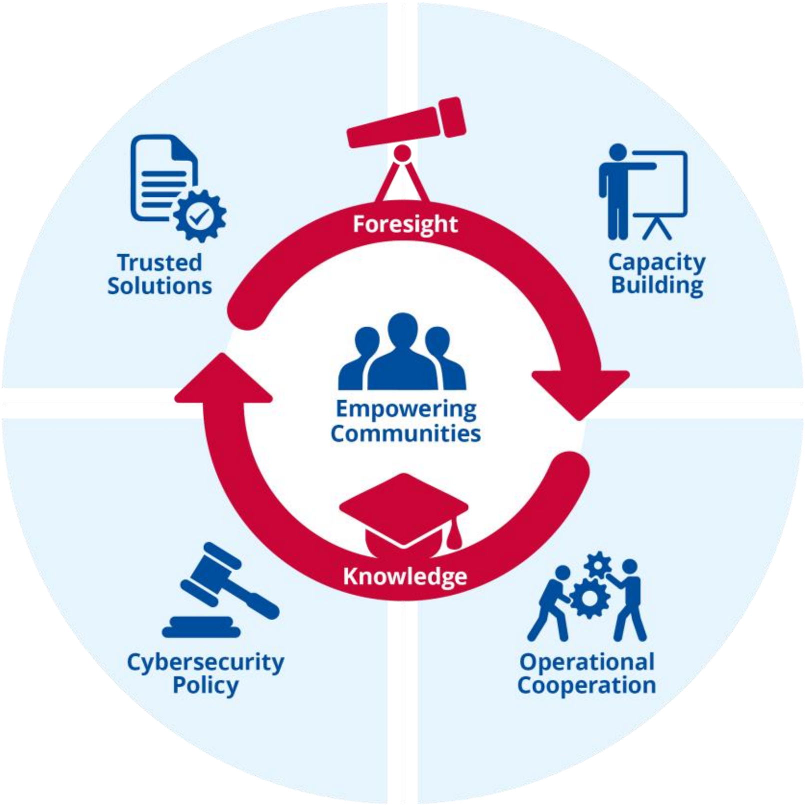
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

AI AND CYBERSECURITY

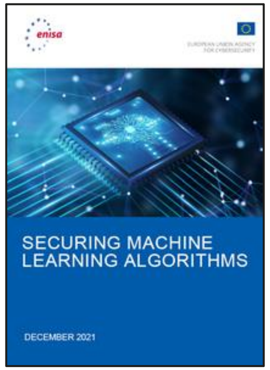
Corina PASCU
Cybersecurity Expert

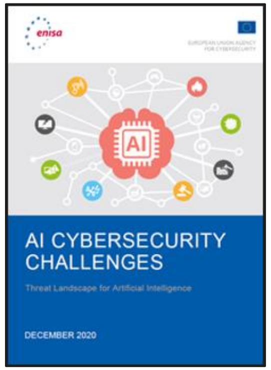
24 01 2025

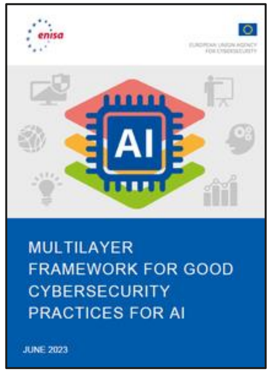
*Our mission is to achieve a **high common level of cybersecurity across the Union***

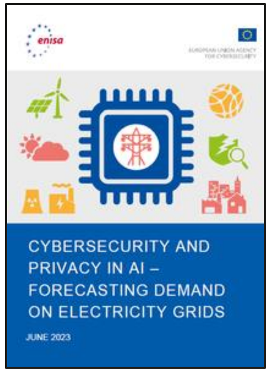


ENISA GUIDANCE ON AI AND CYBERSECURITY

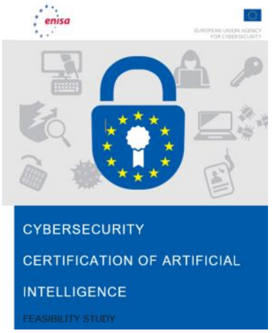




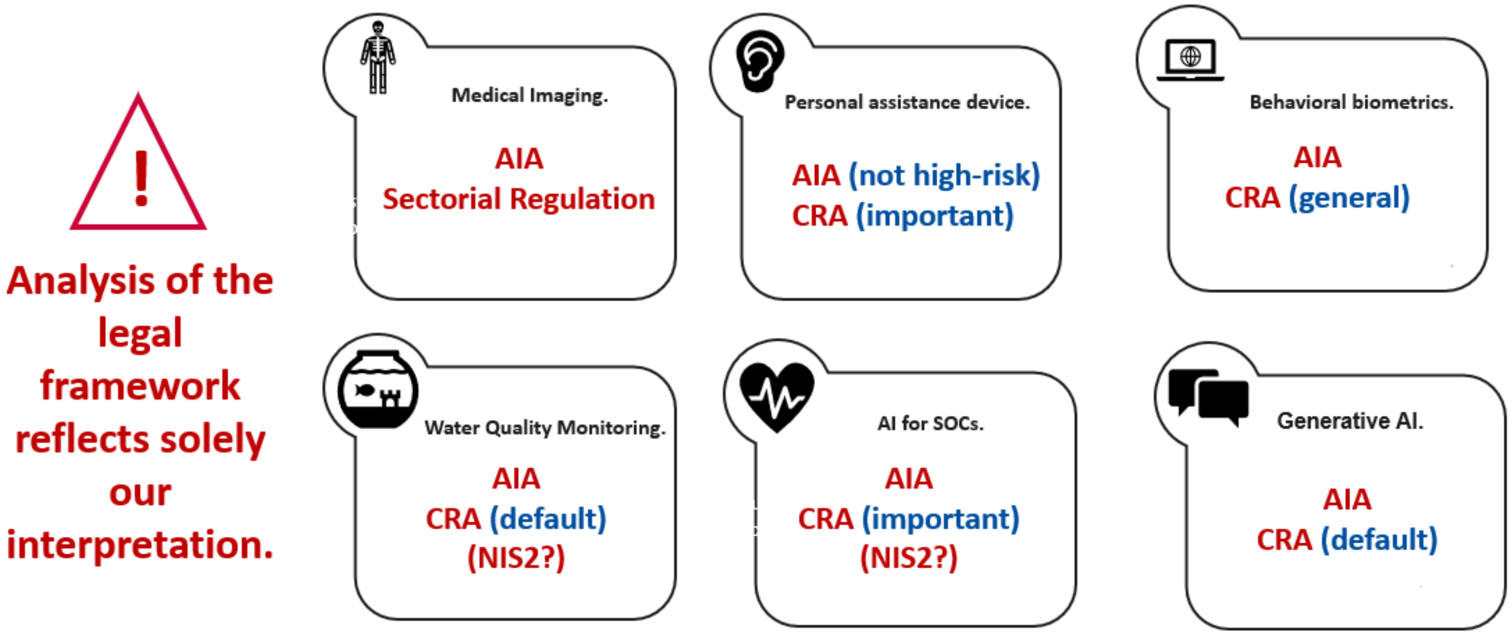




UNDERSTANDING CYBERSECURITY CERTIFICATION STRATEGIES FOR AI



OUR 6 USE CASES AND THEIR REGULATORY UNIVERSE



Publication Q1 2025 at
https://certification.enisa.europa.eu/index_en

UNDERSTANDING CYBERSECURITY CERTIFICATION STRATEGIES FOR AI

Challenges:

- Re-training / continuous learning AI systems
- Non-cybersecurity aspects of trustworthy AI and potential relationships with confidentiality / integrity / confidentiality of the AI System *

Differences between use cases:

- Regulatory requirements, including conformity assessment procedures
- Risk profile, threat landscape, operational environment
- Lifecycle management
- Evaluation activities
- Performance and reliability requirements
- Sensitive data and privacy concerns *(n.b.: we have looked only into the cybersecurity perspective)*

UNDERSTANDING CYBERSECURITY CERTIFICATION STRATEGIES FOR AI – SOME PRELIMINARY RESULTS

Prerequisites for a cybersecurity certification to cover AI systems:

- Extension of EUCC and EUCS to cover some AI-specific security controls, through the development of extended security functional and assurance components, as well as protection profiles for EUCC, and extension profiles for EUCS
- Designing ICT products considering dynamic composition e.g. composition between different certification possibilities
- Designing organizational standards to cover AI-specific threats and security controls
- Development of specific evaluation standards for AI/ML.
- Development of guidelines to support risks assessments for case specific AI systems

It’s a feasibility study, not a full-fledged AI cybersecurity scheme. Results are encouraging and offer another angle to ENISA’s work.

NEXT STEPS- A TEASER

- Publication of the report soon (Q1 2025) on the certification website https://certification.enisa.europa.eu/index_en

- An open consultation regarding the AI feasibility study and welcome input by the community (Q1 2025)

THANK YOU FOR YOUR ATTENTION

https://certification.enisa.europa.eu/index_en

European Union Agency for Cybersecurity
Agamemnonos 14, Chalandri 15231
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu