

Proactive face of cybersecurity – certification: legislation and market response



Dr. Piotr Krawiec

ITSEF Technical Manager

Dr. Elżbieta Andrukiewicz

ITSEF Manager,

National Institute of Telecommunications

– State Research Institute



63rd FITCE INTERNATIONAL CONGRESS

New technologies and services for cybersecurity opportunities and threats

26 September 2024, Kraków, Poland

Agenda

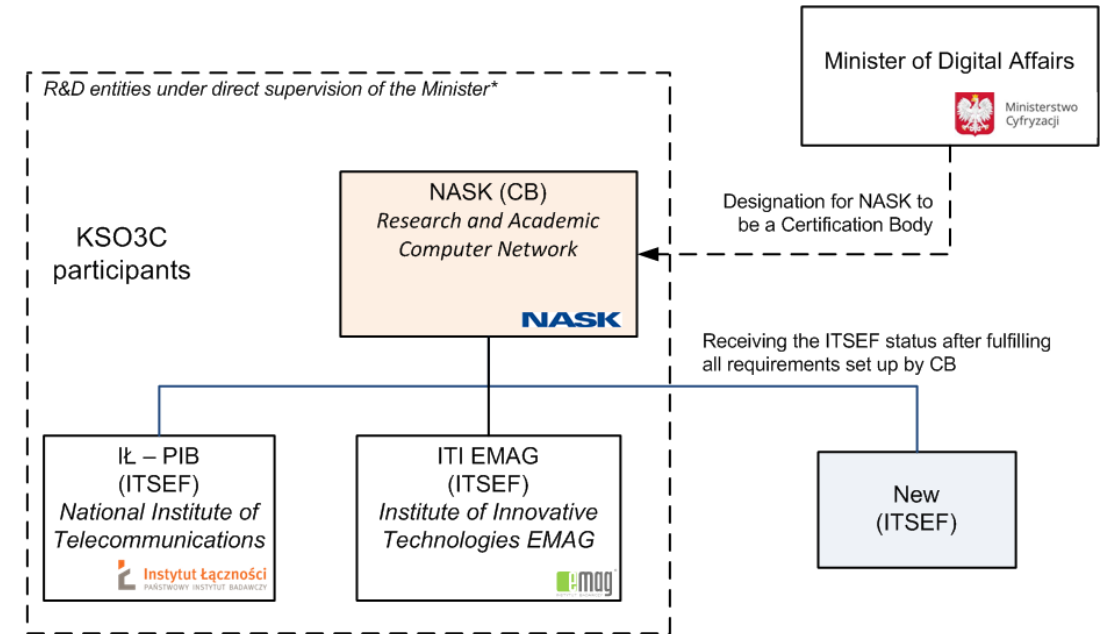
- The landscape of cybersecurity certification of ICT products in Europe and worldwide – now and in the near future, after the first European cybersecurity certification scheme enters into force
- Polish national IT security evaluation and certification scheme compliant with Common Criteria
- Brief analysis of the market: ICT products categories which fall into the Common Criteria cybersecurity certification
- Accredited ITSEF (IT Security Evaluation Facility) in the National Institute of Telecommunications – brief overview
- ITSEF NIT cybersecurity certification capabilities in response to the legislation and market challenges

Current landscape of the Common Criteria cybersecurity certificates: CCRA and SOG-IS MRA

- CCRA (Common Criteria Recognition Arrangement), <https://www.commoncriteriaportal.org/>
- SOG-IS MRA (Senior Officials Group – Information Security Mutual Recognition Agreement), <https://sogis.eu>
- Principles of both arrangements are very similar:
 - Reference standards: Common Criteria (ISO/IEC 15408) and Common Evaluation Methodology (ISO/IEC 18045)
 - Common CC Portal of certified ICT products and protection profiles
 - Procedures and *modus operandi*
 - Status of participants:
 - Consumer Participant (recognition of certificates issued by other participants)
 - Authorized Participant (issuing certificates and recognizing certificates issued by other participants)



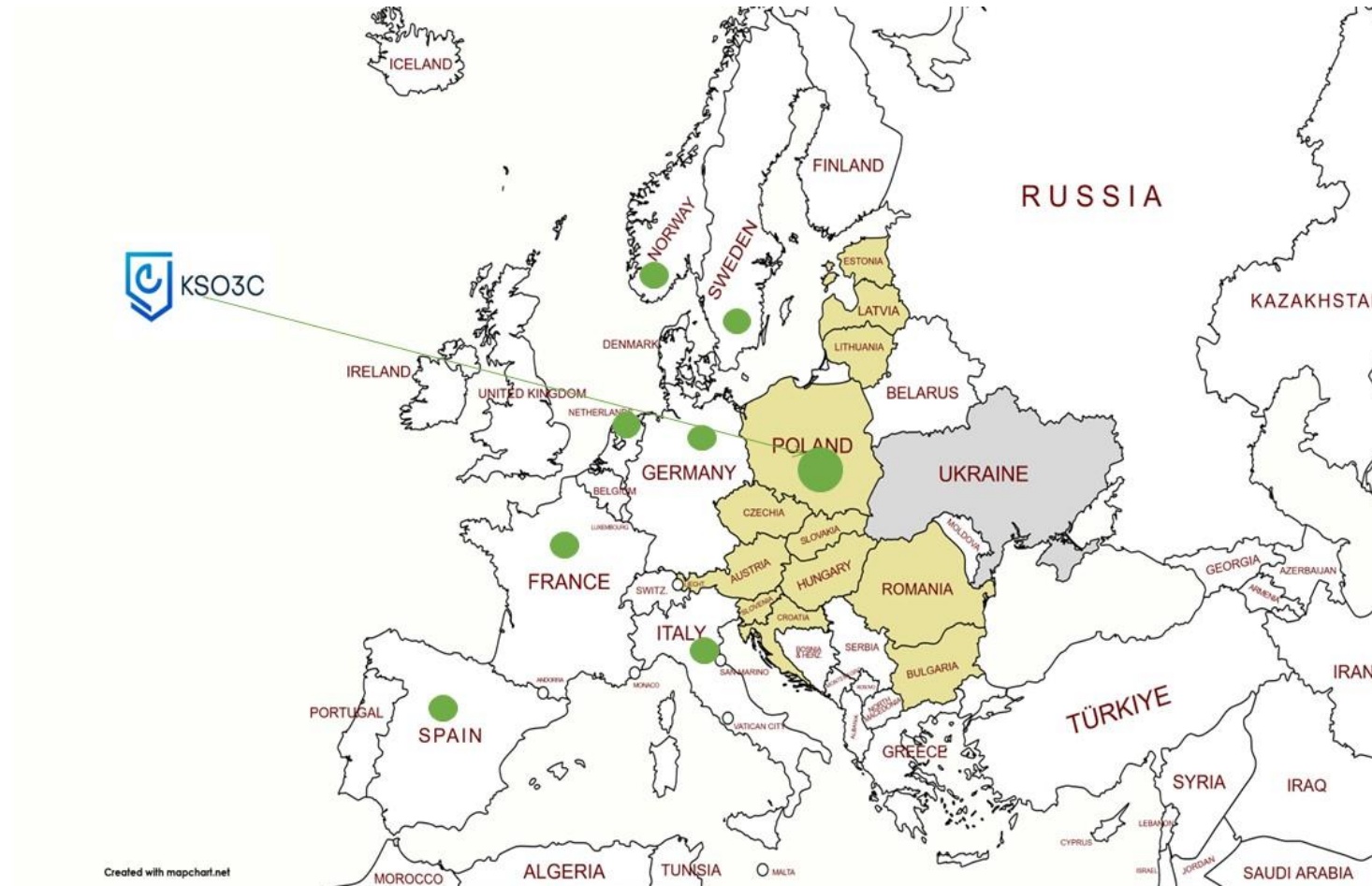
Polish evaluation and certification scheme compliant with Common Criteria



*at the beginning of the Project (2018)

- National evaluation and certification scheme compliant with Common Criteria (Polish acronym: KSO3C) – R&D Project financed by National Centre of Research and Development, conducted in 2018-2022
 - The project objective was to develop the Polish scheme which is capable to issue globally recognized cybersecurity certificates
- KSO3C is present in mutual recognition arrangements as Authorized Participant since 2022

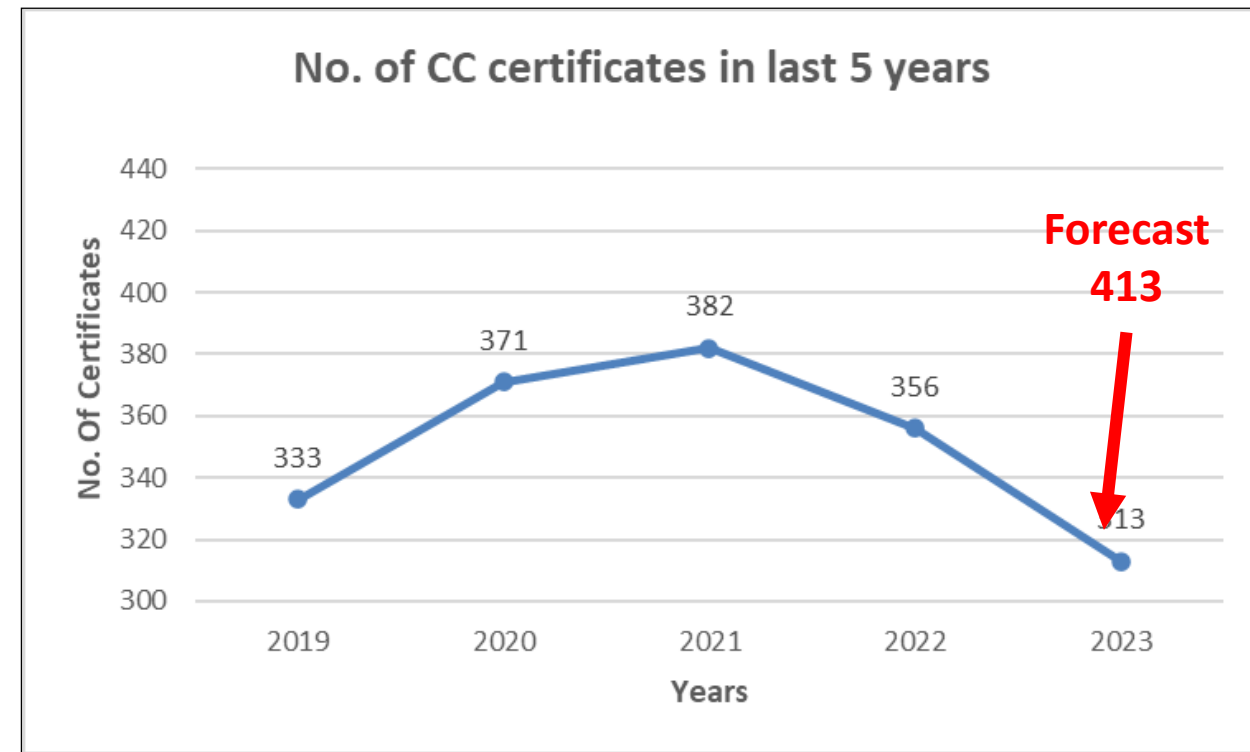
CC landscape in Europe



- Eight European countries are capable to issue CC certificate which are mutually recognized

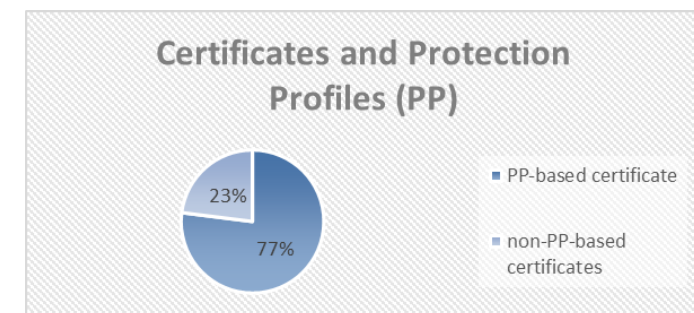
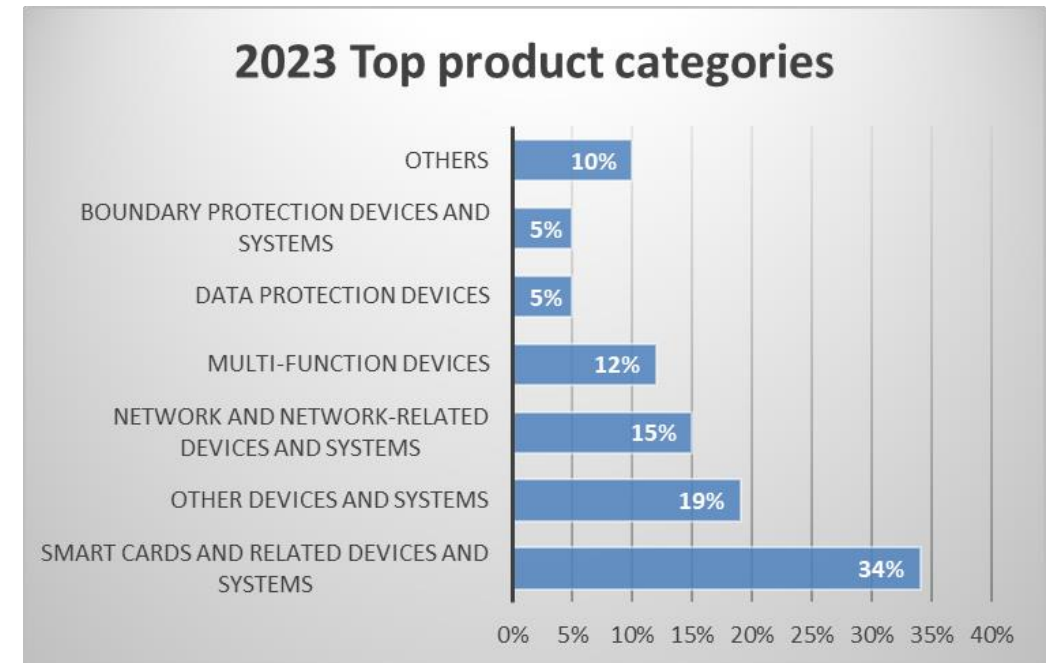
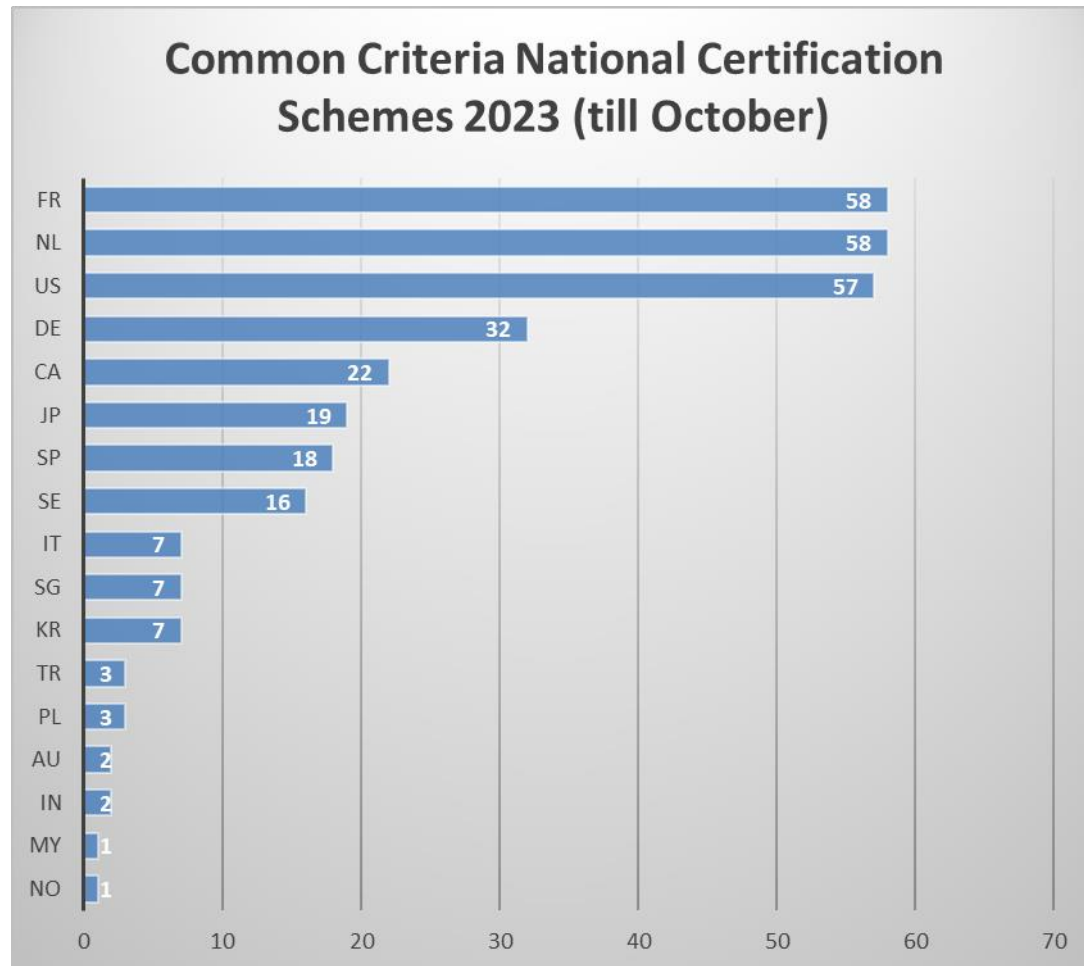
CC certification market in numbers

- Almost all certificates issued under national schemes gathered in the CCRA and SOG-IS MRA are presented at the CC portal <https://www.commoncriteriaportal.org/products/index.cfm>
- Validity period for the certificate is 5 years
- Obsolete certificates are moved to the archive
- More than 2100 certificates at the moment



Source: <https://www.jtsec.es/papers/CC/ICCC%202023%20Statistics%20Report.pdf>

CC certificates in numbers – ICT product statistics in 2023



Source: <https://www.jtsec.es/papers/CC/ICCC%202023%20Statistics%20Report.pdf>

EU Regulation 2019/881 – the Cybersecurity Act is a game changer

7.6.2019

EN

Official Journal of the European Union

L 151/15

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)

(Text with EEA relevance)

- A certificate issued under the European cybersecurity certification scheme is automatically recognized in all EU Member States
- National certification schemes with the same scope will be gradually withdrawn
- New conformity assessment mechanism: self-assessment and declaration of conformity from the vendor

Two dimensions of the framework – first dimension

- Object of certification
 - ICT product - means an element or a group of elements of a network or information system
 - ICT service - means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems
 - ICT process - means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service

Two dimensions of the framework – second dimension

- *Assurance level* - means a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated
 - basic, substantial, high
- Required assurance level shall be proportional to the level of risk of **intended use** of the ICT product, ICT service or ICT process considering the likelihood of the incident occurred and the incident consequences
 - Assurance levels differ in a scope, rigour and depth of the security evaluation

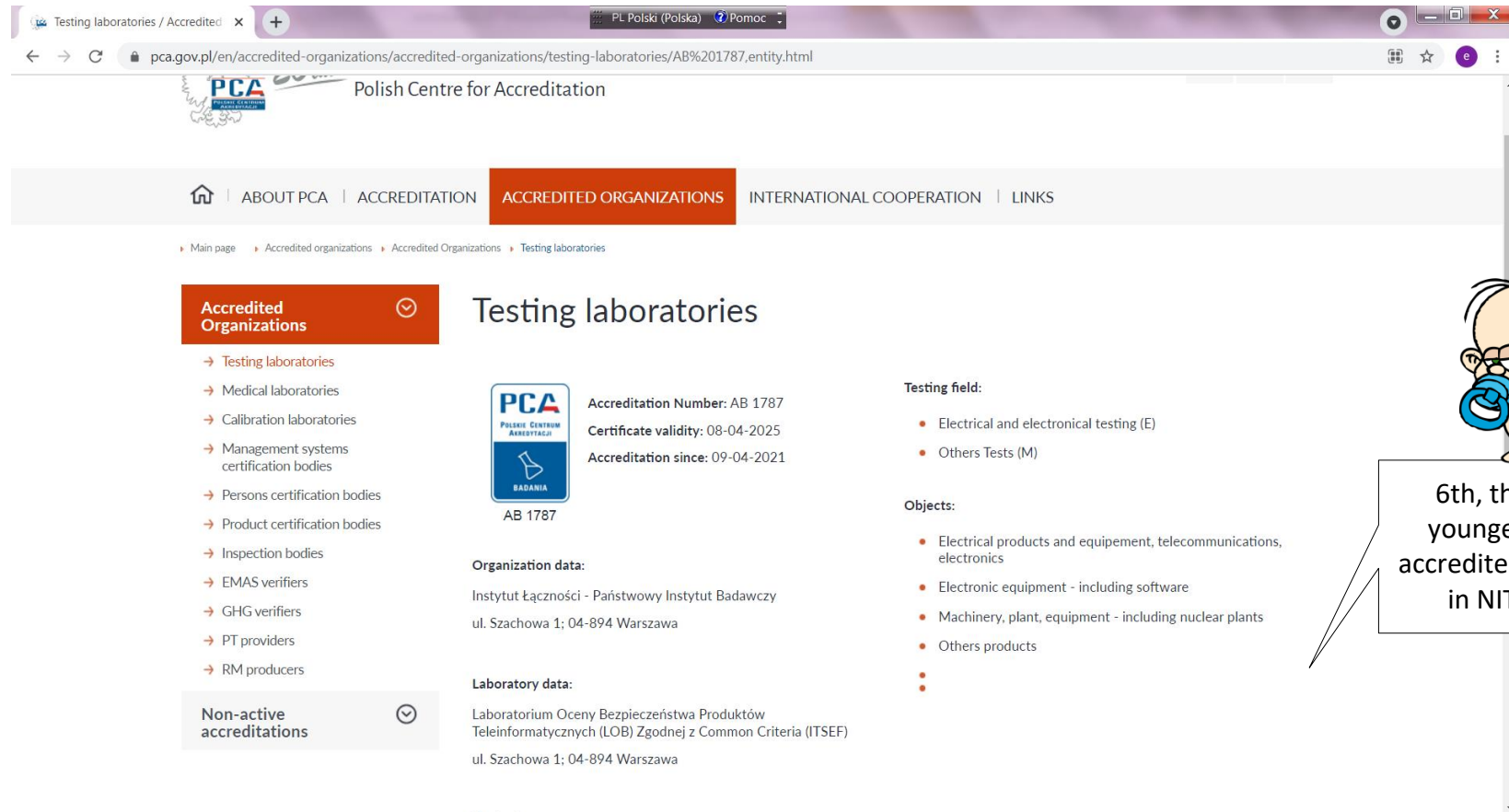
Applicability of the CSA

- As a horizontal act, the CSA encompasses mandatory certification stipulated by different vertical legal acts, e.g.:
 - Machine reading of travel documents,
 - Qualified electronic signature and seal devices (eIDAS regulation)
 - Digital tachographs
 - General machinery directive
 - Implementing act for Radio Equipment Directive (RED) – every radio devices with ability to be connected to the network runs into the certification scope (36-month vacatio legis)
- In general, certification is voluntarily, but...
- The CSA authorizes the European Commission to introduce mandatory certification in the scope of **operating** European cybersecurity certification scheme
 - Example: NIS2 Directive for essential services and their operators

What is happening now: the CSA implementation

- EUCC – first European cybersecurity certification scheme
- EUCC is the successor of SOG-IS MRA
 - The implementing act for EUCC was issued in 1Q 2024
 - The effective date for EUCC is 27 Feb 2025
 - Transition period for national schemes– 12 months from the effective date
 - **Polish scheme is prepared to meet all EUCC requirements for issuing cybersecurity certificates**
- In development:
 - EUCS – for cloud services
 - **EU5G – for 5G network equipment, system and services**
 - EUcrypto – in preliminary phase

Accredited ITSEF in the National Institute of Telecommunications



Testing laboratories / Accredited

PL Polski (Polska) Pomoc

pca.gov.pl/en/accredited-organizations/accredited-organizations/testing-laboratories/AB%201787,entity.html

PCA Polish Centre for Accreditation

ABOUT PCA | ACCREDITATION | ACCREDITED ORGANIZATIONS | INTERNATIONAL COOPERATION | LINKS

Main page > Accredited organizations > Accredited Organizations > Testing laboratories

Accredited Organizations

- Testing laboratories
- Medical laboratories
- Calibration laboratories
- Management systems certification bodies
- Persons certification bodies
- Product certification bodies
- Inspection bodies
- EMAS verifiers
- GHG verifiers
- PT providers
- RM producers

Non-active accreditations

Testing laboratories

PCA
POLSKIE CENTRUM AKREDYTACJI
BADANIA
AB 1787

Accreditation Number: AB 1787
Certificate validity: 08-04-2025
Accreditation since: 09-04-2021

Organization data:
Instytut Łączności - Państwowy Instytut Badawczy
ul. Szachowa 1; 04-894 Warszawa

Laboratory data:
Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych (LOB) Zgodnej z Common Criteria (ITSEF)
ul. Szachowa 1; 04-894 Warszawa

Testing field:

- Electrical and electrical testing (E)
- Others Tests (M)

Objects:

- Electrical products and equipment, telecommunications, electronics
- Electronic equipment - including software
- Machinery, plant, equipment - including nuclear plants
- Others products

6th, the youngest accredited lab in NIT

PCA
POLSKIE CENTRUM AKREDYTACJI
BADANIA
AB 1787

<https://www.pca.gov.pl/en/accredited-organizations/accredited-organizations/testing-laboratories/AB%201787,entity.html>

Scope of accreditation – in detail

- Evaluation services based on Common Criteria/ Common Evaluation Methodology (equivalent to ISO/IEC 15408/18045 reference standards) – one of two testing laboratories in Poland
- Accreditation includes the AVA_VAN.5 assurance component which demonstrates the laboratory's capabilities to conduct penetration tests with the highest attack potential according to Common Criteria – the only one laboratory in Poland
- Conformity assessment for cryptographic modules against EN ISO/IEC 19790 „Security requirements for cryptographic modules” (equivalent to FIPS 140-3) – the only one accredited laboratory in Poland
- Demonstrated capabilities to be authorized CAB providing evaluation services with assurance level „high” under EUCC – the only one in Poland



What makes us unique in cybersecurity?



- IT Security evaluation services are focused on providing confidence for customers – ITSEF offers level of security in evaluations which is appropriate to the level of security of ICT product subject to evaluation
 - Certified ISMS for the same scope as the scope of accreditation – integrated management systems compliant with ISO/IEC 17025 and ISO/IEC 27001
- Full accountability for each evaluation task
- All information systems that support activities of the laboratory are physically and logically separated from the Institute infrastructure
- High security of data center with strong technical controls
 - Defined events that cause secure shutdown of IT systems
- R&D activities constitute a big part of the ITSEF work
- We are ready for providing services under EUCC, for commercial part of the scheme (assurance level ‚substantial’)
- For evaluations with high assurance level we need special authorization from the Ministry of Digital Affairs, and this part of our activity is still under development (mainly formalities)

- Certainly, cybersecurity certification will grow in relevance to European legislation (NIS2 Directive, the Cyber Resilience Act, to name a few)
- Steps towards mandatory certification (radio devices, including 5G, critical infrastructure, essential services) seem to be certain, and the market is gradually aware of that
- European cybersecurity certification schemes are emerging (5G network equipment, IoT devices, secure elements in automotive industry - approx. 20 candidates are waiting in the European Commission, not being processed yet)
- Active participation in European cybersecurity certification to follow European priorities requires significant financial support and the vision of development, and in the NIT we are challenged by this obligation
- Building national capacities in the scope of cybersecurity evaluation is necessary to provide cybersecurity expertise for key areas of national economy, public authorities and social development
- **In long-term perspective, stable financial support for developing and maintaining the cybersecurity evaluation capacity is crucial for the national security**

Thank you for your attention
Dziękujemy za uwagę

<https://www.gov.pl/web/instytut-laczności/lob>

Dr. Elżbieta Andrukiewicz
Dr. Piotr Krawiec

 @Instytut.Laczności  @IL_PIB