirement(s) relating to the properties of products with digital elements (as defined in the CRA Annex I – Part I);
- EUCC supporting evidence – used to obtain the EUCC certificate – showing compliance with (all or part of) the applicable essential cybersecurity requirement(s) relating to the properties of products with digital elements (as defined in the CRA Annex I – Part I) to be assessed through the relevant procedures under Modules B+C or H;
- Coverage of the essential cybersecurity requirement(s) relating to the properties of products with digital elements (as defined in the CRA Annex I – Part I) and not addressed by the EUCC supporting evidence or EUCC certificate through the relevant procedures under Modules B+C or H;
- Compliance with prEN 40000-1-3² to ensure compliance with the essential cybersecurity requirements relating to the vulnerability handling (as defined in the CRA Annex I – Part II) assessed through the relevant procedures under Modules B+C or H.

This combination could allow manufacturers to rely on prEN 40000-1-3 for vulnerability handling as an alternative to the mechanisms provided by the EUCC certificate. This approach allows:

- A complementary vulnerability-handling process in which the EUCC vulnerability-management evidence is reused and mapped to prEN 40000-1-3, with the CRA assessment limited to requirements or lifecycle activities not already demonstrated;
- A lighter, faster and much more flexible vulnerability handling than the procedures envisioned by the EUCC certificate management;
- By design to implement a risk-based continuity mechanism for CRA conformity, unlike the EUCC scheme.

Likewise, such combination could also allow a complementary vulnerability-handling process in which the EUCC vulnerability-management evidence is reused and mapped to prEN 40000-1-3, with the CRA assessment limited to requirements or lifecycle activities not already demonstrated by the EUCC certificate or evidence. This approach is very relevant to address products already holding an EUCC certificate.

² prEN 40000-1-3 “Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling;” draft European Standard covering the vulnerability handling requirements as defined in CRA Annex I, Part II.

Eurosmart recommends that the Delegated Act allows:

- EUCC certificate to be usable to bring a presumption of conformity for every individual CRA essential cybersecurity requirement;
- EUCC supporting evidence to be reusable, subject to validation of its relevance and scope, as part of another applicable route, including the relevant procedures under Modules B+C or H;
- Other CRA conformity assessment routes, including the relevant procedures under Modules B+C or H to be usable to cover every individual CRA essential cybersecurity requirement;
- To combine all the three approaches, insofar all CRA essential cybersecurity requirements are covered;
- To cover CRA essential cybersecurity requirements for vulnerability handling (as defined in CRA Annex I Part II) for an EUCC-certified product by reusing relevant EUCC vulnerability-management evidence and assessing only the remaining gaps against prEN 40000-1-3 under Modules B+C or H. For products already certified, transitional arrangements should allow continued reliance on existing evidence, subject to a proportionate gap analysis and any necessary remediation;
- For the vulnerability-handling requirements in CRA Annex I, Part II, the manufacturer should be able to use the applicable CRA conformity assessment procedure, including Modules B+C or H, instead of relying exclusively on the EUCC methodology. The CRA notified body should be able to assess these requirements directly, while taking account of any relevant EUCC vulnerability-management evidence already available.

This is summarized in the table 1 below.

Table 1: Recommended treatment of EUCC coverage

Situation	Recommended treatment	Result for the manufacturer
EUCC certificate covers the essential cybersecurity requirement	Provide a presumption of conformity for that essential cybersecurity requirement. In that case EUCC certificate demonstrates compliance with properties of products with digital elements (as defined in the CRA Annex I – Part I) and vulnerability handling (as defined in CRA Annex I Part II).	Avoid duplicate demonstration for the covered requirement.
EUCC certificate does not cover the essential cybersecurity requirement	Use another applicable CRA conformity assessment method.	Supply the additional evidence needed for the uncovered requirement.
EUCC evidence covering an essential cybersecurity requirement	Usable as part of a CRA conformity assessment through another applicable route, including the relevant procedures under Modules B+C or H. Permit the evidence to be reused subject to validation of its relevance and scope; supporting	Avoid duplicate demonstration for the covered requirement.

	evidence does not by itself create the same legal presumption as a valid certificate.	
The EUCC certified product complies with prEN 40000-1-3 for the essential cybersecurity requirements on vulnerability handling (as defined in the CRA Annex I – Part II)	The CRA Annex I, Part II requirements should be assessed by the CRA notified body under the applicable procedure, including Modules B+C or H, using prEN 40000-1-3 where appropriate. The manufacturer may rely on this assessment independently of the EUCC methodology or reuse relevant EUCC vulnerability-management evidence, with the additional assessment limited to the remaining gaps.	Lighter, faster and much more flexible vulnerability handling. Risk-based continuity mechanism for CRA conformity.

3. Treatment of changes during the product lifecycle

As a transitional measure, valid EUCC certificates issued before the Delegated Act becomes applicable should be recognised directly for the CRA requirements covered by their certified scope, where feasible. Existing SOG-IS certificates should receive equivalent transitional treatment where legally and technically possible, for their remaining period of validity.

The CRA decision cannot depend only on whether an EUCC certificate is currently valid. When the EUCC certificate status or the relevant risk changes, the affected evidence must be reassessed, and the manufacturer must show whether the product continues to satisfy the applicable CRA requirements.

3.1. Lessons from the QSCD experience

Eurosmart has previously drawn attention to the mismatch between the QSCD conformity assessment cycles and product lifetimes. Under the amended eIDAS framework, a QSCD conformity assessment is valid for a maximum of five years and vulnerability assessments must be performed at least every two years. By contrast, a local QSCD may remain embedded in a national identity card for ten years, and devices from the same generation may continue to be used for production of national identity cards over several years.

The Delegated Act should not reproduce this binary approach. A change in the status of an EUCC certificate should lead to a defined reassessment of the relevant evidence and CRA requirements. The status of the EUCC certificate and the possible continued use of the underlying evaluation evidence should be addressed separately. This experience supports a defined CRA risk-based continuity mechanism process rather than an automatic conclusion about the conformity of the whole product.

3.2. Way to solve this shortcoming: provide a risk-based continuity mechanism for CRA conformity

Eurosmart recommends that the Delegated Act provide a risk-based continuity mechanism for the CRA conformity where an EUCC certificate expires, is suspended or withdrawn, or where a new vulnerability

is identified. The mechanism should determine whether and under which conditions the existing evaluation evidence may continue to be used. It should include:

- The affected CRA requirements and the precise EUCC evidence on which the manufacturer relied;
- The threat model, exploitability, attacker resources, time and cost;
- Available remediation and compensating controls, including usage constraints, authentication measures, policy limits or technical updates;
- The period for which any temporary mitigation remains acceptable and the conditions for review;
- The documentation and decision needed from the responsible CRA conformity assessment body, and;
- A consistent approach across the Union so that equivalent evidence and mitigation plans receive predictable treatment.

This mechanism should not be understood as extending an expired or withdrawn EUCC certificate. It should govern how the CRA conformity treats the existing technical evidence, the changed risk and any compensating measures.

3.3. Approach to manage cases where the EUCC certificate status or risk changes

Vulnerability assessment is an essential part of high assurance certification. The difficulty arises where the legal framework provides no transition between a valid EUCC security certificate and an immediate loss of status. The Delegated Act should therefore define how existing evaluation evidence, an updated risk analysis and any compensating measures are to be considered during the product lifecycle.

In cases in which the EUCC certificate status or risk change, leading to the expiration, suspension or withdrawal of that EUCC certificate, the affected evidence should be reassessed, and a risk-based continuity mechanism should be applied.

Eurosmart recommends that the Delegated Act provide for a risk-based continuity mechanism for products' CRA conformity where the EUCC certificate expires, is suspended, or is withdrawn. This mechanism shall apply both where:

- The EUCC certificate is used to bring a presumption of conformity for one or several individual CRA essential cybersecurity requirements;
- EUCC supporting evidence is reused, subject to validation of its relevance and scope, as part of another applicable route, including the relevant procedures under Modules B+C or H.

This is summarized in the table 2 below.

Table 2: Management of cases where the EUCC certificate expires, is suspended or withdrawn

EUCC certificate status or risk changes	Recommended treatment	Result for the manufacturer
Case 1: EUCC certificate covers the essential cybersecurity requirement	Reassess the affected evidence and apply the defined risk-based continuity mechanism.	Document the changed risk, mitigations and any additional assessment required.
Case 2: EUCC evidence covering an essential cybersecurity requirement	Reassess the affected evidence and apply the defined risk-based continuity mechanism.	Document the changed risk, mitigations and any additional assessment required.

4. Roles and exchange of evidence

Both the CRA conformity assessment framework and the EUCC framework will come into play to demonstrate CRA conformity when evidence other than a sole EUCC certificate are used by the manufacturer. A valid EUCC certificate may provide a presumption for the whole set of applicable CRA requirements only where its certified product scope and boundaries demonstrably cover all those requirements. Therefore, the Delegated Act should clarify the exact interplay between the EUCC and CRA framework in case of interplay. The EUCC and CRA frameworks assign different legal responsibilities. The Delegated Act should preserve those distinctions while enabling relevant technical evidence to be reused securely.

4.1. Clearly define the assessment roles

Under the Cybersecurity Act and the EUCC scheme, the EUCC certification body takes the certification decision on the basis of the technical evaluation performed by an IT Security Evaluation Facility. Under the CRA, the notified body performs the third-party assessment required under Module B or Module H.

While an organization may perform activities under both frameworks, the legal capacity, assessment scope and decision remain distinct.

More precisely it means that for organizations performing activities under both frameworks, their capacity to reuse the knowledge, expertise and understanding of a product gained under an EUCC security assessment for CRA conformity assessment activities may be substantially limited because of (1) the firewall imposed on IT Security Evaluation Facility (EUCC scheme) and notified bodies (CRA), and (2) the restriction of access to the EUCC assessment findings outside the EUCC framework. These challenges may substantially reduce the potential mutualization both for manufacturers and organizations.

Eurosmart recommends that the Delegated Act provides guidance so that organizations performing activities under both frameworks could leverage as much as possible on the knowledge, expertise and understanding of a product gained under an EUCC security assessment for CRA conformity assessment activities to

streamline CRA assessment and reduce costs. This is summarized in the table 3 below.

Table 3: Roles and information flows supporting the EUCC-CRA bridge

Actor	Primary role	Information needed to leverage EUCC for CRA conformity
Manufacturer	Demonstrates CRA conformity and maintains the technical documentation.	Coverage mapping, EUCC certificate and relevant evidence, supplementary CRA evidence, lifecycle reassessment and mitigations.
IT Security Evaluation Facility	Performs the technical evaluation supporting EUCC certification.	Information to be shared with the CRA notified body: Evaluation results that may lawfully be reused, with appropriate protection for sensitive findings.
EUCC Certification Body	Takes the EUCC certification decision and manages certificate status under the EUCC scheme.	Certificate scope, assurance level, status, certification report and relevant conclusions on vulnerabilities or remediation.
CRA Notified Body	Performs the third party CRA assessment where the applicable route requires it.	The coverage mapping, EUCC certificate, admissible EUCC evidence and the evidence for requirements that remain to be assessed.

4.2. Define access criteria to EUCC evidence

Access to detailed EUCC findings may be restricted by confidentiality requirements and by the distinct roles of the ITSEF, the EUCC certification body and the CRA notified body. **The Delegated Act should define which documents and findings may be used for CRA conformity assessment, who may access them, for what purpose and under which security and confidentiality safeguards.**

A common minimum evidence package should include the certificate and its status, the certified scope and boundaries, the assurance level, the relevant security target and Protection Profile references, a light version of the certification report where available (without any sensitive content), and the conclusions needed to establish coverage of the corresponding CRA requirements. More sensitive evaluation material should be shared only where necessary and legally permitted.

4.3. Define the remaining assessment activities by the CRA Notified Body

A CRA notified body is likely to remain necessary where an EUCC certificate or EUCC supporting evidence is combined with other assessment routes. The EUCC certificate should avoid repeating the technical demonstration for requirements it covers but does not remove the need to assess the evidence package for the CRA requirements it does not cover.

The treatment of vulnerability handling under prEN 40000-1-3 is a particularly important example. Where the EUCC certificate is withdrawn, expired or otherwise no longer valid, the EUCC certification body addresses the status of the certificate. Separately, the CRA notified body may need to review the manufacturer's vulnerability handling processes, and the continued relevance of EUCC evidence

affected by the EUCC certificate status or risk changes and any compensating measures. This may entail increasing and expanding CRA assessment activities over the product lifetime for the CRA notified body, while the EUCC certificate status or risk evolve over time, i.e.

- Expanding: a CRA requirement initially covered by an EUCC certificate has to be covered by CRA assessment activities carried out by the CRA notified body as part of vulnerability handling (Annex I – Part II);
- Increasing: a CRA requirement supported by EUCC evidence may have to be supplemented by other evidence or compensating measures, which should be covered by CRA assessment activities carried out by the CRA notified body as part of vulnerability handling (Annex I – Part II).

Therefore, an EUCC certificate removes the need for a separate CRA assessment only to the extent that the valid certificate demonstrably covers the applicable CRA requirements and product scope. However, it should eliminate testing, documentation and reassessment for the requirements already covered by EUCC evaluation evidence.

Eurosmart recommends that the Delegated Act identifies the CRA essential cybersecurity requirements for which:

- EUCC certificate may be relied upon to demonstrate conformity;
- EUCC supporting evidence may be relied upon as part of a conformity assessment. It should also specify how the CRA notified body must take account of evidence produced by the EUCC certification body and ITSEF;
- In case of combination of conformity methods, the Delegated Act should also identify which parts of the CRA assessment remain necessary.

5. Conclusions and recommendations for the Delegated Act

The Delegated Act should make EUCC practically useful under the CRA without turning EUCC into a substitute for the CRA conformity framework. A requirement-by-requirement bridge would preserve the value of existing EUCC certificates and evaluation evidence, confine additional assessment to identified gaps, and provide a controlled response when EUCC certificate status or product risk changes.

Eurosmart recommends that the Delegated Act:

- Define a common method for mapping EUCC certificates and supporting evidence to individual CRA essential cybersecurity requirements;
- Confirm that an EUCC certificate at assurance level substantial or higher eliminates duplicate third-party assessment for the corresponding CRA essential cybersecurity requirements in accordance with Article 27(9);
- Allow manufacturers to combine EUCC coverage, relevant EUCC evidence and other applicable CRA conformity assessment routes for CRA essential cybersecurity outside that coverage;

- **Recognise valid existing EUCC certificates directly, within their certified scope and for their remaining period of validity, and provide appropriate transitional recognition for existing SOG-IS certificates where feasible;**
- **Allow manufacturer to cover CRA essential cybersecurity requirements for vulnerability handling (as defined in the CRA Annex I – Part II) for EUCC certified product by assessing its compliance with prEN 40000-1-3 using the applicable route, including the relevant procedures under Modules B+C or H;**
- **Allow manufacturer to cover CRA essential cybersecurity requirements for vulnerability handling (as defined in CRA Annex I Part II) for an EUCC-certified product by reusing relevant EUCC vulnerability-management evidence and assessing only the remaining gaps against prEN 40000-1-3 under Modules B+C or H. For products already certified, transitional arrangements should allow continued reliance on existing evidence, subject to a proportionate gap analysis and any necessary remediation;**
- **Avoid requiring Protection Profiles or security targets to be expanded automatically or wholesale solely to reproduce the complete CRA essential cybersecurity set, while allowing proportionate updates where technically justified;**
- **Specify the minimum EUCC evidence package, access rights and confidentiality safeguards needed for CRA conformity assessment;**
- **Establish a risk based continuity mechanism for expiry, suspension or withdrawal of an EUCC certificate and for material changes in vulnerability risk; and**
- **Define the residual assessment activities of the CRA notified body, including the treatment of vulnerability handling and reassessed EUCC evidence.**

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.

