Co-funded by
the European Union

MERIT

The evolution of Digital Identity: The IAM Pillar and Beyond

Exploring the Results of the MERIT EU project

Umberto Morelli (Fondazione Bruno Kessler)

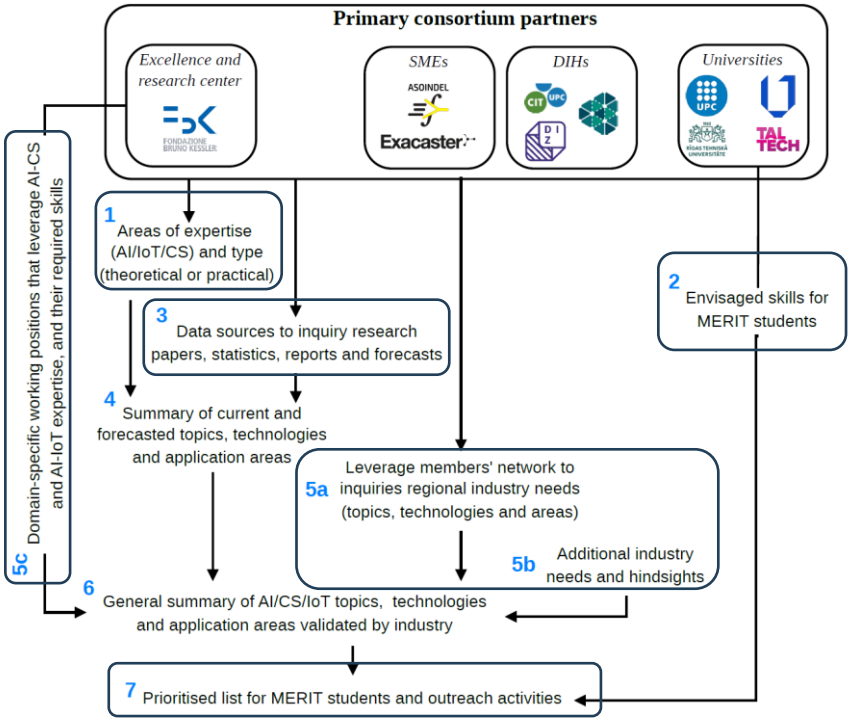
4th International Workshop on Trends in Digital Identity (TDI 2026)

MSc degrees in Smart, Secure and Interconnected Systems

- A Multi-Regional Digital Ecosystem: 5 specialized EU master programs in AI, Cybersecurity and IoT, designed to bridge the advanced digital skills gap.
- A Cross-Sector Consortium: A collaborative network of Universities, Research Centres (FBK), and SMEs, currently training 300+ specialists across two student cycles.
- The "MERIT Engine": A rigorous 7-step methodology that annually synchronizes academic curricula with real-time market needs and technological shifts.

https://digitalmerit.eu/

The 7-steps methodology



ESCO European classification of Skills, Competences, Occupations and Qualifications

European e-Competence Framework

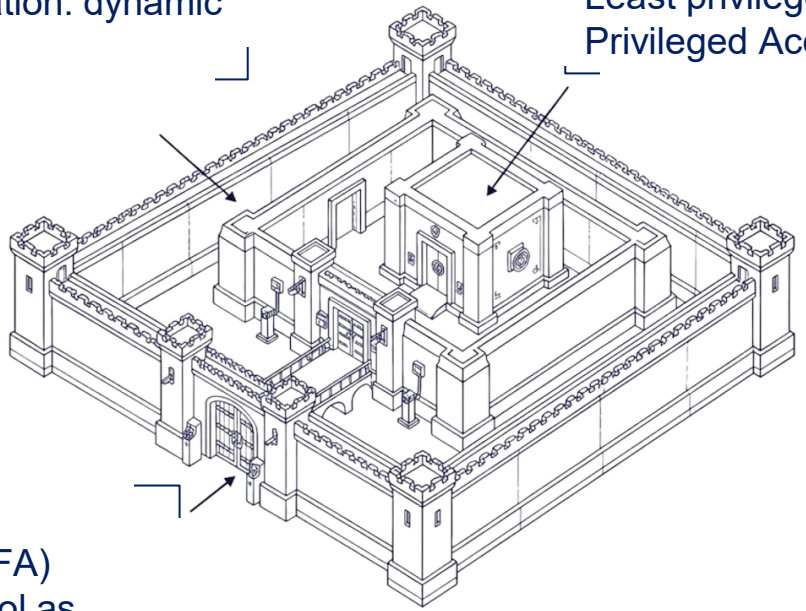
ELSEVIER Scopus

Mapping with MERIT courses

Year 1 (2023) – The IAM bedrock

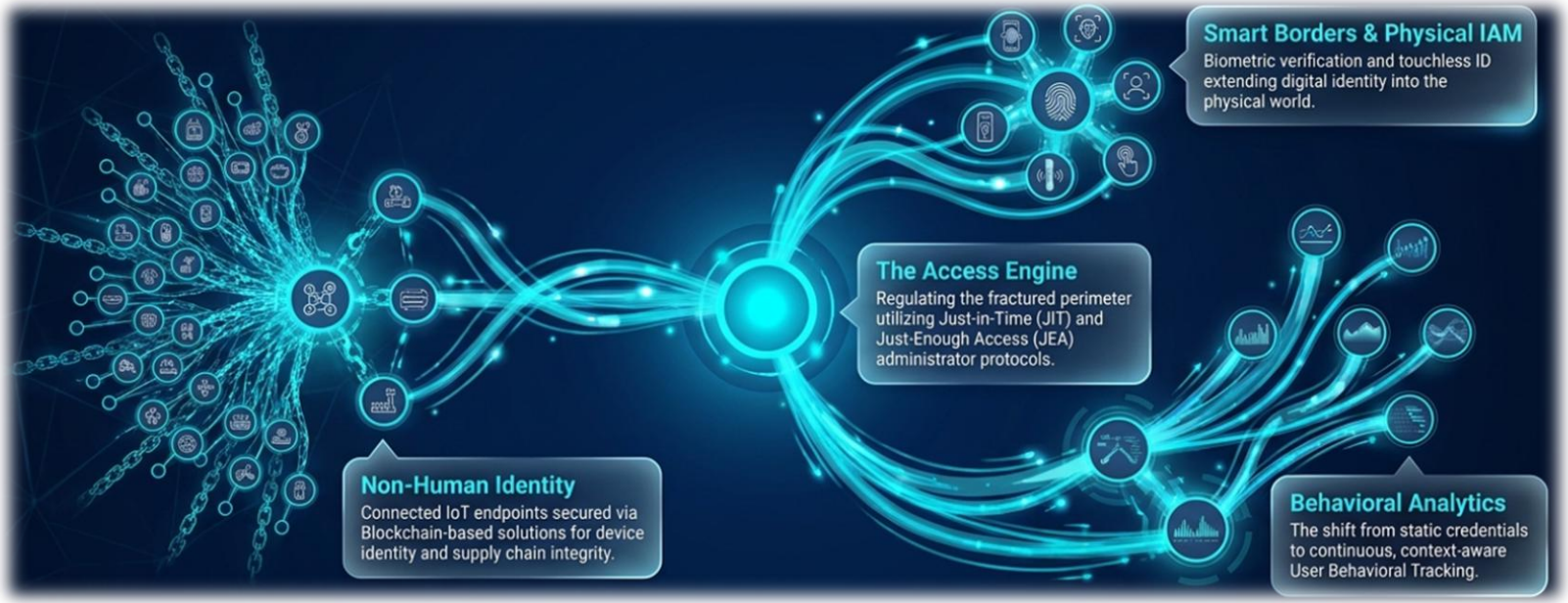
The Inner Ward
Preliminary AI-CS integration: dynamic risk evaluation

The Vaults
Least privilege (JEA/JIT) and Privileged Access Workstations (PAWs)

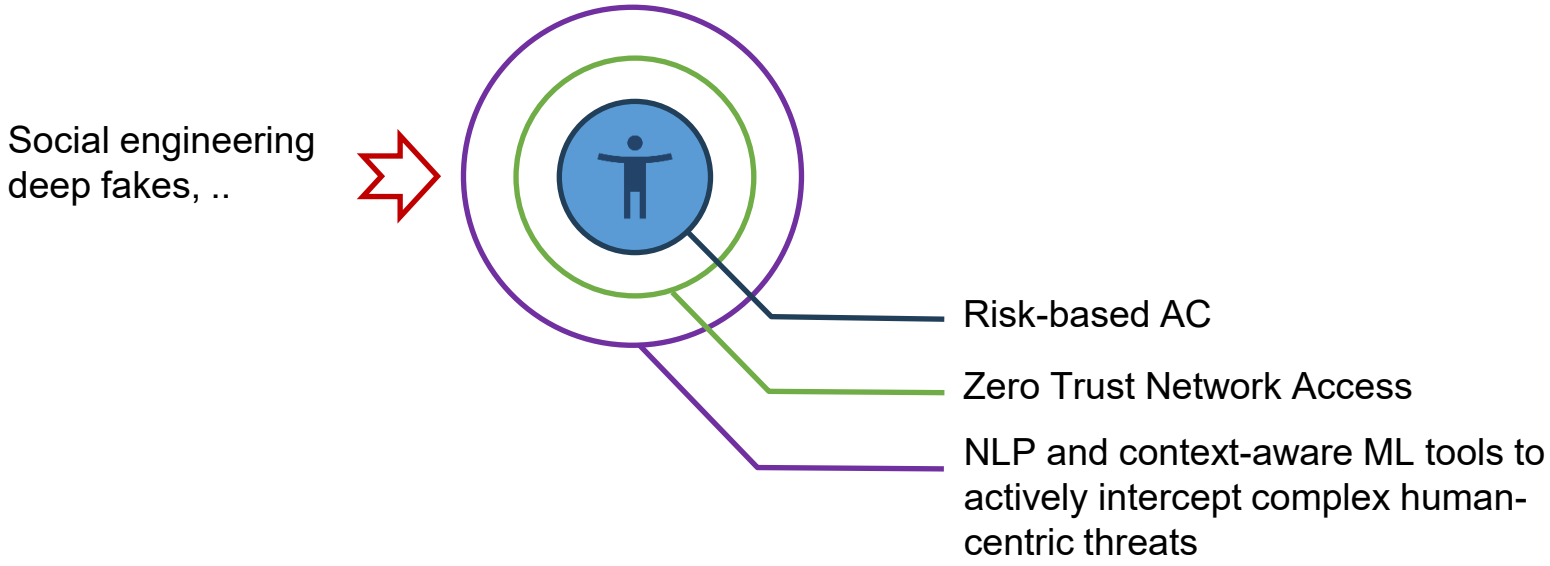


The Gateway
Multi-factor Authentication (MFA) and Conditional Access Control as the primary, immovable entry gateways

Year 2 (2024) – Identity at the distributed edge



Year 3 (2025) – Ai-driven Zero Trust defenses



Year 4 (2026) – IAM as the adaptive identity fabric

Secure users and devices:

- **Phishing detection and social engineering analysis**
  -> Deepfake detection and active mitigation against synthetic media
  -> Phishing resistant MFA and passkeys
- **Securing IoT ecosystems and device-level anomaly detection**

Cross-domain expertise

- CS+AI or CS+IoT valued up to 12% (salary increase)

Proactive resilience, driven by aligning with EU legislations

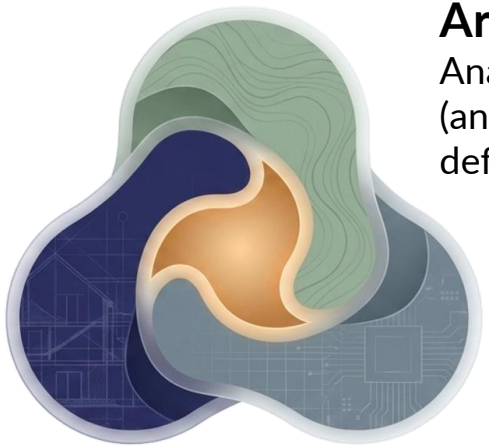
➔ **Build on current security mechanisms**

➔ **Prepare for NIS3**

The interdisciplinary imperative

Artificial Intelligence
Analytics
(anomaly detection, deepfake defence, agentic AI)

Cybersecurity
SOTA protections
(Zero Trust, IAM, Encryption)



Internet of Things
Physical context
(edge telemetry, device-oriented security)

Digital Identity requires professionals who can navigate those three (or more) disciplines simultaneously to protect complex systems

IAM evolution (2023-2026)

MERIT

Year 1 (D 3.1)	Year 2 (D 3.3)	Year 3 (D 3.4)	Year 4 (D 3.5)
Approach Foundational	**Approach** Cyber-physical	**Approach** Zero Trust & AI	**Approach** Human-centric
Key technologies MFA, PAW, Conditional AC	**Key technologies** Biometrics, Touchless ID	**Key technologies** ZTNA, risk-based threat modelling	**Key technologies** Passkeys, deep-fake detection
Focus Infrastructure and policies	**Focus** UX and smart borders	**Focus** Dynamic Beha-vioural Analysis	**Focus** Defend from social engineering

The modern security paradox

Advanced ZTNA architectures, Autonomous AI detection, post-quantum cryptography

Up to 85% of all security breaches

The User

Technology has never been so advanced, but
the weak link has changed: the perimeter is not the digital wall, but the human layer

Shaping the Digital Trust of the future

IAM evolved from a static security pillar into a living, adaptive ecosystem

- From a technological conformity to “anthropocentric resilience”
- From static authentication to continous intelligence

Academia and industry share the same mission: Co-create interdisciplinary cyber defenders

- Up to 12% salary increase when proficient in two or more of the AI/CS/IoT domains

D3.5 Results: the Cybersecurity list

Adaptive Identity & Human-Centric Defense	Expertise & Topics: - Designing workflows that mitigate Human-Centric Security & Social Engineering threats (**X1**). - Managing complex Identity and Access Management (IAM) systems.
	Technologies: Deploying Deepfake Detection (**X2**) to counter synthetic media attacks.
	Application Area: Focuses primarily on the Human Layer (Workforce & Digital Identity).
Zero Trust & Critical Infrastructure Architecture	Expertise & Topics: - Mastering Zero Trust Architecture (ZTA). - Network Defense & DDoS Mitigation to protect IoT, OT, and Critical Infrastructure Security (**X1, X2**). - Cloud Security & Infrastructure (**X1**).
	Technologies: Implementing Cloud-native application protection platforms (CNAPP).
	Application Areas: - Protecting Critical Infrastructure & OT (**X1**). - Manufacturing & Industry 4.0 (**X1, X2**). - Cloud Environments & Virtual Infrastructure (**X1**). - The Government & Defense Industrial Base.
Autonomous Cyber-Ops & Resilience	Expertise & Topics: - Integrating Threat Intelligence into Incident Response (IR) and Resilience workflows (**X1**).
	Technologies: - AI-Powered Defense & Agentic AI for automated response (**X1**). - SIEM & SOAR Platforms for orchestration. - Threat Intelligence & Deception Platforms.
	Application Area: AI Ecosystems.
Quantum-Ready Privacy & Data Persistence	Expertise & Topics: - Applying Data Security & Privacy Engineering principles to protect sensitive assets (**X1**).
	Technologies: - Confidential Computing for data-in-use protection. - Post-quantum cryptography to stay ahead of future decryption threats. - Immutable backup systems for disaster recovery.
Ecosystem Integrity & Compliance Governance	Expertise & Topics: - Managing Supply Chain & Third-Party Risk Management (TPRM) (**X1**). - Ensuring compliance with frameworks like the AI Act or NIS2 (**X1**).
	Technologies: Software Bill of Materials (SBOM) and provenance tracking tools.
	Application Areas: managing the Software Supply Chain & Third-Party Vendors.

X1 - in line with MERIT HEIs vision for their students.

X2 - Relevant from the academic perspective (Scopus)

ESCO: 102 possible working positions