EUROPEAN UNION AGENCY
FOR CYBERSECURITY

# EMERGING TRENDS IN EDGE COMPUTING SECURITY: PRIVACY, PQC, AND DIGITAL TWIN CERTIFICATION

Akis Kourtis, Ph.D. - Researcher
National Center for Scientific Research “Demokritos”
Contact: akis.kourtis@iit.Demokritos.gr

10 | 12 | 2024

# CONTENT

Challenges

Current opportunities & Next Steps

Questions & Contact Details

# SECURITY CHALLENGES IN FOG AND EDGE

## Decentralized Architecture

- Diverse and distributed edge nodes increase attack surfaces
- Lack of centralized control demands advanced trust mechanisms.

## Privacy Concerns

- Handling sensitive data at the edge raises issues of data sovereignty.
- Ensuring compliance with GDPR and other regulations is critical.

## Trust and Certification

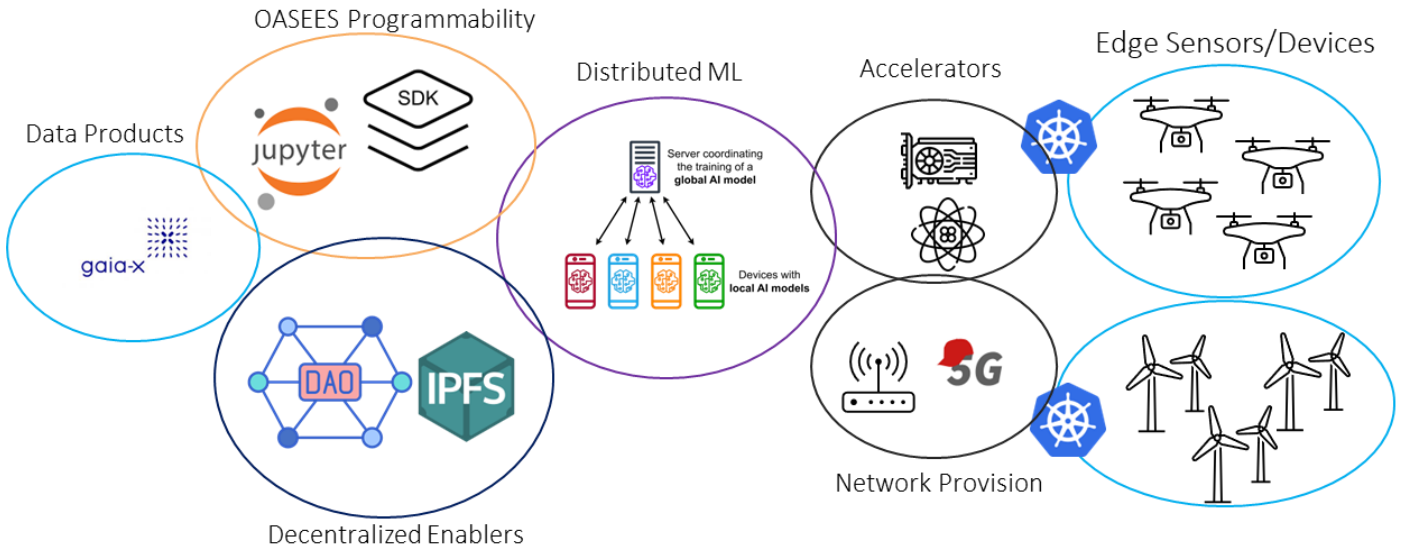
- Certification for edge devices across industries is inconsistent.
- Need for unified models like Digital Twinning for secure process validation.

## Post-Quantum Threats

- Quantum computing threatens traditional cryptographic methods.
- Migration to post-quantum cryptography is necessary to future-proof systems.

# DECENTRALIZED ARCHITECTURES & PRIVACY – OASEES APPROACH

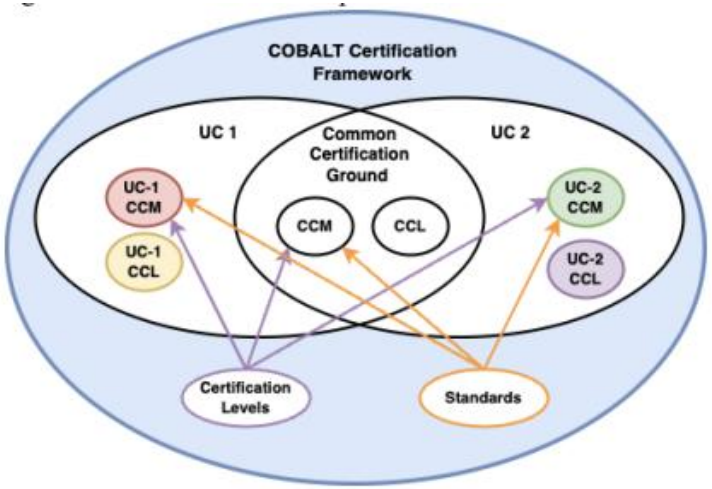
- Blockchain based - Decentralized Autonomous Organization (DAO):
  - Enables self-governance and secure orchestration of edge devices.
- Swarm Intelligence:
  - Facilitates collaboration among smart nodes without reliance on centralized entities.
- Self-Sovereign Identity (SSI):
  - Ensures privacy-preserving Object ID federation.
- Zero-Trust Model:
  - Continuous validation of device integrity across the compute continuum.

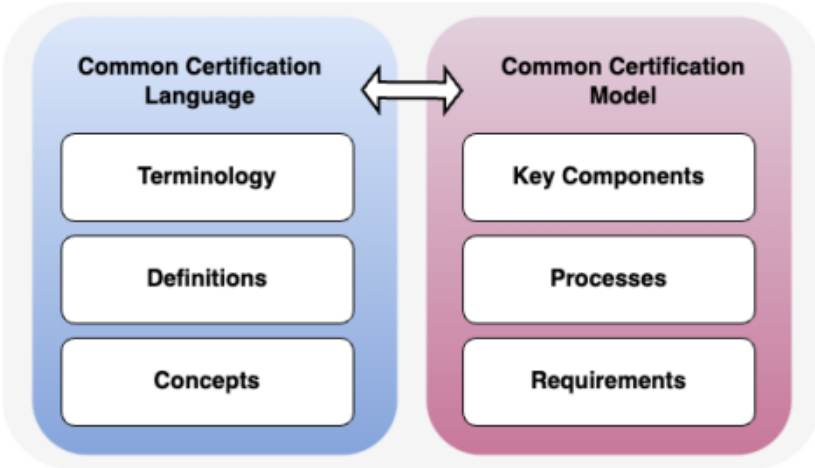


# STRENGTHENING TRUST AND CERTIFICATION – COBALT APPROACH

Lack of consistent cybersecurity certification across industries.

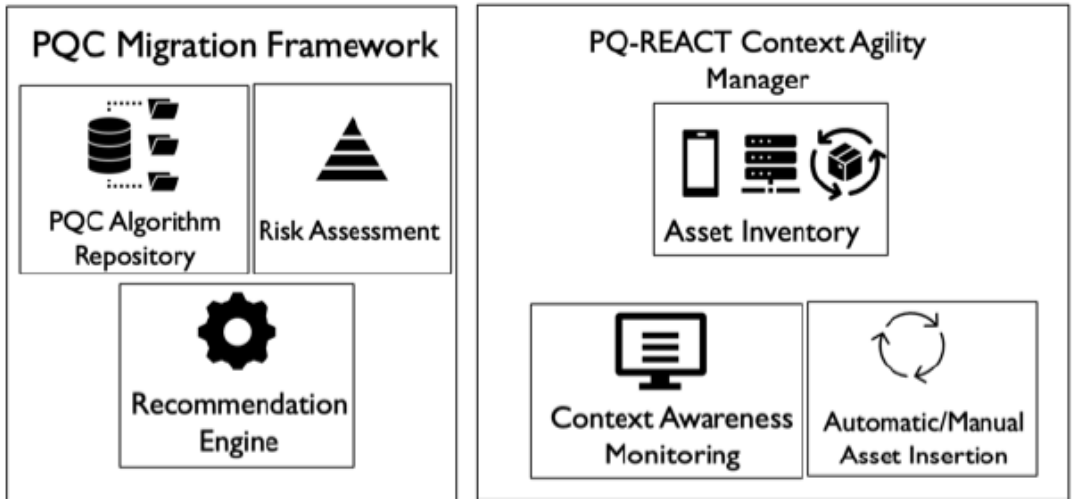
- Digital Twinning
  - Real-time modeling and validation of physical entities in digital counterparts.
- Common Certification Model (CCM):
  - A harmonized approach for ICT products and processes.
- Continuous Audit Mechanisms:
  - Supports dynamic security assessment and lean re-certification.



# ADDRESSING POST-QUANTUM THREATS

- Traditional cryptographic algorithms are vulnerable to quantum attacks.
- Cryptographic Agility:
  - Framework for seamless migration to PQC across various platforms, incl. Edge.
- Hybrid Solutions:
  - Combines classical and PQC algorithms to ensure interoperability during transitions.
- Context Awareness Manager:
  - Ensures algorithm selection aligns with device and network capabilities.
- PQC + QKD Integration:
  - Secures critical 5G and IoT networks with combined quantum-safe approaches.



# THANK YOU FOR YOUR ATTENTION

Dr. Akis Kourtis
National Centre for Scientific Research “Demokritos”

+306948386769 akis.kourtis@iit.demokritos.gr Ln: https://www.linkedin.com/in/akis-kourtis-phd-a2970b49