THE FUTURE OF THE CERTIFICATION OF CYBERSECURITY TECHNOLOGIES

Jakub Vostoupal

Mgr. Jakub Vostoupal, PhD student, Masaryk University, Faculty of Law – Institute of Law and Technology. Veveří 158/70,
611 80 Brno, CZ
Email: Jakvost@gmail.com

Keywords: ***Compliance, Certification, Cybersecurity, The Cybersecurity Act, Conformance assessment***

Abstract: *This paper briefly maps the topic of compliance and certification. The main focus of this paper shall be the Cybersecurity Act as the future of the certification of cybersecurity technologies. This paper introduces the procedural and institutional aspects of the new European certification framework as established by the Cybersecurity Act.*

1. Introduction and Compliance

As the phenomenon of the IoT spreads, the matter of cybersecurity becomes more and more important.[1] According to Europol's report of 2019, the financial impact of the cybercrime still rises (*IOCTA: Internet Organised Crime Threat Assessment 2019*, 2019). Via the unsecured connection of devices to the internet, the position of hackers is way easier and so it is necessary to set a standard of security even for these building blocks of the IoT (e.g. Smart TVs). The standard of security is usually set in a very general way (e.g. «the subject is obliged to take all necessary precautions to achieve a secure state» and the regulator (mainly the state) often uses vague terms or performative rules to form cybersecurity norms (Hurychová & Sýkora, 2018, p. 7; Polčák, Harašta, & Stupka, 2016, pp. 77–78).[2] These techniques allow subjects the freedom to adjust the security countermeasures to their situation. Otherwise, there could be a regulatory requirement to implement high-risk countermeasures for technology in a low-risk environment, which is not only unnecessary but also very costly for SMEs (Hurychová & Sýkora, 2018, p. 7; Polčák, Harašta, & Stupka, 2016, pp. 77–78).

But the freedom that comes with the regulatory vagueness also brings a high level of uncertainty (D'Amato, 1983, pp. 1–4). There is often no way for the public and private subjects alike to determine if they have successfully implemented all necessary measures and achieved what is called the state of regulatory compliance with the relevant normative standard. The only way of testing, if the implemented measures are sufficient, might be a trial or an inspection (Polčák, Harašta, & Stupka, 2016, pp. 77–80). It is obvious that this knowledge comes ex-post (e.g. after harm is done because of a technology regulated by compliance obligations) and for the most subjects, this shall be too late. It imposes an insane level of uncertainty upon them and allows the state authorities a high level of discretion at the same time (D'Amato, 1983, pp. 1–4). The subjects bound by the compliance obligation can't count on expenditures caused by a non-compliance (fines, damages) in advance and are bound to search for ways of the *apriori* assessing conformity (or compliance) with the regulation to solve this situation (Polčák et al., 2016, pp. 76–80).

[1] According to the preliminary estimation of the Commission from the year 2016 should the number of devices connected to the internet rise from 1,8 million in 2013 to 6 billion in 2020 (*Commission Staff Working Document: Advancing the Internet of Things in Europe*, 2016).

[2] That is also the case of the Czech Cybersecurity Act – see sec. 4 of the Czech Cybersecurity Act.

1.1. The certification as a conformance assessment method

One way of the *apriori* conformance assessment is a process called certification («What's the Difference Series,» 2013). Generally, it means that an independent special subject assesses the compliance of a relevant technology[3] with a certain set of rules. If the technology passes the security requirements, the conformance assessment body (so-called CAB) issues a certificate for the owner/manufacturer of the said technology. The certificate proves to the third parties that the technology has passed relevant tests and meets certain security criteria («What's the Difference Series,» 2013). It is important to note that the certificate doesn't prove the technology to be impenetrable. That would be impossible.

There is also a modified model of the general type of certification called «self-certification». It is the manufacturer/owner who tests the technology for meeting the relevant set of criteria. It is both swifter and cheaper way of the certification process, yet it institutes a lower level of trust in the certified technology. The compliance-effects are still the same, but the manufacturer/owner is completely responsible for the whole certification procedure (Axelrod, 2016, pp. 1–2).

The sets of security requirements may be defined in documents called certification schemes or standards (e.g. issued by the International Organization for Standardization; «Developing standards,» n.d.) When these sets are approved by a state to have the effect of satisfyingly fulfilling the standard of «necessary/reasonable measures», the authoritative check of conformance shields the subject against the compliance liability[4] (Polčák et al., 2016, pp. 76–80). In case of a trial or an inspection, it is then presumed that the subject fulfilled the obligation and it has to be proven otherwise. That is a much better position for the subject (Polčák et al., 2016, pp. 76–80).

1.2. The certification of the cybersecurity technologies

The certifiable cybersecurity objects can be divided into two main groups: products[5] and processes. An example of a cybersecurity process is an ISMS (Information Security Management System) which can be certified under the international standard ISO/IEC 27001 (Bârsan, 2017, p. 21). But processes are mostly out of the scope of this paper and from now on I shall mainly focus on products and services.

Probably the most advanced internationally recognized certification system for cybersecurity of products is called Common Criteria (*Common Criteria for Information Technology Security Evaluation-Part 1: Introduction and general model*, 2017) The owners/manufacturers may have their products tested for the fulfilment of specified security properties[6] by independent laboratories functioning under the supervision of the CABs. The certificates issued by the Common Criteria CABs are then recognized by all the signatories of the international agreement called the Common Criteria Recognition Arrangement (CCRA; *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security-Ratification on the 8th September 2014*, 2014; «Common Criteria,» n.d.) All of the procedures, methodologies for the assessment as well as the CABs and their relevant testing laboratories are regulated by the text of Common Criteria itself or by the supporting documents. But the advancement of Common Criteria was stopped by the lack of international trust and by many faults and gaps in the system itself. The system wasn't made for the certification of services (there is no service certified). The certification procedures are costly and very time consuming even

[3] In a general model of certification almost anything can be subjected to certification, not only technology – people, processes, products, services etc.

[4] It is a liability for not fulfilling the obligation to comply with a regulation.

[5] And services alike.

[6] The severity of the tests is determined by the assurance level required by the owner/developer. It is usually dependant upon the risk assessment of the technology itself. For example, the high assurance level certificate may prove that the technology was tested by penetration testing and doesn't obtain any known vulnerabilities. So it should withstand attacks of the defined level.

for the lowest assurance levels and because of that out of a reach for many SMEs (Hearn, 2004, pp. 64–65; Kallberg, 2012, pp. 50–52). Among other things that led to the creation of the Cybersecurity Act.

2. The Cybersecurity Act

The European cybersecurity market was shattered by numerous national certification systems and obligations that required specific technologies to be certified according to their national certification system. These systems, unlike Common Criteria, were usually not internationally recognized (Drogkaris, 2017; Mitrakas, 2018; Negreiro Achiaga, n.d.; Sparenberg & Pohlmann, 2018). So, for vendors to sell a product, which had to be certified, on a market of Great Britain, France and Germany, they had to undergo a certification procedure in all three countries. That tripled costs and time needed. Even though the national certification procedures were usually cheaper and faster than the Common Criteria certification, this fragmentation still constituted an obstacle for many European vendors and did not allow the creation of a single digital market (Drogkaris, 2017; Ježová, 2017; *Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes of the workshop*, 2014).

The Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) no 526/2013 (or shortly «the Cybersecurity Act») aims to change that. It introduces a unified certification system of products, services and processes. Certificates of this systems are to be uniformly recognized among all of Union[7] and the new certification schemes shall replace those on the national level.[8]

The Cybersecurity Act is only a framework for the new certification system, it is not a set of schemes. That would be practically impossible to maintain for any change in a scheme would require the changing of the Regulation itself.

It is important to note, that some member states (e.g. France, Germany) are much more prepared for the coming of the European certification than others (e.g. the Czech Republic) that still have to create appropriate expert capacities (testing laboratories and CABs). And because of that, parts of the Regulation concerning certification framework are still being implemented (as of the 12th December 2019) and the adaptation period should end by the 27th June 2021.[9]

2.1. Creating certification schemes

According to Article 47 of the Cybersecurity Act, the Commission shall publish by the 28th June 2020 a Union rolling work programme for the European cybersecurity certification (Programme). The Programme is a plan that identifies strategic priorities for new schemes. It shall include what products (and services and processes) would benefit from a new certification scheme, why, inspirations[10], when would such schemes come into an effect etc. Its main purpose is to prepare the stakeholders and member states for the upcoming schemes.[11]

There are two options for the creation of new schemes. Either based on the Programme or extraordinarily (in duly justified cases)[12] even without that basis.[13] Preparation is issued either by the Commission in a case that the scheme is already a part of the Programme or by the Commission or the European Cybersecurity

[7] See Article 56 of the Cybersecurity Act.

[8] See Article 57 of the Cybersecurity Act.

[9] See Article 69 of the Cybersecurity Act.

[10] If any national or international schemes could be assimilated into the new scheme.

[11] See Article 47 of the Cybersecurity Act.

[12] It is probable that in the beginning months of the certification framework, the «extraordinary» way shall be much more frequent than «ordinary». I do not expect the Programme to contain many schemes in the beginning and the need for improvisation and flexibility will be great (something like a testing phase).

[13] See Article 48 of the Cybersecurity Act.

Certification Group (ECCG, newly constituted body to help ENISA[14] in administering the framework).[15] The preparation of candidate schemes was entrusted to ENISA. For each scheme, ENISA shall establish an ad hoc working group to help them with the creation of the scheme. Also, ENISA must closely cooperate with the ECCG and even with the public.[16] There is no time limit for the preparation period even though there was one in the first draft-stages of the Act. I find this solution to be a better one because the quality of the framework depends on the quality of the schemes. And the schemes should be thorough and complex for the Act itself is composed in a very general way.[17]

When finished, ENISA submits the candidate scheme to the Commission which can (doesn't have to) approve it and adopt it in a form of an implementing act. Only then the scheme becomes active and may be used in a certification procedure. ENISA is obliged to evaluate adopted schemes afterwards (at least every five years) to improve the functioning of the framework.[18]

The Act predefines security objectives for the certification schemes in Article 51.[19] But unfortunately, the analysis of the sufficiency of these objectives goes beyond the focus of this article. However, the Act also predefines three levels of assurance: basic, substantial and high.[20] Assurance levels correspond with the risks the products may face in a relevant environment. Each scheme must contain at least one of these levels. Each level determines what should relevant cybersecurity countermeasures be capable of achieving and how severe should the testing made by the testing laboratory be. For example, cybersecurity measures of a product certified to a high level of assurance should «*minimise the risk of the state-of-the-art cyberattacks carried out by actors with significant skill and resources*.»[21] In an earlier draft-stage of the Act, there was stated an example of this danger – a hacking group backed by a state actor.[22]

2.2. The Certification Procedure

The cybersecurity certification is generally voluntary. The member states can further regulate this by their national laws and set any sort of certification as mandatory for relevant subjects.[23] But even the Commission has a say in this matter. According to Article 56 of the Act, the Commission has the power to make (after careful and thorough evaluation) a scheme mandatory for the whole Union. The first evaluation shall be carried out by 31st December 2023, a surprisingly short period of time after the launch of the framework.

Before I describe the certification procedure itself, I must introduce the two most important bodies on a national level – the National cybersecurity certification authority (NCCA) and the Conformity assessment body (same as CAB mentioned above, the Act uses the same name). NCCA is a supervisory body which is responsible for «*carrying out the will of the Cybersecurity Act*» (e.g. the performance of the CABs). In some cases, it even may act as a CAB itself (e.g. in cases of high assurance level certification). The NCCA monitors the CABs, investigates abnormalities during the certification procedures and in the certificates and enforces the rules of the Act upon all relevant subject on the territory of the member state. It shall have its representative in the ECCG and be subjected to the peer review of other NCCAs.[24]

[14] The European Union Agency for Cybersecurity.

[15] See Article 49 of the Cybersecurity Act.

[16] Ibidem.

[17] And because the Act contains a few gaps which may prove «fatal» for the framework if not addressed individually by the schemes (e.g. the procedure of revoking the certificates during peer review).

[18] Ibidem.

[19] E.g. «a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process».

[20] See Article 52 of the Cybersecurity Act.

[21] Ibidem.

[22] See the draft of the Cybersecurity Act – version from July 2018.

[23] See Article 56 of the Cybersecurity Act.

[24] See Articles 58, 59 and 62 of the Cybersecurity Act.

The CAB is the body which carries out the certification itself.[25] The Act defines very strict requirements for the operation of the CAB. Without the CABs, there is no certification, and with bad CABs, there is no security in the certification. They are without an overestimation the cornerstones of the whole framework. The creation of the CAB and relevant professionally-equipped testing laboratory is financially very demanding, and it is not impossible that there will be member states without their own CABs.

The CAB has to be accredited by the national accreditation body to have fulfilled all requirements that the Act has set out (in the Annex). Then the CAB may choose schemes according to which it will offer certification services. That is because the CAB practically can't be universally equipped for all the cybersecurity tests and it has to prioritize. The equipping of the CABs is also in the cooperating testing laboratories which have the same limitation. Unlike Common Criteria the Cybersecurity Act doesn't stipulate the requirements for the testing laboratories (except the obligation of the CABs to ensure that the laboratories used for testing meet the requirements of the relevant standard – e.g. ISO/IEC 17025). That led to an unfortunate gap in the Act where no rule forbids the CAB from using laboratories based in the third countries (e.g. Russian Federation), which is a giant security risk.[26]

The certification procedure will probably look like this. A developer who wants to or has to have their product certified (either because of national or European laws) should first consult the ENISA certification website. There shall be information about the existing and upcoming schemes as well as about the issued certificates.[27] On this website, the developer can find out if there is a relevant scheme.[28] Then the developer needs to study the scheme itself to know what is needed and what the scheme offers. The important information is the assurance level. If there are more than one, the developer should probably undergo a procedure of a risk assessment of their product to know which assurance level of the scheme is relevant for them.

The next goal of the developer is finding a competent CAB. With this, he should also consult the mentioned website for there should be a list of all the CABs and their offered scheme-services. Then the developer contacts the CAB and they enter into a contract.[29] The developer has to cooperate with the CAB even afterwards (supplying the documentation for the CAB etc.). The product is then sent to be tested in the testing laboratory and if it passes all criteria set out by the relevant scheme, the CAB shall issue a certificate.[30] If the product doesn't pass the tests and the developer doesn't agree with the CAB, there is a possibility to lodge a complaint, possibly even to take the matter to the court.[31]

The Act offers an alternative procedure for the classic certification procedure. If the scheme allows it and only for the basic assurance level, the so-called Conformity self-assessment. It is the certification procedure only without the CAB. The fulfilment of the criteria of the relevant scheme is assessed by the developer and the developer alone is responsible for the assessment procedure. This shall probably be the favourite form of certification for many subjects. The developer may «*issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated*».[32] The developer by doing so assumes responsibility for the compliance of the certified product with the requirements in the scheme.[33]

[25] See Article 60 of the Cybersecurity Act.

[26] See Article 60 and the Annex of the Cybersecurity Act.

[27] See Article 50 of the Cybersecurity Act.

[28] For the sake of this paper, let's presume there is one. There is a way even if there wasn't, but it exceeds the limitations of this brief paper.

[29] Certification shall be a commercial undertaking for CABs.

[30] And it shall inform ENISA because the existence of the certificate must be verifiable online.

[31] See Articles 63 and 64 of the Cybersecurity Act.

[32] See Article 53 of the Cybersecurity Act.

[33] See Article 53 of the Cybersecurity Act.

3. Conclusion

The Cybersecurity Act is a revolution in the world of the cybersecurity certification and if administered correctly, it is the future of the certification of the cybersecurity technologies for more than just the European Union. Having said that there are many gaps in the Regulation, and much will depend on the quality of the individual schemes.

4. Bibliography

Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security—Ratification on the 8th September 2014. https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf.

Axelrod, C. W. The creation and certification of software cybersecurity standards. 1–6. 2016. https://ieeexplore.ieee.org/document/7494112.

Bârsan, M. Aspects regarding the implementation of information security standards in organizations. Revista Română de Biblioteconomie Și Știința Informării = Romanian Journal of Library and Information Science, 13(1), 21–26. 2017. https://doi.org/10/gfgkt8.

Commission Staff Working Document: Advancing the Internet of Things in Europe. 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN

Common Criteria. (n.d.). New CC Portal website (accessed on 12. 12. 2019). https://www.commoncriteriaportal.org/.

Common Criteria for Information Technology Security Evaluation—Part 1: Introduction and general model (Version 3.1, 5th edition). 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5_marked_changes.pdf.

D'Amato, A. Legal Uncertainty. California Law Review, 71(1), 1. 1983. https://doi.org/10/d48z36

Developing standards. (n.d.). ISO website (accessed on 12. 12. 2019). http://www.iso.org/cms/render/live/en/sites/isoorg/home/developing-standards.html.

Drogkaris, P. Considerations on ICT security certification in EU – Survey Report. 2017. https://www.enisa.europa.eu/publications/certification_survey/at_download/fullReport.

Hearn, J. Does the common criteria paradigm have a future? IEEE Security & Privacy Magazine, 2(1), 64–65. 2004. http://ieeexplore.ieee.org/document/1264857/.

Hurychová, K., & Sýkora, M. Compliance programy (nejen) v České republice. Wolters Kluwer, Praha, Česká republika, 2018.

IOCTA: Internet Organised Crime Threat Assessment 2019. 2019. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019.

Ježová, D. EU Digital Single Market—Are we there yet? Ad Alta: Journal of Interdisciplinary Research, 7(2), 99–102. 2017. https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=12&sid=f9683978-876b-416a-a2d0-5fa83e889a40%40sessionmgr120.

Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes of the workshop. 2014. https://www.enisa.europa.eu/events/sog-is/minutes/view

Kallberg, J. The Common Criteria Meets Realpolitik: Trust, Alliances, and Potential Betrayal. IEEE Security & Privacy Magazine, 10(4), 50–53. 2012. http://ieeexplore.ieee.org/document/6148206/

Mitrakas, A. The emerging EU framework on cybersecurity certification. Datenschutz Und Datensicherheit, 42(7), 411–414. 2018. https://link.springer.com/content/pdf/10.1007%2Fs11623-018-0969-2.pdf

Negreiro Achiaga, M. D. M. (n.d.). EU Legislation in Progress—Briefing: ENISA and a new cybersecurity act (as of 16. 1. 2018). http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf

Polčák, R., Harašta, J., & Stupka, V. Právní problémy kybernetické bezpečnosti, 1st edition. 2016. https://is.muni.cz/auth/repo/1375719/Polcak_kniha2.pdf?fakulta=1422;obdobi=7343;kod=MV735K;predmet=1120828

Sparenberg, M., & Pohlmann, N. Cybersecurity made in EU: Ein Baustein europäischer Sicherheit. Datenschutz und Datensicherheit – DuD, 42(4), 220–223. 2018. http://link.springer.com/10.1007/s11623-018-0911-7

What's the Difference Series: Compliance vs. Certification. (2013, January 14). Retrieved October 27, 2018, from Mireaux Management Solutions website: http://mireauxms.com/vanguard-blog/whats-the-difference-series-compliance-vs-certification