The Proactive Face of Cybersecurity: Certification. Legislation and Market Response from the Perspective of ITSEF

Elżbieta Andrukiewicz and Piotr Krawiec

National Institute of Telecommunications, Warsaw, Poland

https://doi.org/10.26636/jtit.2025.FITCE2024.1984

Abstract — The first European Cybersecurity Certification Scheme according to the Common Criteria (EUCC) specifies a number of additional requirements for Conformity Assessment Bodies (CABs) to be technically competent to provide evaluation and certification services. The NIT Testing Laboratory (ITSEF) has developed a roadmap to meet these requirements and obtain the status of an authorized ITSEF that can provide assessments of ICT products at the "high" assurance level. The roadmap consists of 3 parts: one organizational part concerning the management system and two technical parts concerning evaluations. The paper presents two action points: the innovative approach that NIT ITSEF has implemented regarding the integrated management system in the laboratory in order to achieve optimal cost-benefit ratios and the reliable and verifiable methodology for calculating the attack potential that NIT ITSEF has used to prove that the penetration tests developed and executed on the evaluated software product meet the requirements of AVA_VAN.5. The roadmap will fulfill all the requirements necessary to obtain the status of an authorized ITSEF in the EUCC program.

Keywords — Common Criteria, cybersecurity certification, EUCC, ITSEF, testing laboratory

1. Introduction

Today, European legislators increasingly refer to cybersecurity certification to ensure the proper implementation of many new cyber regulations, such as the Artificial Intelligence Act, the EU Digital Identity Framework, the NIS2 Directive, and the Cyber Resilience Act. The EU requires its member states to rely on cybersecurity certification by providing proactive solutions, often referred to as "compliance" and "presumption of conformity".

The European Cybersecurity Certification Framework, adopted by the European Union in the Cybersecurity Act (CSA) [1], has a twofold objective. First, it aims to help increase trust in ICT products, ICT services, and ICT processes that have been certified under European cybersecurity certification schemes. Second, it should help avoid the proliferation of conflicting or overlapping national cybersecurity certification schemes, thereby reducing costs for businesses operating in the Digital Single Market.

In order to meet the objectives of the European Union, the first European cybersecurity certification scheme is just around the corner. The EU Cybersecurity Certification Scheme on Common Criteria (EUCC) covers the cybersecurity certification of ICT products based on Common Criteria [2] and a Common Methodology for Information Technology Security Evaluation [3] and their corresponding ISO standards, ISO/IEC 15408 and ISO/IEC 18045 respectively.

The EUCC is based on third-party conformity assessments carried out by accredited conformity assessment bodies at two levels: test laboratories providing cybersecurity evaluations and certification bodies issuing certificates based on completed evaluations.

The Common Criteria have proven to be particularly effective over the last two decades in Europe for the certification of integrated circuits and smart cards, thus contributing to increasing the security level of many ICT products, such as electronic signature devices, machine-readable travel documents (passports), bank cards, and digital tachographs.

Poland is one of eight countries in the European Economic Area (EEA) technically and organizationally prepared to evaluate ICT products and issue certificates under the EUCC umbrella. The Polish certification structure consists of an accredited certification body (located at the National Research Institute NASK) issuing cybersecurity certificates and two accredited testing laboratories, the leading and most advanced of which is part of the National Institute of Telecommunications (NIT).

In this article, we present the innovative approach we have taken at the NIT laboratory to become a fully authorized testing entity for the future EUCC scheme. This approach includes the specific implementation of a laboratory management system that seamlessly integrates the requirements of two standards, i.e., ISO/IEC 17025 and ISO/IEC 27001, achieving an optimal cost-benefit ratio.

Furthermore, we propose a reliable and verifiable methodology for calculating the attack potential to prove that the penetration tests developed and executed on the evaluated software product meet the high requirements of AVA_VAN.5 (vulnerability analysis). The proposed methodology fills the gap experienced in software product assessments that require high attack potential due to the lack of any direct references to catalogs containing descriptions of relevant attacks. By using highly systematic methodologies, the NIT laboratory achieves the goals of its roadmap, which aims to meet all the requirements necessary to obtain the status of an authorized laboratory in the EUCC program.

2. Related Works

The EU Regulation [4] sets the entry-in-force date of the EUCC on 27 February 2025. As a result, all stakeholders who play their roles in the cybersecurity certification ecosystem have begun final preparations to achieve readiness.

It should be noted that the EUCC scheme follows the pattern of existing schemes used for Common Criteria certificates: certification and evaluation services are provided by different Conformity Assessment Bodies (CABs), called Certification Bodies (CBs), and Testing Laboratories called IT Security Assessment Facilities (ITSEFs). ITSEFs provide cybersecurity evaluation services and CBs issue certificates after the successful completion of ITSEFs' evaluations.

For the assurance level "substantial", no restrictions are provided in [4], except that the CAB must be accredited. The national accreditation body grants accreditation if the CAB meets all the requirements specified in certain international standards. There is no limit to the number of CABs operating in Europe.

However, in order to provide services at the assurance level "high", the certification and evaluation capabilities of the relevant CABs must be additionally confirmed by the National Cybersecurity Certification Authority (NCCA), designated in each Member State. According to [4], separate requirements refer to specific technical domains, that is, "Smart Cards and Similar Devices" and "Hardware Devices with Security Boxes", and ITSEFs demonstrate their capabilities to develop and conduct penetration tests with a specified attack potential. CABs can demonstrate their capabilities in specific application areas and, after successful assessment, the NCCA grants the relevant authorization.

The preparation process in the different existing national schemes will vary depending on the complexity of the conformity assessment body structure and current operational practices in the Member State. An interesting overview of the strategy and its implementation for the German EUCC national structure is given in [5] and [6] and for the Netherlands in [7].

However, a critical factor is that the process of preparing the accreditation requirements, according to [4], has not yet been completed. For example, the state-of-the-art document [8] describing the accreditation requirements for certification bodies contains a reference to the ISO/IEC 19896-3 standard, which is still under development. This standard is needed in the context of the EUCC because it deals with the competence management system to be applied to certifiers.

From a vendor perspective, the certification process is similar to those conducted in the national Common Criteria schemes gathered in the SOG-IS MRA [9]. Certification and evaluation service providers offer workshops, guidelines, and other types of communication to vendors to increase awareness and knowledge. However, this may be only a technical part of the vendor's concerns. Vendors generally express concerns about the additional obligations included in [1]. They point to a shift in responsibility for disclosing and handling vulnerabilities that may be identified in the certified product and other information obligations that are new to them. The fees and penalties in case of inappropriate demonstration of fulfilling the obligations by the vendor, appear to be enormous.

Furthermore, vendors may be negatively affected by the lack of mutual recognition of certificates issued under the EUCC scheme and national certification schemes outside Europe, mainly collected under the global Common Criteria Recognition Arrangement (CCRA) [10]. The lack of mutual recognition may be seen as an additional barrier to the recognition and acceptance of non-EU cybersecurity certificates. It should be noted that around 50% of Common Criteria certificates are issued outside of Europe [11]. A long-term lack of mutual recognition can harm the prospects of the global cybersecurity certification market.

3. Conducted Research

NIT ITSEF began operations in 2019. Since its inception, the ITSEF concept has been based on three principles:

1) ITSEF provides levels of confidentiality and integrity of the target of evaluation equivalent to the assurance level at which the evaluation is conducted,
2) The security requirements for the test laboratory are constructed in exactly the same manner as for the site(s) where the target of evaluation is developed,
3) The ITSEF maintains a constructive interaction with the NIT Cybersecurity Department, which is responsible for cybersecurity research and development (R&D) activities.

The preparation of ITSEF to achieve readiness of ITSEF for EUCC started immediately after the publication of CSA [1]. ITSEF recognized three work packages:

1) Organizational, which covers accreditation requirements for ITSEF,
2) Technical, to support ITSEF authorization; it covers completion of at least one successful evaluation of software products with an attack potential of at least AVA_VAN level 4 of vulnerability assessment class and in accordance with a specified European standard,
3) Technical, to support ITSEF authorization; it covers proving the technical capability of ITSEF to evaluate one or two technical domains, i.e. "Smart Cards and Similar Devices" and "Hardware Devices with Security Boxes".

On the date of submission, the first two work packages have been completed. The third is under development. As such, NIT ITSEF will be the first test laboratory in Poland authorized to conduct ICT product evaluations at the "high" assurance level.

3.1. An Innovative Approach to the ITSEF Management System

Looking at CSA regulations [1], there is a general lack of security requirements to protect the evaluation process, including maintaining the confidentiality and integrity of the evaluation target, its documentation and the evaluation results. Considering that meeting the accreditation requirements is the only prerequisite to provide evaluation and certification services at the "substantial" assurance level, a significant information security gap has been identified.

To cover the gap, ITSEF should seek independent confirmation that it is adequately managing information security. If market acceptance is essential for the ITSEF business model, such a management system should be based on the widely recognized international standard ISO/IEC 27001. The question is how to verify that all requirements are implemented correctly and perform as expected.

One option is to include the requirements of the Information Security Management System (ISMS) in the scope of accreditation. Unfortunately, this is not acceptable for the National Accreditation Body (NAB), as they cannot include in the scope of the accreditation audit requirements that could be subject to conformity assessment activities performed by entities covered by other accreditation programs. In this case, the ISMSs are certified by entities accredited to ISO/IEC 17021 and ISO/IEC 27006. NABs cannot accept the appearance of a conflict of interest. However, the NAB will respect a certificate confirming that the ITSEF ISMS is compliant with ISO/IEC 27001 if issued by an accredited certification entity.

The solution requires a huge workload for ITSEF to implement two management systems, one for laboratory activities and one for information security. However, taking into account the legal loopholes and formal constraints and following its original principles, NIT ITSEF has developed a unique approach to the management of its laboratory activities by defining one integrated management system that covers all topics, with a significant reduction of the efforts initially assessed. The concept is presented in [12]. The main steps to develop integrated management systems include the following:

- establishing an unified scope of both management systems,
- integrating security objectives with the primary process implemented in ITSEF,
- identifying standard components of the management system,
- identify parts of the management system that must be kept separately,
- implementing an appropriate system for documentation management,
- ensuring continuous support from top management,
- implementing awareness and training programs.

During the initial analysis, several parts are identified as the same or similar. These include:

- the context of the organization (ITSEF in this case),
- risks and opportunities in the management system,
- system procedures and related records (internal audits, management review, document control, corrective actions, continual improvement).

Then, several parts of the management system are closely related, and these include:

- information security and quality objectives,
- dealing with vendors and subcontractors,
- supporting assets, i.e. information systems, environmental and physical facilities,
- personnel competence management.

Finally, some parts of the management system should remain separate, and these include:

- ISO/IEC 27001: information security risk management, security of sites and IT facilities,
- ISO/IEC 17025: evaluation methodology and related activities.

The ITSEF integrated management system has successfully passed the relevant audits, and ITSEF is accredited (as of 2021) and certified (as of 2023). Experience gained during the maintenance of the integrated management system shows that the overhead for the integrated system is small. In 2024, when detailed requirements for the EUCC program were published [4], it became clear that the ISMS fully covers the extension of the accreditation requirements for information security implemented and successfully operating in the NIT ITSEF.

3.2. Challenges in Evaluations of Software Products with the Highest Attack Potential

The second important aspect of ITSEF readiness for the EU-CC program is the ability to conduct evaluations of software products with the highest attack potential. Document [4] indicates two European standards that include protection profiles that require ITSEF to be used in evaluations with the highest attack potential (AVA_VAN.5).

The target of evaluation in the case under consideration was a software component of Trustworthy System Supporting Server Signing, which offers a remote qualified electronic signature as a service. The Signature Activation Module (SAM) component is responsible for authorizing the signing operation by checking whether: a) the signer authentication is correctly associated with the signing key and the data to be signed, and b) the signer is authenticated.

To ensure that the signer has exclusive control over the signing key, the signing operation is authorized by the SAM, which verifies a specific set of signature activation data (SAD) received from the signer via a dedicated application located on the server and activates the signing key in a cryptographic module (CM), both located in a protected environment. SAD verification means that the SAM checks the validity and integrity of the SAD elements and verifies that the signer is authenticated.

The SAM security specification and related security assurance requirements are included in the protection profile published in the European standard [13]. With respect to the security assurance requirements, the standard states that the vulnerability assessment should be performed with the attack potential indicated in the security assurance component AVA_VAN.5. Paper [13] does not provide any detailed methodology for developing appropriate penetration tests with such high attack potential.

Furthermore, no commonly recognized sources provide attack methods that could be relied upon for the evaluation of software products. Hence, the most challenging part of the ITSEF work was to develop tests and prove that the actual attack potential for these tests is equal to or higher than that indicated in the component AVA_VAN.5.

The starting point for the development of the methodology was the general approach to calculating the attack potential presented in [14]. Determining the attack potential corresponds to identifying the effort required to create an attack and demonstrating that it can be successfully applied to a specific object, thereby exploiting a vulnerability in that object.

When analyzing the attack potential required to exploit a vulnerability, the following factors should be considered:

- Time to identify and exploit (Elapsed time) – refers to the total time it takes an attacker to identify that a specific potential vulnerability may exist in targeted object, to develop an attack method, and to exert the effort required to attack that object.
- Technical expertise required (Specialist expertise) – refers to the level of general knowledge of the underlying principles, type of product, or attack methods (e.g., Internet protocols, Unix operating systems, buffer overflows).
- Knowledge of the design and operation of an object (Knowledge of the targeted object) – refers to specific specialized knowledge about the object (e.g., access to the source code and the ability of the evaluator to interpret and exploit it).
- Window of opportunity – refers to the identification or exploitation of a vulnerability that may require significant access to the target, which can increase the likelihood of detection. Some attack methods may require offline effort, and only short access to the target may be exploited. Access may also need to be continuous or over several sessions.

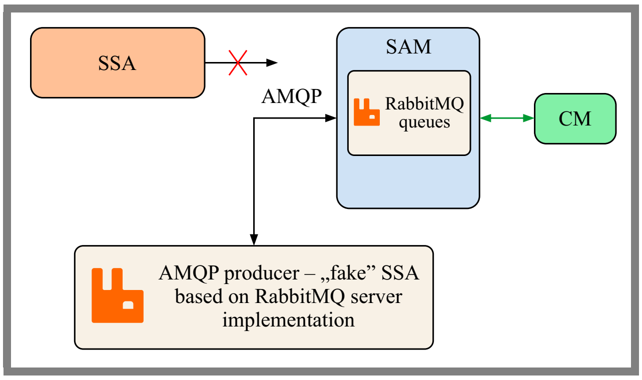
SSA
SAM
AMQP
RabbitMQ queues
CM
AMQP producer – „fake" SSA based on RabbitMQ server implementation

Fig. 1. Penetration test with the fake queue requester.

- IT hardware/software or other equipment required for exploitation – refers to the equipment required to identify or exploit the vulnerability (this may be standard, specialized, or bespoken equipment and generally measures equipment availability and cost).

Each factor is appropriately assessed, and an arithmetic value appropriate to the target of evaluation is assigned based on predefined rating tables. The attack potential is expressed as a score calculated by adding the values of all factors.

The general values given in [14] are intended to be replaced or refined according to the context (technology, type of product, etc.). Defining the set of values shared in each community is a non-trivial achievement. The leading CSPN framework [15] dedicated to pure software products has developed a set of factors and associated values derived from the general outline given in the specification [14].

The set of factors used in CSPN [15] is as follows:

- Time taken for the exploitation – it relates directly to the factor Elapsed time specified in [14],
- Attacker expertise – relates directly to the factor Specialist expertise specified in [14],
- Knowledge required by the attacker – relates directly to the factor Knowledge of the targeted object specified in [14],
- Access to the product by the attacker – it relates directly to the factor Window of opportunity specified in [14],
- Type of equipment needed – this factor is assumed from IT hardware/software or other equipment by simplifying the rating by using two levels: standard and specialized software tools.

In the performed evaluation, the methodology from [15] has been applied.

Furthermore, another reference source was considered to further validate the approach. The Common Vulnerability Scoring System (CVSS) methodology, described in [16], has been widely used by the IT security community for many years and is suitable for software products. When assessing the criticality of an identified vulnerability, one dominant factor called "attack complexity" is subject to rating. The "attack complexity" factor refers to the concept of the attack potential. It is defined as a metric that captures the measurable actions that must be taken by an attacker to actively avoid or bypass existing built-in security enhancement conditions in order to obtain a working exploit.

According to [16], when the attack complexity is considered "high", the successful attack depends on evasion or circumvention of security enhancing techniques in a place that would otherwise hinder the attack. The attacker needs to gather some knowledge about a specific target to carry out the final successful attack. To obtain specific information, the attacker must carry out additional attacks or otherwise break the security measures.

To present the methodology for calculating the attack potential, let us consider one attack developed for a given object. This attack is presented in detail in [17].

Tab. 1. Calculation of the attack potential for the test case.

Attack potential factor, based on the approach in [15]	Value	Score	Remarks
Time taken for (identification and) exploitation	$>$ 1 month	7	Two distinct types of software are to be investigated, and in-depth fuzzing is required
Attacker expertise	Multiple experts	8	The attack was needed to develop complex software
Knowledge required by the attacker	Critical	11	The source code was reviewed to find potential vulnerabilities
Access to the product by the attacker	Easy	1	Access to the front-end application as the user without any privileges
Type of equipment required	Specialized software	2	See the category “attacker expertise”
Total		29	Over 25, i.e. **Very High**

Tab. 2. The attack categories for the technical domain of “Hardware Devices with Security Boxes”.

Attack category	Exemplary attack
Physical security invasive	Sensors removal and deactivation, removing and penetration potting materials, attack to an anti-tamper processor
Physical security semi-invasive	Perturbation test using a laser beam
Physical security non-invasive	Reverse engineering, power consumption analysis, emanation analysis, timing analysis
Electromagnetic and sound attacks	Monitoring keyboard sound or emanation, microwave scanning
Random number generation feature	Entropy analysis searching weaknesses
Software attacks off-device	Direct protocol attacks, man-in-the-middle and reply attack
Software attacks on the device	Secure operating system, hypervisor, virtual machine
PIN and cryptographic key-related	Limit key encryption key search by value, weakly padded PIN blocks

The penetration test aimed to deceive the authentication procedure provided by the SSA component and force the cryptographic module CM to sign an unauthenticated request from a fake signer. To do this, a fake queue requester was prepared and fake requests were made including false parameters (see Fig. 1). Another goal of the test was to force the service to crash and reject each request. The calculation of the attack potential relevant to the penetration test is presented in the Tab. 1.

It should be noted that the final calculation of the attack potential was further verified using the approach of [16] and the attack complexity value was evaluated at the level of “high”. Therefore, the methodology for calculating the attack potential was shown to be correct and verifiable.

4. Future Work

The third work package is still under development. It aims to demonstrate the technical capabilities of NIT ITSEF in one of the two technical domains envisaged by [4] for the application for authorization. The domain “Hardware Devices with Security Boxes” requires ITSEF be capable of performing the most advanced attacks with the attack potential of AVA_VAN.5. However, for such types of evaluated products, there is a set of state-of-the-art attack methods [18]. This means that ITSEF shall perform numerous attack categories, as shown in the Tab. 2.

The NIT ITSEF already covers most of the test methods presented in the Tab. 2 in the pilot evaluation required by [4]. Some of them still require additional effort to be completed and documented accordingly.

5. Conclusions

The requirements for ITSEFs that evaluate ICT products at the “high” assurance level [1] are challenging. AVA_VAN.5 is described in the Common Evaluation Methodology (CEM) [3] only in general terms, leaving room for certification schemes to specify detailed requirements that depend on technical domains or technologies.

The highest attack potential means that an appropriate methodology will be adopted, which on the one hand must be compliant with the CEM, but on the other hand must be specific to the relevant attacks. The accreditation of test laboratories creates a significant advantage, since the basic principle of performing any tests under accreditation is the validation of the method and tool before testing.

The test laboratory management system, in the context of the EUCC, should include many security requirements due to the high sensitivity of the objects to be assessed and the test results. The best way is to integrate a management system for the quality and security of laboratory activities.

References

[1] European Parliament and the Council, *Regulation (EU) 2019/881 of the of April 17 2019*, No. 526/2013 (Cybersecurity Act) (https://eur-lex.europa.eu/eli/reg/2019/881/oj).

[2] Common Criteria for Information Technology Security Evaluation (CC:2022), Revision 1, November 2022 (https://www.commoncriteriaportal.org/index.cfm).

[3] Common Methodology for Information Technology Security Evaluation (CEM:2022). Revision 1. Standard developed by the Agreement on the Recognition of Common Criteria Certificates in the field of IT Security (CCRA). November 2022 (https://www.commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf).

[4] European Parliament and the Council *Commision Implementing Regulation (EU) 2024/482 of 31.1.2024* (http://data.europa.eu/eli/reg_impl/2024/482/oj).

[5] F. Bollman and K. Geyer, "Transition from National to the EUCC Scheme – BSI's Strategy for Supporting the Product Manufacturers and the ITSEFs during the Transition Phase", *2022 International Conference on the EU Cybersecurity Act*, Brussels, Belgium, 2022 (https://eucyberact.org/wp-content/uploads/2022/05/S22a-GeyerK.pdf).

[6] F. Bollman, K. Geyer, "Implementation of the EUCC Scheme in Germany: First Observations and the Way Forward", *International Conference on Cyber-Security & Resilience Act*, Brussels, Belgium, 2024.

[7] W. Slegers, "Implementation of and Transition to EUCC", *International Common Criteria Conference (ICCC'23)*, Washington DC, USA, 2023.

[8] Draft Accreditation of CBs for the EUCC Scheme, Version 1.6a, 2024 (https://certification.enisa.europa.eu/publications/draft-accreditation-cbs-eucc_en).

[9] Senior Officials Group – Information Systems Security, Mutual Recognition Arrangement (SOG-IS MRA), 2024 (https://www.sogis.eu/uk/mra_en.html).

[10] Common Criteria Recognition Arrangement (CCRA) (https://www.commoncriteriaportal.org/).

[11] J.M. Pulido, "2023 CC Certification Report", *International Common Criteria Conference (ICCC'23)*, Washington DC, USA, 2023.

[12] E. Andrukiewicz, "Unexpected Side Effect of the CSA – How CABs Could Demonstrate Their Competency in Information Security Area? ITSEF Use Case", *International Common Criteria Conference (ICCC'21)*, 2021.

[13] iTeh Standards, EN 419241-2:2019 – Trustworthy Systems Supporting Server Signing – Part 2: Protection Profile for QSCD for Server Signing.

[14] ISO, "Methodology for IT Security Evaluation", ISO/IEC 18045:2022 (https://www.iso.org/standard/72889.html).

[15] France's National Agency for the Security of Information Systems (ANSSI), "Procedure – Criteria for Evaluation in View of a First Level Security Certification", 2020.

[16] FIRST, "Common Vulnerability Scoring System version 4.0: Specification Document", 2024 (https://www.first.org/cvss/v4.0/specification-document).

[17] E. Andrukiewicz and P. Krawiec, "Use Case Related to the Software Product Evaluated with the Highest Attack Potential", *International Common Criteria Conference (ICCC'22)*, Toledo, Spain, 2022.

[18] Application of Attack Potential to Hardware Devices with Security Boxes Version 1.2, 2023 (https://certification.enisa.europa.eu/publications/application-attack-potential-hardware-devices-security-boxes_en).

Elżbieta Andrukiewicz, Ph.D.
ITSEF Manager
https://orcid.org/0000-0002-1030-6332
E-mail: e.andrukiewicz@il-pib.pl
National Institute of Telecommunications, Warsaw, Poland
https://www.gov.pl/web/instytut-lacznosci

Piotr Krawiec, Ph.D.
ITSEF Technical Manager
https://orcid.org/0000-0002-2395-5155
E-mail: p.krawiec@il-pib.pl
National Institute of Telecommunications, Warsaw, Poland
https://www.gov.pl/web/instytut-lacznosci