Cyber resilience and the future EU Cybersecurity Certification Framework

Published as part of the EU-funded project co-financed by the

Connecting Europe Facility 2014-2020

Call Reference: CEF-TC-2020-2 – Cybersecurity; Project Number: 2020-EU-IA0222

Project title: **Cybersecurity Certification and enhancing (business) flows (A4CEF)**

Project Partners and Contributors

Costas Efthymiou
Alternate ENISA Management Board Member for the Republic of Cyprus
Nicosia, Cyprus
https://www.dsa.cy

Athina Panayiotou,
Vassos Vassiliou,
Diamantis Zafeiriades,
Christos Koutsioupis,
Chrystalleni Papadopoullou
CyberSecurity Unit
Nicosia, Cyprus
www.cycert.org.cy

Roland Atoui,
Ayman Khalil,
Isaac Dangana,
Testing and Certification
Red Alert Labs
Alfortville, France
https://www.redalertlabs.com/

Stewart Hickey,
Denis Ryan,
Brian Connaughton,
Pat McHugh,
Khalimatou Samirah
Certification
National Standards Authority of Ireland
Dublin, Ireland
www.nsai.ie

***Abstract* – The increase in cybercrime continues to raise trust concerns in ICT products processes and services in the industry. To address these concerns the European Commission has adopted the Cybersecurity Act, that defines requirements for Cybersecurity Certifications for ICT products, processes and services that will be recognised through the EU region. In line with this framework, the European Agency for Cybersecurity (ENISA) is developing Cybersecurity Certification schemes to support certification activities in relation to specific types of ICT products or services such as Cloud Services for which the EU Cloud Services (EUCS) scheme is being developed. The increase in adoption of cloud services has pushed a consortium of European partners to engage in a project to develop capabilities for Cybersecurity Certifications in line with the EUCS scheme. The project named A4CEF for "Advancing Cybersecurity Certification Capabilities with Cross-border exchange and Enhancing (business) Flows" has run from 2021 to 2023 and involved series of activities aiming to tackle the challenges faced by stakeholders involved in the Cybersecurity Certification Framework and provide recommendations for efficient certification processes as envisaged in the Cybersecurity Act.**

Keywords – Cybersecurity, Cloud, Certification, Cybersecurity Certification, ENISA, Cybersecurity Act, A4CEF, EU Cloud Services, EUCS

I. INTRODUCTION

Cybercrime has increasingly raised concerns these last few years and continues to be an issue to organisations and states security. Governments around the world are responding to this issue and within the European Union (EU) the Cybersecurity Act 2019 was adopted. This regulation sets out a framework for Cybersecurity Certifications that will be recognised throughout the EU region, to increase trust in ICT products, processes, and services. The Cybersecurity Act also strengthen the role of the European Network and Information Security Agency (ENISA) that develops schemes upon request from the EU commission, covering different type of ICT products, processes, or services such the EU Cloud Services (EUCS) scheme for Cloud Services. It is probable that schemes will be mandated for certain categories of

products or services. According to the new rules, vendors in the EU will have to certify these products or services before placing them on the EU market.

Previous research work has explored cybersecurity certifications. Khalimatou proposed a methodology to assess the readiness of Cloud Service Providers (CSPs) to partake in EUCS certifications based on a Cloud Security Readiness (CSR) model [1]. However, this involved CSPs that were not aware of the requirements of the scheme and did not take into consideration the submission of supporting documentation as part of the assessments and did not explore audit processes. Markus and Stefan worked on a Business Process Model and Notation (BPMN) based approach to model and monitor security aware processes in Industrial Internet of Things (IIoT) [2]. Leira et al. developed a framework, called MEDINA, that supports continuous audit-based certifications based on the EUCS to tackle the challenges faced by Conformity Assessment Bodies (CAB)s and Cloud Service Providers (CSP)s during the audit cycle [3]. However, this framework focuses on specific requirements of the scheme and may not be applicable to EU schemes in general. Furthermore, the process does not involve other stakeholders such as the National Accreditation Body (NAB) and the National Cybersecurity Certification Authority (NCCA).

At national level within the EU states, it will be necessary to appoint or establish entities to meet obligations under the Cybersecurity Act 2019 and the Cybersecurity Certification Framework. These entities include Conformity Assessment Bodies (CABs), National Cybersecurity Certification Authorities (NCCAs) and National Accreditation Bodies (NABs) assuming different responsibilities. In 2020, a consortium of European partners, from France, Cyprus, and Ireland, was successful in securing funding under the Connecting Europe Facility (CEF) Telecom Work Programme, to work on a project aiming to develop their internal capabilities and exchange best practices in relation to Cloud Services Cybersecurity Certifications.

The project entitled “Advancing Cybersecurity Certification Capabilities with Cross-border exchange and Enhancing (business) Flows” (A4CEF) has been running since 2021 and is nearing its completion in June 2023. The activities involved as part of this project have allowed the partners to develop their internal capabilities through training, cross border exchange workshops and contribute to the development of the EUCS. These contributions include the development of process flows covering the cybersecurity certification framework from A to Z as defined in the Cybersecurity Act and the results of EUCS pilot certifications in accordance with the EUCS – CLOUD SERVICES SCHEME - DECEMBER 2020. The process flows developed can be used as a basis for the development of an IT system that will support efficient cybersecurity certifications as envisaged by the Cybersecurity Act and the EU schemes. The recommendations resulting from the pilot certifications will feedback into the development of the EUCS scheme contributing to more efficient certification processes. This article is structured as follows; Section II presents the cybersecurity certification Framework as defined in the Cybersecurity Act 2019. Section III provides information on the ongoing work carried out as part of the A4CEF project, focusing on the process flows and the results of the EUCS Pilot Certifications. Finally, Section IV presents the recommendations resulting from this work.

II. THE EU CYBERSECURITY CERTIFICATION FRAMEWORK

The EU Cybersecurity Certification Framework as laid out in the Cybersecurity Act (Regulation (EU) 2019/881) provides guidance for the creation of EU Cybersecurity Certification schemes covering different ICT Products, Processes or Services. Upon request from the EU Commission, ENISA develops schemes following a normalized approach that specify various levels of assurance (e.g., Basic, Substantial or High), based on the risk associated with the use of these ICT Products, Processes or Services [4]. As Cybersecurity Certification plays a key role in increasing trust in Products, Processes and Services, a formal evaluation against defined set of criteria and standards, by an independent accredited organization is required. As such, the Cybersecurity Certification framework provides for independent parties to support certification activities. These include the NCCA, NAB, CAB and testing laboratories. The NCCA supervises the schemes and enforces its obligations at the national level. The CAB carries out investigations in the forms of audits and evaluations. The role of NAB is envisaged as providing accreditation and oversight to CABs, assisting the NCCA in its supervising role as shown in the following figure Fig1.

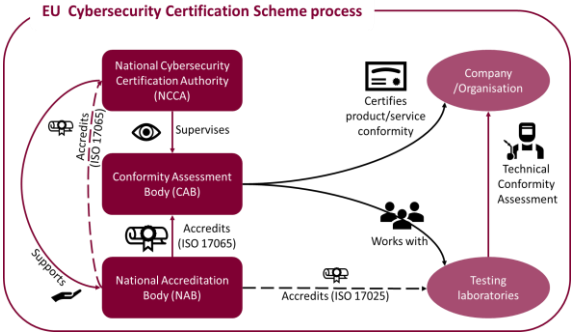

Fig. 1. EU Certification Framework

Additionally, Cybersecurity Certification also provides assurance to users about the level of conformity of ICT Products, Processes or Services against requirements said in the different schemes, following the same framework. Currently three cybersecurity certification schemes are under development at different maturity levels. The EU Common Criteria (EUCC) is the most advanced in the process and has received a positive opinion from the European Cybersecurity Certification Group (ECCG). The EUCC scheme was passed to the EU commission to become an implementing Act. The EU Cloud Services (EUCS) scheme is about to enter the process of the ECCG opinion and the first draft of the EU 5G scheme should be available for public consultation around mid-2023 [5]. To support EU member countries in the development of their capabilities in relation to EU Cybersecurity Certifications, the EU Commission is funding a series of projects. From a national perspective, Ireland has a large ICT industry consisting of top global multinationals including many leading cloud computing providers e.g. Microsoft, Oracle, Google etc. Ireland hosts almost 50 data centres with the Dublin Metro Area being Europe's largest data centre market. The country also hosts a strong indigenous SME base in the ICT sector offering products and services ranging from data protection and smart analytics, identity and access management to IT hardware infrastructure and network management.

Having a strong cyber security accreditation and certification infrastructure would be strategically important for Ireland, and for the EU particularly given the considerable number of cloud data centres in Ireland that are used by many EU businesses and citizens. However, it is important that a suitable model is established for Ireland, and one that would help build national capabilities and capacity in a key area of cyber infrastructure.

A consortium was established comprising of national certification bodies (the National Standards Authority of Ireland (NSAI) and The Certification Company of Cyprus (CCC)), a designated NCCA (the Digital Security Authority (DSA)) of Cyprus and a testing laboratory in France, Red Alert Labs (RAL), in order to develop internal capabilities under the project named A4CEF (Action 2020-EU-IA-0222), for *Advancing Cybersecurity Certification Capabilities with Cross-border exchange and Enhancing (business) Flows*.

III. A4CEF

The A4CEF project aims to:

- Develop of internal capabilities of NSAI as a Conformity Assessment Body (CAB) for cybersecurity certification through a CAB gap analysis in the context of the European Cybersecurity Certification Framework;
- Enhance the internal capabilities of the consortium partners, through existing and newly developed training material on cloud computing certification and;
- Exchange best practices and relevant information related to conformity assessment between Cyprus and Ireland.

The project also involved a series of activities including the development of a reference model architecture that can be adopted by technological means, for example process management platforms, to support Cybersecurity Certifications as envisaged in the Cybersecurity Act and the implementation of EUCS pilot certifications involving SMEs in the EU region.

A. Modelling

Certification activities can be repetitive, time and resource heavy resulting in increased cost for certification consumers. As such, a reference model architecture has been developed, aiming to support efficient certification activities, and reducing certification time and cost.

Following a modular approach, the reference model is designed to provide near real time monitoring, process optimization and efficiency in the lifecycle of cybersecurity certification as envisaged in the Cybersecurity Act, as well as reporting capabilities from distributed data sources from different stakeholders involved in the process. The reference model is composed of modules and highlights interfaces between stakeholders.

1) NCCA module model

Although each stakeholder can start developing their capabilities independently, the NCCA is responsible for supervising the implementation and maintenance of EU schemes nationally within EU member countries. As such, the process starts here. The NCCA is also responsible for monitoring and authorizing CABs, as well as handling complaints under certain conditions specified in each scheme as shown in the following Fig 2.

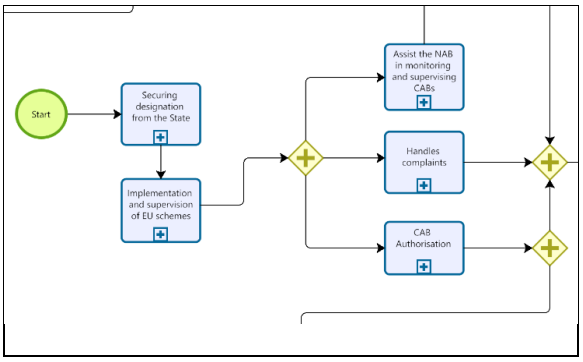

Fig. 2. NCCA Module model – part 1

Other responsibilities of the NCCA include enforcing the obligations of ICT products manufacturers/service providers, monitoring the developments in the field of cybersecurity, and cooperating with other NCCAs through peer reviews and other activities. The NCCA will report on its activity annually to ENISA as shown in the following Fig 3.

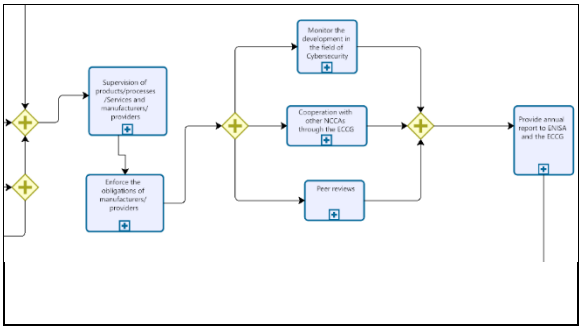

Fig. 3. NCCA Module model – part 2

The NCCA interacts with the CAB and vendors as part of authorization and with the NAB as part of monitoring compliance of CABs as shown in Fig 4 below.

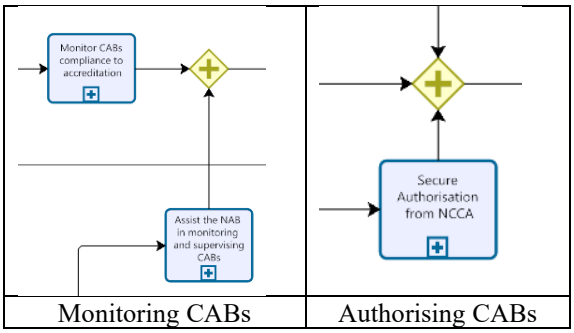

Fig. 4. NCCA interfaces with NAB and CAB

2) NAB module Model

The NAB is responsible for the accreditation of CABs and monitoring their compliance with accreditation requirements as shown in the figure Fig 5.

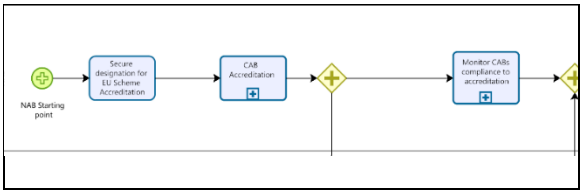

Fig. 5. NAB module model

3) CAB module model

The CAB performs evaluation and certification activities for ICT products, processes, or services. Under certain conditions, that differ based on the scheme, accredited CABs must be authorized by NCCA as shown in the following Fig 6.

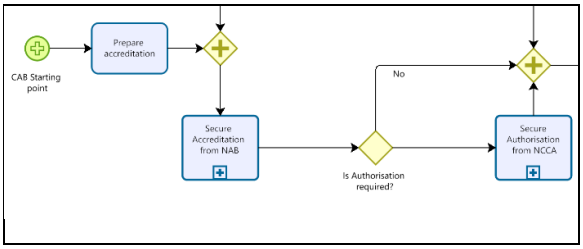

Fig. 6. CAB module model – part 1

The methodologies and requirements for the evaluation and certification of ICT products, processes or services are defined in the different schemes as illustrated in Fig 7.

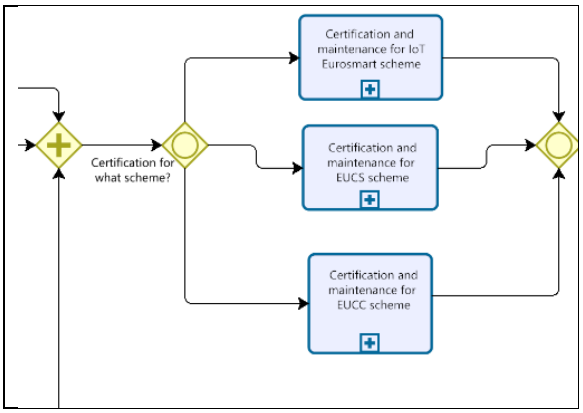

Fig. 7. CAB module model – part 2

Certificates of EU scheme compliant ICT products, processes or services will be published in a centralized platform maintained by ENISA.

4) Product manufacturer/service provider

ICT product manufacturers or service providers will be able to avail themselves of conformity self-assessment or 3rd party conformity assessment from CABs, depending on the scheme they apply for, as shown in the following illustration Fig 8.

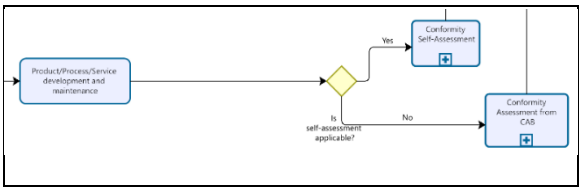

Fig. 8. Product manufacturer/service provider module model

This reference model provides higher level view of the activities and interactions involved as part of cybersecurity certifications. However, further developments are required to obtain a fully functional reference model that will support ICT products, processes and services cybersecurity certifications as envisaged in the Cybersecurity Act. This will only be possible when the schemes, such as the EUCS, are finalised and published by ENISA, providing the full set of requirements and obligations involved as part of cybersecurity certifications.

Although the EUCS scheme is at candidate stage at ENISA level, its first draft was published in 2020, EUCS – CLOUD SERVICES SCHEME December 2020. The consortium partners have used this document to perform EUCS pilot certification to understand what is involved as part of cybersecurity certifications in the context of EUCS. The results of these pilot certifications will contribute to the identification of further development required to enhance the internal capabilities of the partners.

B. EUCS Pilot certifications

Two ISO 27001 certified Cloud Service Providers (CSPs) in Ireland and one CSP from Cyprus were selected to take part in the EUCS pilot certifications for a period of 6 months in the context of this project. ISO 27001 certified CSPs were deemed suitable as participants as they were more mature in the implementation of information security management systems (ISMS) and familiar with auditing processes. This exercise involved:

- 2 Cloud Services evaluated at Basic assurance level
- 1 Cloud Service CSP evaluated at High assurance level

The methodology also involved the partners as follows:

- The partners developed, reviewed, and validated a Cloud Security Maturity Questionnaire (CSMQ) to assess the maturity of the CSPs. 2 CSMQ were developed and issued to CSPs, one for Basic Assurance level and another for High Assurance level.
- The responses and evidence provided by the CSPs were reviewed in accordance with the requirements of the EUCS Candidate scheme, and giving the vendors opportunity to provide clarifications and additional supporting evidence.
- Evaluation reports were then issued and reviewed according to the current requirements of the candidate scheme and the consortium partners' experience.

This assessment showed that:

- At basic assurance level, the cloud services fully complied with 2% of the requirements, partially complied with 10% and were not compliant with 84% of the requirements of the EUCS candidate scheme.
- At high assurance level, the cloud service was compliant to 17% of the requirements, partially compliant to 10% and not compliant to 66% of the requirements of the candidate scheme as illustrated in the table below.

TABLE 1. PILOT CERTIFICATIONS COMPLIANCE RESULTS

Cloud Services	Compliance		
	Compliant	*Partially compliant*	*Non-Compliant*
At Basic assurance	2%	9.5%	84%
At High assurance	17%	10%	66%

The remaining requirements were considered not applicable for the assessed cloud services. The justification for these exclusions was recorded in observation reports.

Furthermore, all cloud services assessed demonstrated the highest level of compliance in Organisation of Information Security (OIS) over the 20 categories of controls available in Annex A of the EUCS candidate scheme and demonstrated highest level of noncompliance with Product Safety and Security (PSS) and Dealing with Investigation Requests from Government Agencies (INQ) categories. This assessment highlighted the following insights:

- The increased awareness of the participating CSPs for the requirements included in Annex A of the EUCS candidate scheme.
- The lack of guidance associated with the said requirements as the guidance on requirements of the EUCS candidate scheme is not fully available yet, the required evidence to meet those requirements is not clear;
- The significant number of requirements to meet even at Basic assurance level and the time taken to provide input to the questionnaires and collate the evidence do demonstrate compliance;
- The need for a centralised platform that will support information exchange and processing between stakeholders in the context of the Cybersecurity Certification framework.

5) RECOMMENDATIONS

The activities involved as part of this project has allowed to make the following recommendations:

- Promotional campaigns targeted at industry and government organisations, aiming to raise awareness in relation to the current developments in EU cybersecurity certifications; especially in the area of cloud as this is of interest to most organisations with the increased adoption of cloud technologies;
- The provision of adequate training covering certification and related activities is vital to the success of the implementation of EU cybersecurity certification schemes in EU member countries;
- It is crucial to develop a centralised platform to support information exchange and processing between stakeholders at national and EU level;
- Further work is required to explore the additional activities involved as part of the EU Cybersecurity Certification Framework, for example in relation to vulnerability handling in certified solutions that was out of the scope of this project. However, this aspect represents an important part of maintaining compliance of certification in ICT products, processes or services.

ACKNOWLEDGEMENTS

This work was funded by the EU Commission under Connecting Europe Facility 2014-2020 CEF-TC-2020-2 – Cybersecurity.

REFERENCES

[1] K. Samirah, “Assessing the Readiness of Cloud Service Providers in Ireland for the EU Cloud Services Scheme,” NORMA eResearch @NCI Library, Dublin, 2021.

[2] M. H. &. S. Schönig, “SIREN: Designing Business Processes for Comprehensive Industrial IoT Security Management,” in 18th International Conference on Design Science Research in Information Systems and Technology, DESRIST 2023, Pretoria, 2023.

[3] J. L. G. C. B. a. J. A. Leire Orue-Echevarria, “Medina: Improving cloud services trustworthiness through continuous audit-based certification,” in 1st SWForum Workshop on Trustworthy Software and Open Source, TSOS 2021, 23 March 2021 - 25 March 2021, 2021.

[4] THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, “REGULATION (EU) 2019/881 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),” Official Journal of the European Union, 2019.

[5] ENISA, “EU Cybersecurity Certification,” ENISA, [Online]. Available: https://certification.enisa.europa.eu/. [Accessed 28 Apr 2023].

[6] G. Aggarwal, “How The Pandemic Has Accelerated Cloud Adoption,” Forbes Councils Member, 15 Jan 2021. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2021/01/15/how-the-pandemic-has-accelerated-cloud-adoption/. [Accessed 02 May 2023].