EUROPEAN
COMMISSION

Brussels, 7.2.2024
SWD(2024) 38 final

COMMISSION STAFF WORKING DOCUMENT

Union Rolling Work Programme for European cybersecurity certification

1. Introduction

The present Staff Working Document (hereafter "SWD") delivers on the requirement of the Cybersecurity Act[1] (hereafter "CSA") under Article 47(1) that *"The Commission shall publish a Union rolling work programme for European cybersecurity certification (the 'Union rolling work programme')"* which, more specifically, *"shall identify strategic priorities for future European cybersecurity certification schemes"* (section 2 of this SWD).

In addition, Article 47(2) of the CSA requires *"The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes or categories thereof that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme"* (section 3 of this SWD).

More generally, the CSA, which entered into force on 27 June 2019, lays down in its Title III the European Cybersecurity Certification Framework (hereafter "the Framework") for the establishment of voluntary European cybersecurity certification schemes. These schemes aim at ensuring an adequate level of cybersecurity for information and communication technology (hereafter "ICT") products, services and processes in the European Union (hereafter "the Union"), as well as reducing the fragmentation of the internal market.

This first Union rolling work programme (hereafter "URWP") takes account of the Cyber Resilience Act[2] (hereafter "CRA") for which EU co-legislators reached a provisional political agreement on 30 November 2023[3]. The CRA will introduce mandatory horizontal cybersecurity essential requirements for products with digital elements, including software and connected devices, made available on the internal market and throughout their lifecycle. It prescribes appropriate conformity assessment methods, including third-party conformity assessment, depending on the level of cybersecurity risks concerned. The CRA foresees a specific interplay with the European cybersecurity certification schemes and its implementation will be facilitated by standardisation.

Furthermore, the upcoming amending Regulation (EU) No 910/2014 establishing a framework for a European Digital Identity (hereafter "European Digital Identity Regulation")[4] foresees a future European cybersecurity certification for European Digital Identity Wallets. Certification also plays a role in the proposal for the EU Cyber Solidarity Act[5], which puts forward certification for managed security services as one of the selection criteria for the trusted providers forming the EU Cybersecurity Reserve (see section 3 of this SWD). In this light, the Commission also proposed on 18 April 2023 a targeted amendment to the CSA to enable the adoption of European cybersecurity certification schemes for 'managed security services'[6].

---

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[2] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final.

[3] Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. Final text as endorsed by the Permanent Representatives Committee on 20.12.2023, 2022/0272(COD).

[4] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM(2021) 281 final. A provisional political agreement was reached between EU co-legislators on 29 June 2023.

[5] Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, COM(2023) 209 final.

[6] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services, COM(2023) 208 final.

Other new legislative initiatives that mention cybersecurity certification in relation to demonstrating conformity with cybersecurity requirements or promoting trust may impact future European cybersecurity certification in a longer term. This includes the upcoming Regulation laying down harmonised rules on artificial intelligence (hereafter "Artificial Intelligence Act")[7] for which respectively EU co-legislators recently reached a provisional political agreement. Furthermore, the Joint Communication to the European Parliament and the Council on EU Policy on Cyber Defence[8] calls for exploring the development of EU level cybersecurity certification schemes for cybersecurity industry and private companies. The Regulation (EU) 2023/1781 on the Chips Act[9] refers to the need to develop, among others, certification procedures in terms of cybersecurity requirements and calls on the industry to develop with the Union such procedures for specific sectors and technologies with potential high social impact. Lastly, the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union ("NIS2")[10] refers to the possibility to require essential and important entities to use particular ICT products, ICT services and ICT processes that are certified under European cybersecurity certification schemes.

This first URWP points to areas where European cybersecurity certification schemes are envisaged due to legislative developments as well as to areas for future reflection regarding cybersecurity certification, which might eventually lead to requests for new schemes where necessary and appropriate. Furthermore, it outlines the strategic priorities to be considered when preparing any European cybersecurity certification scheme. For this purpose, the above-mentioned legislative initiatives have been taken into account. In particular, any future European cybersecurity certification scheme should fully consider the essential requirements and rules of the CRA as well as the related standards development work. Likewise, any future scheme related to European Digital Identity Wallets should build on the standards and technical specifications developed under the European Digital Identity Regulation.

In line with Article 47 (4) of the CSA, in drafting this URWP, the European Commission (hereafter "the Commission") took due account of the opinions[11] issued by the European Cybersecurity Certification Group (hereafter "ECCG") and the Stakeholder Cybersecurity Certification Group (hereafter "SCCG")[12]. Overall, the opinions of the ECCG and the SCCG supported the approach taken by the draft URWP as regards the choice of strategic priorities. They underlined the importance of coherence among schemes under the Framework, the risk-

---

[7] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final. A provisional political agreement was reached between EU co-legislators on 9 December 2023.

[8] Joint Communication to the European Parliament and the Council 'EU Policy on Cyber Defence', JOIN(2022) 49 final.

[9] Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act).

[10] Regulation (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[11] The Opinions can be found on the groups websites. ECCG website available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework. SCCG website available at: https://digital-strategy.ec.europa.eu/en/library/stakeholder-cybersecurity-certification-group

[12] The ECCG was established pursuant to Article 62 of the Cybersecurity Act (CSA) to help ensure the consistent implementation of the CSA. It is composed of national cybersecurity certification authorities of Member States. The SCCG was established pursuant to Article 22 of the CSA to assist the European Commission in the preparation of the Union's rolling work programme and provide strategic advice in the field of cybersecurity certification. It is composed of 50 members from academic institutions, consumer organisations, conformity assessment bodies, standard developing organisations, companies and trade associations.

based approach, the composability of the schemes, and the possibility to use elements of existing schemes for the future ones. The opinions indicate that possible future schemes could be considered in particular for internet of things (IoT) products and Industrial Automated Control Systems (IACS). As areas of possible future reflection, the opinion of the SCCG mentions also smart city data systems, managed security services, identity and trust services across the EU and drone command systems. The opinions also underlined that preparation of any future certification scheme should take into account relevant EU legislation, provide for coherence with schemes that already exist or are in development, and be carried out in close cooperation with the stakeholders.

In accordance with Article 48(2) of the CSA, the Commission has already issued three requests to the European Union Agency for Cybersecurity (ENISA) to develop candidate cybersecurity certification schemes: the European Common Criteria scheme (EUCC), the European scheme on cloud computing services (EUCS) and the European scheme on 5G networks[13]. Having not been included in a URWP, the requests were duly justified on the basis of the current market developments and recent policy and legislative developments in Member States and at EU level (see also Recital 84 of the CSA). The EUCC, adopted on 31 January 2024, is the first adopted European cybersecurity certification scheme under the Framework[14].

2. Strategic priorities for future European cybersecurity certification schemes

Based on the provisions of the CSA and the consultations with stakeholders, and considering recent legislative and market developments, a set of key aspects to consider when proceeding to cybersecurity certification were identified for the Framework to fully realise its potential and meet its objectives.

2.1. Standardisation

The use of international and European standards will have a direct positive impact on the uptake of European cybersecurity certification schemes, in the EU but also globally. For this reason, their use within the Framework, and their further development in close cooperation with the relevant European Standardisation Organisations and other relevant organisations, is a strategic priority.

In this context, the Rolling Plan for ICT Standardisation[15] and the Annual Union Work Programme for European standardisation[16] are appropriate instruments to signal the need for standardisation related actions as necessary.

In the context of the Framework, standards that can be used to express horizontal security requirements and sectoral requirements, as well as standards related to evaluation methodologies, are particularly important. Standards can further sustain requirements of EU

[13] The candidate schemes on EUCS and 5G networks are in preparation.
[14] Commission Implementing Regulation (EU) …/… of 31.1.2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC), C(2024) 560 final.
[15] The Rolling Plan for ICT Standardisation is drafted by the European Commission in collaboration with the European Multi-Stakeholder Platform (MSP) on ICT Standardisation, and is updated annually.
[16] Article 8 of Regulation (EU) No 1025/2012 of the European Parliament and of the Council on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council.

and Member States' policy as well as other regulatory requirements that are relevant for cybersecurity certification e.g. on personal data and safety, and provide a link to cybersecurity certification for policy areas that depend on harmonised standards. It is therefore important to ensure consistency and complementarity between European cybersecurity certification and various standards being developed in support of Union harmonisation legislation.

In particular, the standards to be developed in support of the implementation of the CRA and the European Digital Identity Regulation should be considered for any future European cybersecurity certification scheme. The future CRA standards will build on prior relevant standardisation work, in particular the one concerning the Delegated Regulation 2022/30 under the Radio Equipment Directive (hereafter "RED Delegated Regulation")[17] [18].

Standards are also key elements to coherently express the concept of assurance levels. According to the CSA, cybersecurity certification schemes may cover up to three assurance levels (basic, substantial and high) capturing different levels of risk and involving incremental levels of rigour and depth of the evaluation, as well as its different types (ranging from self-assessment to third party certification of conformity). Finally, further standardisation and guidance as regards evaluation activities can contribute to the harmonisation of conformity assessment methods across the EU.

2.2. Security-by-design, lifecycle security and security-by-default

Often, security-related activities are carried out only in a specific point in time, which leads to high number of security issues discovered too late or not discovered at all [19]. A more effective approach is to integrate these security-related activities across the development lifecycle to help discover and reduce vulnerabilities early, effectively building security in (security-by-design and default).

The Framework encourages organisations, manufacturers or providers involved in the design and development of ICT products, services or processes to implement appropriate measures at the earliest stages of design and development throughout their lifecycle, to protect the security of those products, services and processes to the highest possible degree. Such security-by-design approach would ensure that the impact of cyberattacks is anticipated and minimised. As part of the overall product lifecycle approach, vulnerability handling and disclosure[20] should also be considered in accordance with the Framework. It is in this spirit that the Secure Development Lifecycle (SDL) approach arises (see section 3 of this SWD below).

---

[17] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive.

[18] CEN and CENELEC address cybersecurity needs through the horizontal joint technical committee CEN-CENELEC/JTC 13 'Cybersecurity and data protection' and work closely with ENISA in the context of the European certification schemes, and with the Commission in the framework of the cybersecurity-related standardisation request under the Radio Equipment Directive.

[19] Commission Staff Working Document accompanying the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020:Impact Assessment Report, SWD(2022) 282 final.

[20] As referred to in Article 12 of Directive (EU) 2022/2055 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Similarly, organisations should deploy ICT products, services or processes with inherent secure settings ('security-by-default') or make it easy for the user to configure them to this secure state for the particular use case. This would decrease the burden on users of having to configure their devices appropriately.

Security-by-design, security-by-default and lifecycle considerations are core aspects of the CRA that will apply to all software and hardware products available on the internal market. The CRA foresees the obligation for manufacturers to meet essential cybersecurity requirements, including security-by-default, for the products with digital elements made available on the internal market throughout the design, development, and production phases (see Article 10 and Annex I Section 1). Furthermore, the CRA requires the manufacturers and other economic operators to ensure the cybersecurity and to handle vulnerabilities of such products during a support period which should reflect the time the product is expected to be in use (see Article 10 and Annex I Section 2).

The activities under the Framework are expected to complement and build on the CRA and to promote the incorporation of security features in the early stages of their technical design and development. The formal process of certification, supported by identification or development of appropriate standards, should enable users to ascertain that these security features are verified by independent entities and by the use of effective evaluation methodologies. The adoption of a "security-by-design & security by default" approach can itself be, where appropriate, subject of certification, either as a stand-alone scheme or as part of a broader scheme. In this context, the essential requirements and rules of the CRA as well as the related standards development work should be fully considered.

2.3. Risk-based assurance

The determination of cybersecurity requirements and associated evaluation methods in each scheme should be risk-based. This risk-based approach to cybersecurity certification has been captured in the Framework with the requirement to specify one or more assurance levels in each scheme as follows: 'basic', 'substantial', 'high', as provided in Article 52 of the CSA. In addition, it is specified that the assurance level should be based on the risk associated with the intended use of the product, service or process, in terms of the probability and impact of an incident.

As a given ICT product, service and process may be used in different contexts, each European cybersecurity certification scheme should specify corresponding evaluation levels with different degrees of rigour and depth of the evaluation methodology used. For instance, for any ICT product, service and process with limited impact or in well-governed and controlled environments, self-assessments may be considered as an acceptable option.

As much as possible, assurance levels in each scheme should include a vulnerability assessment. Such assessment should focus on the identification of vulnerabilities and the calculation of attack potential for each identified vulnerability and its impact. Analysing the attack potential required to exploit a vulnerability may include factors, such as the opportunity and time taken to identify and exploit it and the specialist tools and techniques required for exploitation.

The selection of assurance levels, and more importantly, the requirements and corresponding evaluation methods may have direct impact on the efforts spent on and duration of certification. It is therefore necessary to timely gather relevant criteria to duly assess these aspects through,

for example, consultations with manufacturers (including SMEs), conformity assessment bodies and end-users of certified ICT products, services or processes.

2.4. Coherence, 'composability' and common processes

In the context of the Framework, coherence should be pursued at various levels as individual components and services may be employed across various supply chains. Each scheme should be as much as possible compatible with existing relevant schemes under the Framework. Furthermore, European cybersecurity certification schemes should consider relevant requirements stemming from sectoral and horizontal regulations.

Future schemes will need to consider the possibility to re-use existing certificates and schemes ('composability'), including from horizontal, technology-specific and sectoral schemes. The possibility to 'compose' certificates is particularly useful for the certification of complex, large systems relying on sub-systems. It would reduce redundant or double evaluation activities and thus simplify and decrease the organisations' efforts related to compliance in shorter time periods.

However, it is important to duly explore the legal and technical boundaries of composing certificates to avoid uncontrollable or unpredictable side effects. It is necessary to ensure that the certification scheme of systems for which a composition of certificates is allowed, captures all the cybersecurity requirements and desired properties of that system through coherent assurance methods. It is also important to establish appropriate rules for the validity and consistency of evaluation results stemming from the composed certificates.

Finally, coherence should also be achieved with respect to the evaluation of cybersecurity requirements. Divergent approaches may place additional unnecessary burden on stakeholders involved in cybersecurity certification.

Furthermore, evaluation and conformity assessment under European cybersecurity certification schemes should be carried out in a uniform manner in all Member States in order to prevent 'certification shopping'. Existing provisions on peer reviews and peer assessments can mitigate this risk, while building capacity of stakeholders responsible to undertake conformity assessment activities and encouraging cooperation amongst them are also expected to contribute to harmonisation in the EU.

2.5. International cooperation

The Framework has the potential of becoming a benchmark for other international certifications systems. For example, the security requirements and, evaluation methods of European schemes could be adopted as a baseline for cybersecurity certification carried out in other world's regions. This would also support the activities of European manufacturers and developers who trade globally and often have to achieve multiple certifications. In this context, it is important to underline that EU cybersecurity certification schemes will be designed in line with EU's international obligations, including obligations under the frameworks of the World Trade Organisation and bilateral trade agreements.

It is important that schemes would be based on standards in respect of WTO's founding principles[21], as long as those standards are fit for the EU level of ambition and legal framework.

Furthermore, each scheme developed under the CSA may define conditions that can provide the basis for mutual recognition with third countries, in line with the scope of the agreement, including the target assurance level(s) of recognition.

2.6. Measurement of scheme efficiency and improvement over time

Certification contributes to the trust in the cybersecurity qualities of ICT products, services and processes. At the same time, the procedural steps and resources required to obtain a certificate involves a burden for organisations. Considering this, it would be appropriate that stakeholders concerned by the Framework contribute to and advise on the cost-benefit analysis related to each scheme of the Framework. Therefore, it is important to identify metrics and criteria to assess the overall effectiveness and efficiency of the Framework and its schemes over time. A suitable set of metrics, in accordance with Article 67 of the CSA, should capture the relative quantitative or qualitative improvement of cybersecurity assurance of certified ICT products, services and processes, and be consulted with the ECCG, in accordance with Article 58(6) of the CSA, and with SCCG, in accordance with Article 22(3) with the CSA. In addition, supporting measures, including through EU financial programmes such as the Digital Europe Programme, allow to ease access to certification for SMEs and to support capacity building of newcomers to certification and should therefore be promoted.

3. Areas for future European cybersecurity certification

This section outlines areas for possible future European cybersecurity certification schemes linked to legislative developments as well as areas for future reflection regarding cybersecurity certification, which might eventually lead to requests for new schemes where necessary and appropriate. In this context, the European Digital Identity Regulation, the Cyber Resilience Act and the potential extension of the CSA to cover managed security service are particularly relevant.

With a view to promote coherence during the development of potential future schemes, under the referred legislative proposals or otherwise, it will also be important to consider the possibility of re-using the schemes already developed or being developed under the Framework, namely the EUCC, and the EUCS and EU5G schemes currently under development, as well as the possibility to compose certificates.

In line with Article 46(1) of the CSA, the areas identified below concern ICT products, ICT services and ICT processes.

3.1. Possible requests on European cybersecurity certification linked to legislative developments

[21] Regulation (EU) No 1025/2012 of the European Parliament and of the Council on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council.

Areas for possible upcoming requests are expected to be related to European Digital Identity Wallets and manages security services, pending legislative outcomes.

3.1.1. Certification of European Digital Identity Wallets

The European Digital Identity Regulation mandates for a robust and comprehensive certification scheme for the European Digital Identity Wallet, which is crucial to ensure trust, security and the good functioning of the Wallet ecosystem. The European Digital Identity Wallets are electronic identification means and are products proposing a service that includes the provision and operation of Wallets. Consequently, the Wallets must be certified against the relevant cybersecurity requirements relying, as much as possible, on relevant and available European schemes. Until a European Wallet certification scheme will be available under the CSA, the European Digital Identity Regulation allows to complement the European certification with national certification schemes. The Regulation allows the use of national certification only for those parts that cannot be covered by the future European certification and only until appropriate European certification schemes are available. Even during this transition period, a high degree of harmonisation will be ensured by the availability of compulsory common technical specifications of the Wallet and by the establishment of common rules on how these national certification processes will be carried out during the transition period.

3.1.2. Certification of managed security services

Managed security services providers are a key element to high-level certification and have gained increasing importance in the prevention and mitigation of cybersecurity incidents. Managed security services comprise incident response, penetration testing and cybersecurity audit and consultancy services. Some Member States have already created schemes intended to certify the provision of specific managed security services. To prevent an increasing risk of fragmentation of the internal market with regard to cybersecurity certification schemes in the Union, on 18 April 2023 the Commission proposed an amendment to the CSA that will enable the adoption of certification schemes for managed security services. Once this amendment has been adopted by the co-legislators and enters into force, a European cybersecurity certification scheme for managed security services can be elaborated.

3.2. Other areas for reflection regarding cybersecurity certification

3.2.1. Areas for reflection in the light of the Cyber Resilience Act (CRA)

Considering the fundamental impact of the CRA for the cybersecurity of products, the need for potential new certification schemes covering products with digital elements should be assessed in the light of the CRA, including its essential requirements, conformity assessment rules and the work related to the development of harmonised standards specifying the essential cybersecurity requirements set out in Annex I of the CRA.

The CRA extends the cybersecurity obligations for manufacturers beyond the RED Delegated Regulation, by prescribing horizontal cybersecurity requirements for all products with digital elements (hardware and software) made available on the internal market and will therefore have a considerable impact on future European cybersecurity certification schemes.

The CRA establishes conformity assessment methods required depending on the level of cybersecurity risks concerned and entails a specific interplay with European cybersecurity certification schemes. Article 18 of the CRA foresees that European cybersecurity certification schemes can be used to demonstrate conformity with the essential requirements of the CRA or

parts thereof. Certificates issued under such European cybersecurity certification scheme at assurance level at least substantial eliminate the obligation for third-party conformity assessment under the CRA for the requirements that are covered. Furthermore, the agreed text includes a list of categories of critical products (Annex IIIa), for which the Commission may specify the products for which manufacturers shall be required to obtain a European cybersecurity certificate at assurance level at least substantial, by means of delegated acts. The Commission is empowered to amend that list to add or withdraw product categories taking into account the cybersecurity risk of relevant product categories linked to critical dependencies by essential entities under the NIS2 Directive, or to critical supply chains across the internal market.

3.2.1.1. Internet of Things (IoT), Industrial Automation Control Systems (IACS)

Immediately after the entry into force of the CSA, the Commission and the Member States considered the area of the IoT as a potential priority for certification[22]. In addition, with regard to IACS, the CSA specifically refers to the importance to focus on the cybersecurity of critical infrastructures when it comes to the development of certification schemes. In particular, Article 56(3) of the CSA indicates that the Commission must prioritise the sectors listed in Annex II to the NIS Directive[23].

In light of the CRA, it seems appropriate to reassess further with the relevant stakeholders the need to launch new schemes for cybersecurity certification in this area. The CRA covers all products with digital elements whose intended or reasonably foreseeable use include a direct or indirect logical or physical data connection to a device or network, including hardware and software intended for final use and components separately made available on the market. In relation to conformity assessment, the CRA applies a risk-based approach: the vast majority of products with digital elements will be subject to self-assessment, with a smaller category of important products (Annex III) subject either to the application of harmonised standards or to third-party conformity assessment (class 1), or to mandatory third-party conformity assessment irrespective of whether harmonised standards are applied (class 2), or, for critical products (Annex IIIa), to potential mandatory cybersecurity certification where specified by the Commission.

According to the provisionally agreed text of the CRA, several consumer IoT product categories are listed as important products that will need to undergo stricter conformity assessment, while industrial IoT devices and IACS are no longer listed as important products as initially foreseen in the Commission proposal (see Article 24 and Annex III). In the latter case, manufacturers may choose whether to demonstrate conformity with the requirements of the CRA via self-assessment or third-party assessment. Furthermore, products with digital elements, whether they are subject or not to stricter conformity assessment rules, that have been certified or for which a statement of conformity has been issued under a European cybersecurity certification scheme can benefit from a presumption of conformity with the essential requirements of the

[22] The IoT as a possible priority for certification was mentioned in the Joint Communication to the European Parliament and the Council 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' JOIN(2017) 450 final; The Council Conclusions of 2 December 2020 on the cybersecurity of connected devices, 13629/20.

[23] This Directive has been replaced by the NIS2 Directive, which expands the scope of cybersecurity rules to new sectors and entities, refers explicitly to the use of European cybersecurity certification schemes in Article 24. Many of these sectors, e.g. chemicals, food, waste water management, rely on IACS for their operations.

CRA in so far as the cybersecurity certificate or EU statement of conformity cover those requirements.

Hence, any future European cybersecurity certification scheme covering products with digital elements, e.g. IoT or IACS, should build on the requirements and rules set out in the future adopted CRA, as well as take into account any related harmonised standards, in order to facilitate compliance with the CRA.

3.2.1.2. Secure Development Lifecycle (SDL)

Developments in cybersecurity are evolving at an impressive speed. To deal with this dynamic environment, a process-based approach to cybersecurity is essential and seen as the most stable (see section 2.2 of this SWD).

An SDL process makes software security a continuous concern by ensuring that activities such as structural penetration testing, code review, and secure architecture analysis are an integral part of the development effort. There are a number of advantages in pursuing this approach. For example, an increased awareness of security considerations among stakeholders and within the supply chain, cost reduction due to early detection and resolution of issues and, overall reduction of business risks for the organisation.

Typically, practices for SDL are not associated with a specific product. For this reason, they have a horizontal scope and therefore, they can be applied to software developed in support of a range of diverse use-cases, from industrial control systems and IoT, to cyber-physical systems and information technology in general. Similarly, SDL should take a supply chain approach. For instance, the high level of dependability of hardware components (e.g. microprocessors) makes these components a priority target in the context of the SDL approach.

The CRA foresees essential requirements for the vulnerability handling processes put in place by manufacturers from the design, throughout the development and during the support period of products with digital elements (see Annex I Section 2). Those essential requirements will also be covered by the upcoming standardisation work that will facilitate the implementation of the CRA, including for SMEs. The harmonised standards development work for the products of digital elements covered by the CRA will also consider existing European and international standards.

Today, generic standards related to lifecycle engineering and specifications (e.g. ISO/IEC 27034), to lifecycle assessments (e.g. ISO/IEC 21827 and ISO/IEC 15408-3) and more specific ones related to areas such as industrial systems (e.g. IEC 62443) exist, as well as some private initiatives promoting practices and recommendations on code reviews and testing (e.g. the Open Worldwide Application Security Project).

Building on the essential requirements and rules of the CRA and taking into account related standardisation work, future efforts, including on certification, should focus on identifying and, if necessary developing relevant standards and technical specifications on SDL approaches, considering also national, European and international best practices.

3.2.2. Cryptographic Mechanisms

Cryptographic-based security systems are widely used to protect sensitive data and functions in ICT, and the proper choice of cryptographic mechanisms, as well as the security of their implementation shall be ensured to meet effective protection.

Part I of the Common Criteria for Information Technology Security Evaluation[24] indicates that the criteria for the assessment of the inherent qualities of cryptographic algorithms, such as confidentiality, integrity and authentication, are not covered. Hence, in case an independent in-depth assessment related to cryptography is required, the evaluation scheme that applies Common Criteria should consider provisions for such assessments. On this basis, the SOG-IS community has adopted a catalogue of Agreed Cryptographic Mechanisms (ACM)[25], which specifies the mutually recognised cryptographic mechanisms to be accepted by all SOG-IS participants. The ACM is a living document that is currently being updated to incorporate recommendations for post-quantum cryptography, including considerations for their implementation. In addition, the SOG-IS group has also proposed harmonised cryptographic evaluation procedures and associated tools[26].

The established ECCG subgroup on cryptography enables Member States to analyse the elements of the SOG-IS community for the benefit of European cybersecurity certification schemes. It will also investigate on standards to enhance the assessment of secure implementation of cryptographic mechanisms at EU level, as well as map other existing specifications and guidelines on cryptography. Furthermore, the sub-group will serve as a forum for discussing the possibility of a dedicated EU certification scheme on cryptography, considering relevant European and international developments.

3.2.3. Fixed-time Evaluation

Fixed time cybersecurity evaluation describes a methodology that is implemented using pre-defined time and workload resources and therefore that can be adapted to products that may require a lower assurance[27]. Cybersecurity certification may be regarded as a resource- and time-intensive process. Demanding documentation obligations and evaluation activities may disincentivize businesses to undergo certification processes. This can also create an issue for software solutions (e.g. mobile applications) that have rapid evolution and undergo frequent updates, therefore necessitate more frequent and shorter-lived evaluations as compared to other solutions with longer life cycles (e.g. smartcards embedded in passports).

The Framework promotes schemes that can be based on risk-based standards and specifications, to encourage organisations to certify their ICT products, services, and processes for the risk levels that are adequate to the intended use. Fixed-time certifications aim to provide for more flexible forms of assessments adapted to specific needs of individual ICT products, services or processes by focusing on selected security aspects. Certification schemes based on fixed-time evaluation could therefore be beneficial to organisations or products that rely on frequent security updates to continuously address new vulnerabilities. Fixed-time schemes may also benefit SMEs, as a first step before entering a more demanding certification approach, such as under EUCC.

---

[24] The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria is a framework that enables computer system users to specify their security functional requirements (SFRs) and security functional assurance requirements (SARs) using Security Targets (STs) or Protection Profiles (PPs).

[25] SOG-IS Crypto Working Group. *SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms*, version 1.3, February 2023.

[26] SOG-IS Crypto Working Group. *SOG-IS Crypto Evaluation Scheme - Harmonised Cryptographic Evaluation Procedures*, version 0.16, December 2020.

[27] CEN and CENELEC published the standard EN 17640 'Fixed-time cybersecurity evaluation methodology for ICT products' (FITCEM) that was elaborated in JTC 13 'Cybersecurity and data protection'.

4. Conclusion

In today's digital age, cybersecurity challenges are ever more pervasive, calling for a comprehensive response. The European cybersecurity certification framework is part of that response, as it contributes to making ICT products, services and processes more cybersecure, and thus the internal market more resilient. Furthermore, it enhances trust of consumers and businesses in the digital world.

The Framework is an important tool to support the implementation of recent EU initiatives in the digital policy and has to adapt to an evolving regulatory and technological space. Extending its scope through the inclusion of certification schemes for managed security services will equally strengthen the positive contribution of cybersecurity certification schemes to increase the level of cybersecurity in the EU.

The CRA complements the Framework by establishing mandatory horizontal cybersecurity requirements for products with digital elements, and by foreseeing an obligation for manufacturers to demonstrate conformity with these requirements. In this context, European cybersecurity certification schemes, e.g. the EUCC and future schemes, can play an important role to facilitate compliance. Furthermore, the European Digital Identity Regulation foresees the development of European cybersecurity certification for European Digital Identity Wallets.

While three European cybersecurity certification schemes are already at various stages of preparation and adoption, the present URWP outlines strategic priorities to be considered when preparing any scheme, as well as some areas for future cybersecurity certification, taking into account the opinions of relevant stakeholders represented in the ECCG and SCCG.

The EU cybersecurity landscape remains very complex and dynamic, facing a plethora of attacks and threats. The Framework should constitute a flexible tool with procedures being able to adapt to products, services or processes that face specific challenges and needs in terms of cybersecurity assurance. As the demand for such assurance continues to raise, the collective efforts of harmonizing cybersecurity certifications remain essential for providers and users across the internal market as well as for Europe's global digital leadership. These aspects and the overall experience of implementing the Framework will feed in the upcoming evaluation of the CSA[28].

[28] As foreseen in Article 67 of the CSA.