Horizon Europe | *Civil Security for Society*

4. Destination – Increased Cybersecurity

Call – Increased Cybersecurity 2023

Session Chairs:

- *Ana Ayerbe Fernandez-Cuesta (Tecnalia)*
- *Jeannette Klonk (FFG)*

Increased Cybersecurity

#	ACRONYM	Organisation	Presenter
HORIZON-CL3-2023-CS-01-01: Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)			
1	ARIES	gradiant	Lilian Adkinson
2	NewCTI	Amadeus	Vincent Rigal
3	CLEARANCE	citypassenger	Yohann Cornilliere
CL3-2023-CS-01-02: Privacy-preserving and identity management technologies			
4	PERSONA	Defence Research Institute	Alessandro Marani
5	eID Wallet	Locknest	Pierre Le Roy
6	enhancedCTI	gradiant	Lilian Adkinson

Increased Cybersecurity

#	ACRONYM	Organisation	Presenter
CL3-2023-CS-01-02: Privacy-preserving and identity management technologies			
7	scalable PPT	TREE Technology	Santiago Macho González
8	MAP	SESTEK	Tuba ARLAN KIR

Increased Cybersecurity

#	ACRONYM	Organisation	Presenter
CL3-2023-CS-01-03: Security of robust AI systems			
9	robustAI	KEMEA	George Kokkinis
10	Sec-AI	Gradiant	Lilian Adkinson
11	DETECT-AI	TREE Technology	Santiago Macho Gomzáles
12	New-AI	ZEUS consulting	Konstantinos Voukydis
13	Robust-AI	AIT	Markus Wurzenberger
14	SecureAI	DeepKeep	Rony Ohayon
15	AI AutoSec	University of Reading	Atta Badii

CS-01-01

Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

#	Organisation	Presenter
1	gradiant	Lilian Adkinson

ARIES: AI based technologies for the pRotection of IoT EcoSystems

- *Lilian Adkinson*
- *ladkinson@gradiant.org*
- *Gradiant (RTO, Spain)*

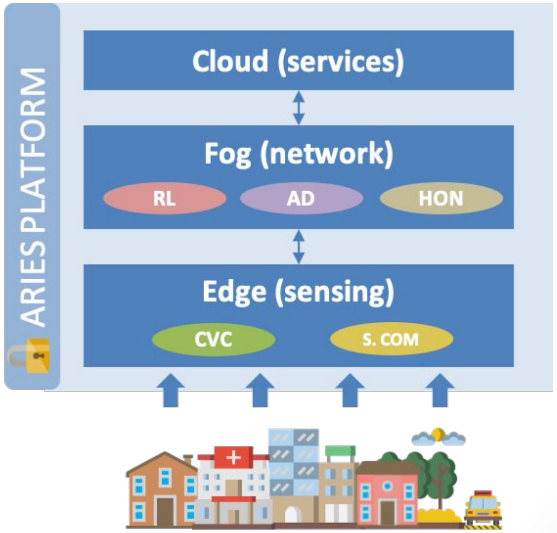
- Role: *WP leader, S/T provider. Potential proposal coordinator*

- Proposal activity: *HORIZON-CL3-2023-CS-01-01 Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)*

gradiant
Connectivity · Intelligence · Security
for your business

Proposal idea/content

- *The focus of ARIES is to secure advanced IoT infrastructures, such as smart cities, covering the communication of the devices, their data collection and processing, and the integration of new untrusted devices in the infrastructure*
- *The platform will include a set of technological modules to enable the automated **detection, analysis, and mitigation of cybersecurity attacks** on the cloud and edge*
- *The proposal will include the following:*
  - ***AI based tools** for cyber threat intelligence, including the use of **anomaly detection** (AD) techniques and the analysis of **honeypots** data*
  - ***Reinforcement Learning** (RL) techniques to improve the resilience of IoT devices against cyber attacks, such as DDoS attacks, jamming or spoofing*
  - ***Confidential and verifiable computing** (CVC) in the edge*
  - *Securizing communications and device identity*



Project participants

- Existing consortium:
  - Proposed coordinator: *TBD*
  - Partners / Other participants:
    - *Gradiant (Spain):*
      - *AI based tools (RL, honeypots analysis, anomaly detection).*
      - *Confidential and verifiable computation in the edge.*
      - *Secure communications and identity device protection.*
- Looking for partners with the following expertise/ technology/ application field:
  - *Software technology providers*
  - *Industry partners*
  - *Use cases*

gradiant
Connectivity · Intelligence · Security
for your business

Lilian Adkinson / ladkinson@gradiant.org

SMI2G
Security Mission Information & Innovation Group

CS-01-01

Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

#	Organisation	Presenter
2	Amadeus	Vincent Rigal

New tools for Cyber threat intelligence

- Vincent Rigal
- vincent.rigal@amadeus.com
- Amadeus
- Role: partner in a consortium under creation

- Proposal activity reference: HORIZON-CL3-2023-CS-01-01

  Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

- Sub-topics:
  - Tools to support cybersecurity resilience, preparedness, awareness, and detection within critical infrastructures and across supply chains
  - AI-based automation tools for cyber threat intelligence

Proposal idea

- Build a project that will gather **several cybersecurity use cases** around the web protection:
  - Advanced **anti-bot detection** and mitigation for e-commerce websites: new methods for scrapers identification behind Residential IP Proxies (RESIP) that use **IoT devices**
  - Automated **cyber threat intelligence** to better protect IT environment
  - **AI attacks** management
- Amadeus will develop above three listed solutions for the travel industry sector
- Other consortium’s partners expertise already identified:
  - Federated machine learning
  - User behaviour data analysis capabilities

Project participants

- Existing consortium:
  - Proposed coordinator: to de defined (potentially Amadeus)
  - Partners / other participants:
    - Amadeus, Global Distribution System and world leader in IT travel industry
    - Two academic partners (PT and UK)
- Looking for:
  - Partners that provide OT (operational technology) systems
  - IoT / OT systems with exposure to Internet, directly or indirectly, or physical security systems also
  - Multi-cloud technology providers

CS-01-01

Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

#	Organisation	Presenter
3	citypassenger	Yohann Cornilliere

CLEARANCE - Communication soLution for a sEcure And inteRoperAble computiNg Continuum Environment

Presenter

- *Yohann CORNILLIERE*
- *ycornilliere@citypassenger.com*
- *Citypassenger*
- Role: *WP leader, S/T provider*

Coordinator

- *Nikos AVGERINOS*
- *navgerinos@diadikasia.gr*
- *Diadikasia Business Consulting*
- Role: *Coordinator*

- Proposal activity: *CL3-2023-CS-01-01*

Proposal idea/content

- ***CLEARANCE** aims to secure the transformation of our digital society from a legacy network of interconnected components to a complex, connection-persistent, massive and highly heterogeneous Computing Continuum ecosystem.*
- *Demonstrate robust and interoperable network implementations for IoT/Edge/Cloud Computing Continuum towards a new paradigm for wider adoption.*
- *Zero-Trust architectures & lifecycle management and obsolescence for IoT to address IoT being the weakest part of the Computing Continuum.*
- *Fine granular management of the different levels of privileges, especially in a mutli-entities context, to guarantee a secure usability of resources augmenting user-centric privacy.*

Project participants

- Existing consortium:
  - Proposed coordinator: DBC
  - Partners: SMEs / IT companies, End Users, privacy & ethics experts from France, Greece, Ireland, Lithuania and Cyprus.

- Looking for partners with the following expertise/ technology/ application field:
  - *Additional End Users to provide use cases for the validation*
  - *IoT environment industrial*
  - *Zero-trust technology provider*
  - *Expert in AI for cyber threat*
  - *Academics labs are welcome*

Yohann CORNILLIERE – ycornilliere@citypassenger.com

SMI2G
Security Mission Information & Innovation Group

CS-01-02

Privacy-preserving and identity management technologies

#	Organisation	Presenter
4	Defence Research Institute	Alessandro Marani

PERSONA

Privacy-prEserving comprEhensive SOlutions for better health aNd reseArch

Alessandro MARANI

(alessandro.marani@defenceresearchinstitute.eu)

DRI
Defence Research Institute

Role: *Proposal Coordinator/Scientific & Technical Coordinator*

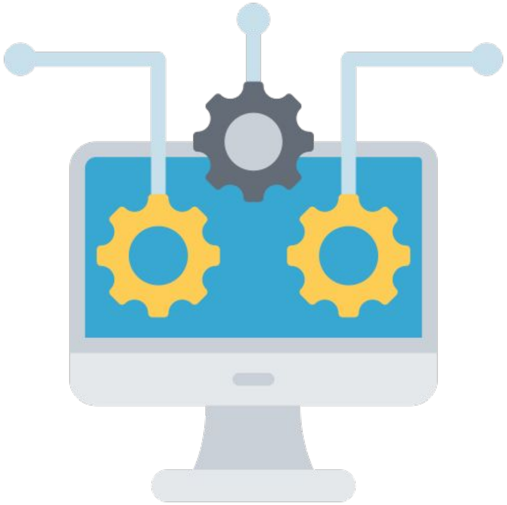
Proposal activity: *HORIZON-CL3-2023-**CS-01-02***

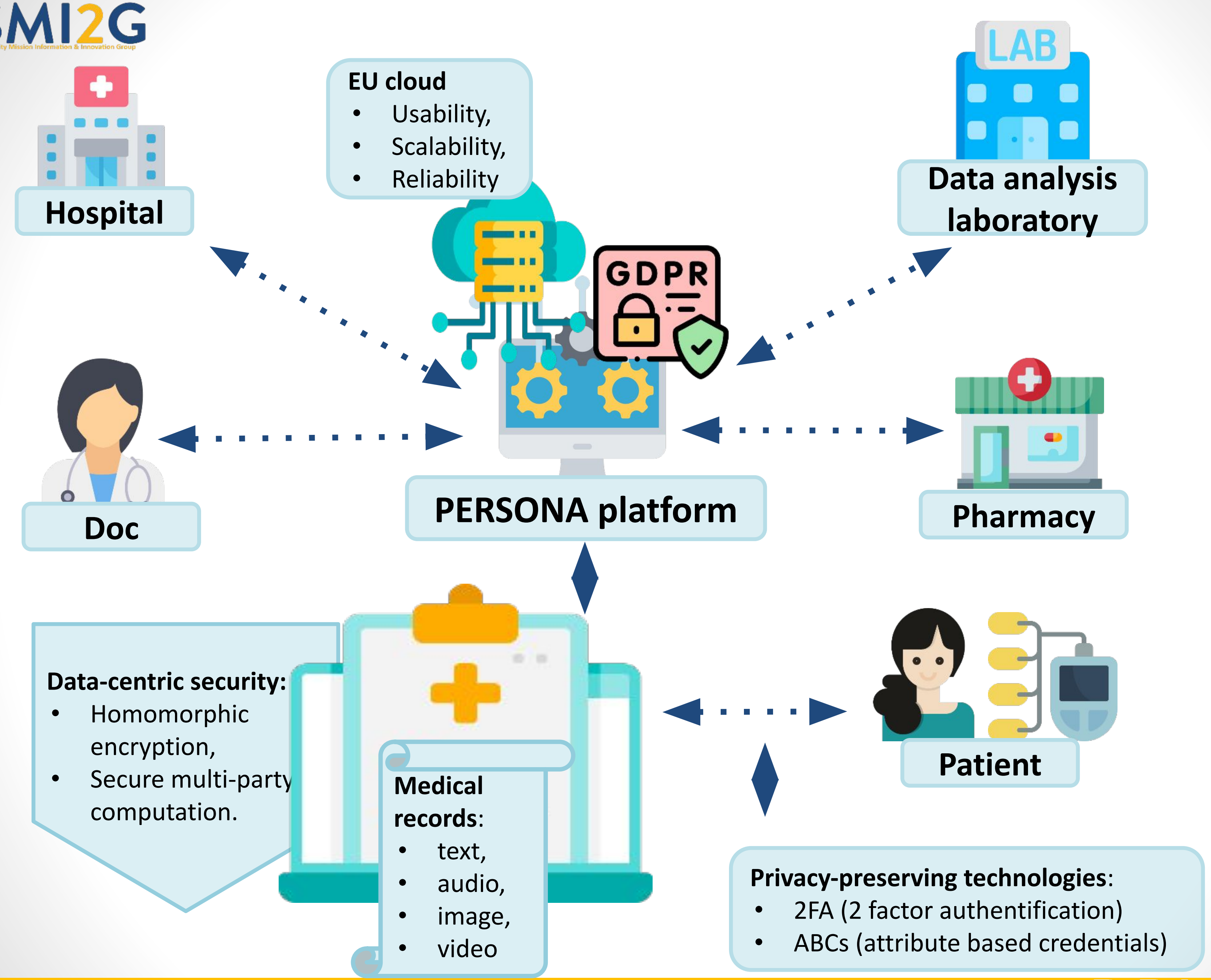
PERSONA idea

- ***OBJECTIVE***: *making the exchange of healthcare information more secure, privacy-oriented for the benefit of users.*

- ***SOLUTION***: *an integrated and interoperable platform for data sharing while fully respecting users' privacy.*

  DRI has already involved ***2 large hospitals*** *in this proposal!*





Hospital

EU cloud
- Usability,
- Scalability,
- Reliability

Data analysis laboratory

Doc

PERSONA platform

Pharmacy

Data-centric security:
- Homomorphic encryption,
- Secure multi-party computation.

Medical records:
- text,
- audio,
- image,
- video

Patient

Privacy-preserving technologies:
- 2FA (2 factor authentification)
- ABCs (attribute based credentials)

Project participants

- **Proposed Coordinator/ Scientific & Technical Coordinator:**
  - *DRI (French SME)*

- **Other consortium members:**
  - *Israelite Hospital (IT)*
  - *Humanitas Research Hospital (IT)*
  - *University of Strasbourg (FR), TBC*

- **DRI is also interested in:**
  - *HORIZON-CL3-2023-**BM-01-01***
  - *HORIZON-CL3-2023-**BM-01-03***
  - *HORIZON-CL3-2023-**INFRA-01-02***
  - *HORIZON-CL3-2023-**CS-01-03***

- **Looking for:**
  - *(Healthcare) system integrators and developers*
  - *IoT experts*
  - *Cyber threats and Cryptography experts*
  - *Experts in digital identity*
  - *Cloud and data-storage providers*
  - *SMEs in the field of healthcare*

CS-01-02

Privacy-preserving and identity management technologies

#	Organisation	Presenter
5	Locknest	Pierre Le Roy

The eID Wallet

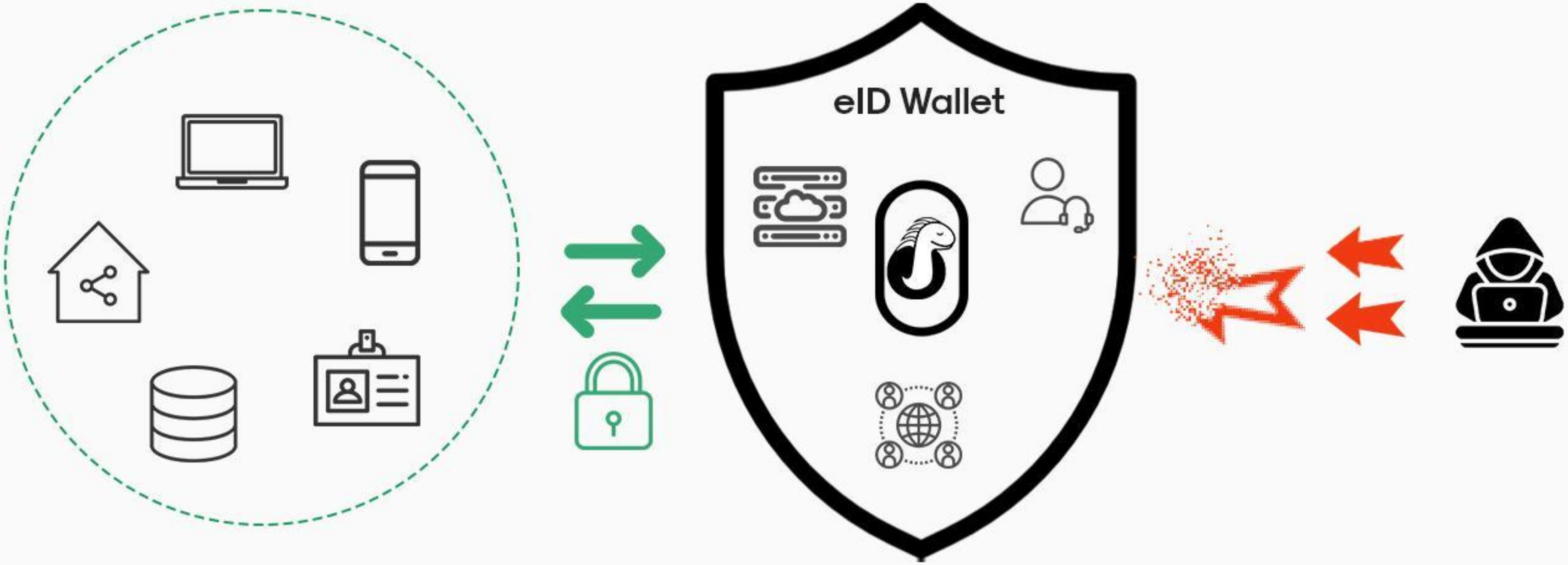
- *LE ROY Pierre*
- *Pierre.LeRoy@locknest.fr*
- *LockNest Group*
- Role: *Proposal coordinator*

- Proposal activity: HORIZON-CL3-2023-CS-01-02 : **Privacy-preserving and identity management technologies**

The eID Wallet: Concept

- *The **eID Wallet** project will design, create and commercialize an ecosystem centered around a **reliable** and **easy** to **use physical device** for **small and medium enterprises.** It will store, protect and distribute the user's **digital identity**.*
- *This project will:*
  - Offer a **physical,** state of the art, secure **digital identity wallet**.
  - **Increase** the **security** by drastically reducing the attack surface.
  - Be compliant with all **existing authentication infrastructures** and operating systems.
  - Provide **privacy by design,** data are only available to the data owners who has a **complete control** over their **personal data**.
  - Be **Open Source** and **Open Hardware**.
  - Be **scalable** by design in a complete ecosystem (Hardware, Cloud, Software solution).
  - Enforce **GDPR.**
  - Use **Self-Sovereign Identity** management technology.

The eID Wallet: Ecosystem



Protected corporate devices and data

European Cloud
SOC/NOC team
Support team

Project participants

- Existing consortium:
  - Proposed coordinator: LockNest Group (France)
  - Infrastructure and antiDDoS provider : antiddos s.r.o. (Czechia)
  - Technical Partner : Citypassenger (France)

- Looking for partners with the following expertise, technology, application field:
  - Design and production of enclosure.
  - Hardware and software pentesting.
  - Legal expertise on GDPR and data privacy issues.
  - SaaS/Cloud infrastructure partner.

CS-01-02

Privacy-preserving and identity management technologies

#	Organisation	Presenter
6	gradiant	Lilian Adkinson

Enhanced cyber threat intelligence on a privacy preserving and federated computation

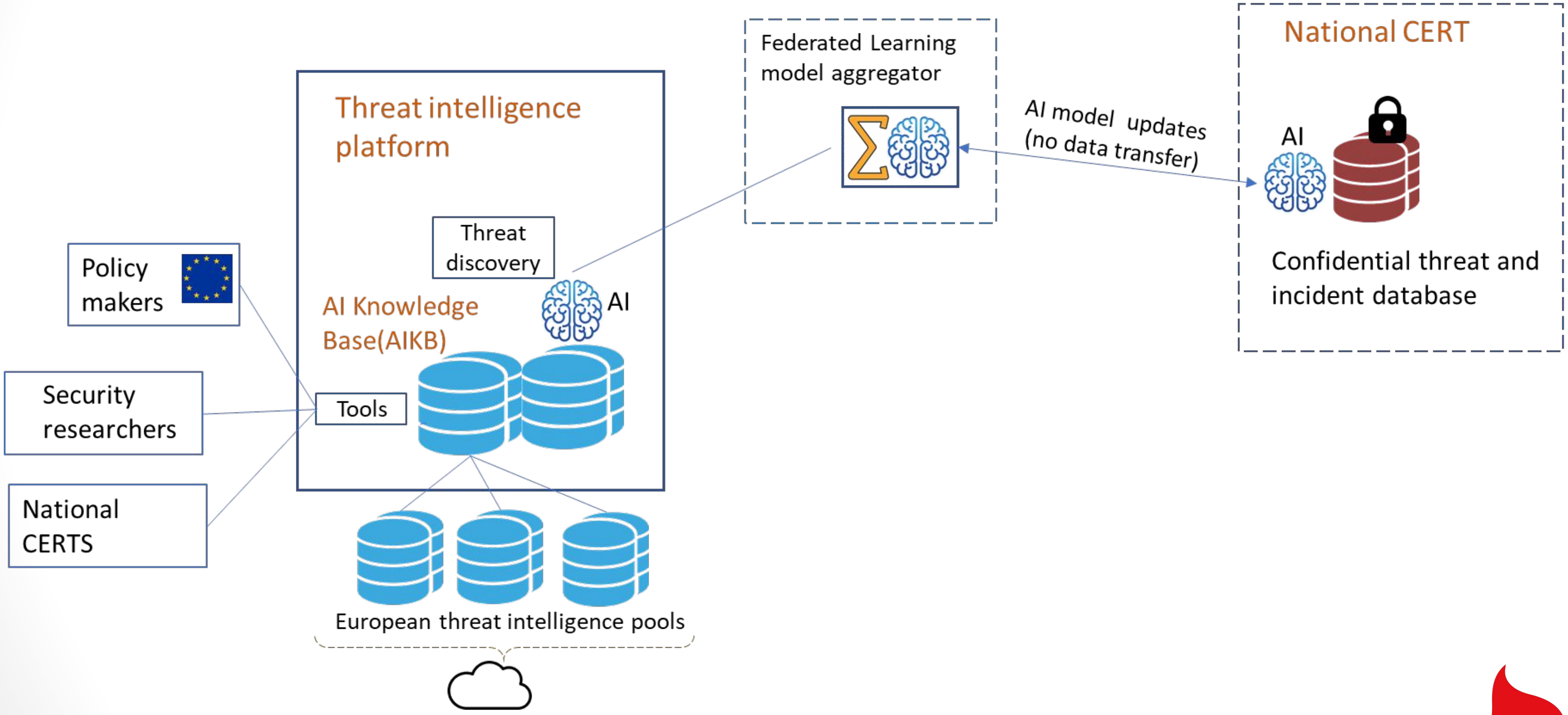
- *Lilian Adkinson*
- *ladkinson@gradiant.org*
- *Gradiant (RTO, Spain)*

- Role: *WP leader, S/T provider. Potential proposal coordinator*

- Proposal activity: *HORIZON-CL3-2023-CS-01-02 Privacy-preserving and identity technologies*

gradiant
Connectivity · Intelligence · Security
for your business

Proposal idea/content


Federated Learning model aggregator
National CERT
AI model updates (no data transfer)
Threat intelligence platform
AI
Confidential threat and incident database
Threat discovery
Policy makers
AI Knowledge Base(AIKB)
AI
Security researchers
Tools
National CERTS
European threat intelligence pools

Proposal idea/content

- The aim of the proposal is to create a reliable privacy preserving federated platform for sharing and improving cyber threat intelligence
- Platform for predicting zero day attacks based on AI analysis of pooled national threat and incident data
- Privacy of data contributors (attack victims) and CERTs is 100% preserved
- Validation or piloting of privacy-preserving computation in realistic federated data infrastructures
- *The platform will include the use of:*
  - *Improved scalable and reliable privacy-preserving technologies for federated processing of cyber threat intelligence and their integration in real-world systems: Differential Privacy, Secure Multi-Party Computation, Multi Key homomorphic encryption and trusted Execution Environments*
  - *Privacy by design and privacy metrics*
  - *Effective FL algorithms and aggregator methods*

gradiant
Connectivity · Intelligence · Security
for your business

Project participants

- Existing consortium:
  - Proposed coordinator: *TBD*
  - Partners / Other participants:
    - *Gradiant (Spain): PETs (DP and MKHE), privacy attacks, privacy metric*
- Looking for partners with the following expertise/ technology/ application field:
  - *Federated learning algorithms experts*
  - *Cyber Threat Intelligence experts*
  - *Policy makers and GDPR experts*
  - *CERTs*

gradiant
Connectivity · Intelligence · Security
for your business

SMI2G
Security Mission Information & Innovation Group

CS-01-02

Privacy-preserving and identity management technologies

#	Organisation	Presenter
7	TREE Technology	Santiago Macho González

SMI2G
Security Mission Information & Innovation Group

Scalable and reliable privacy-preserving technologies for self-sovereign identity solutions

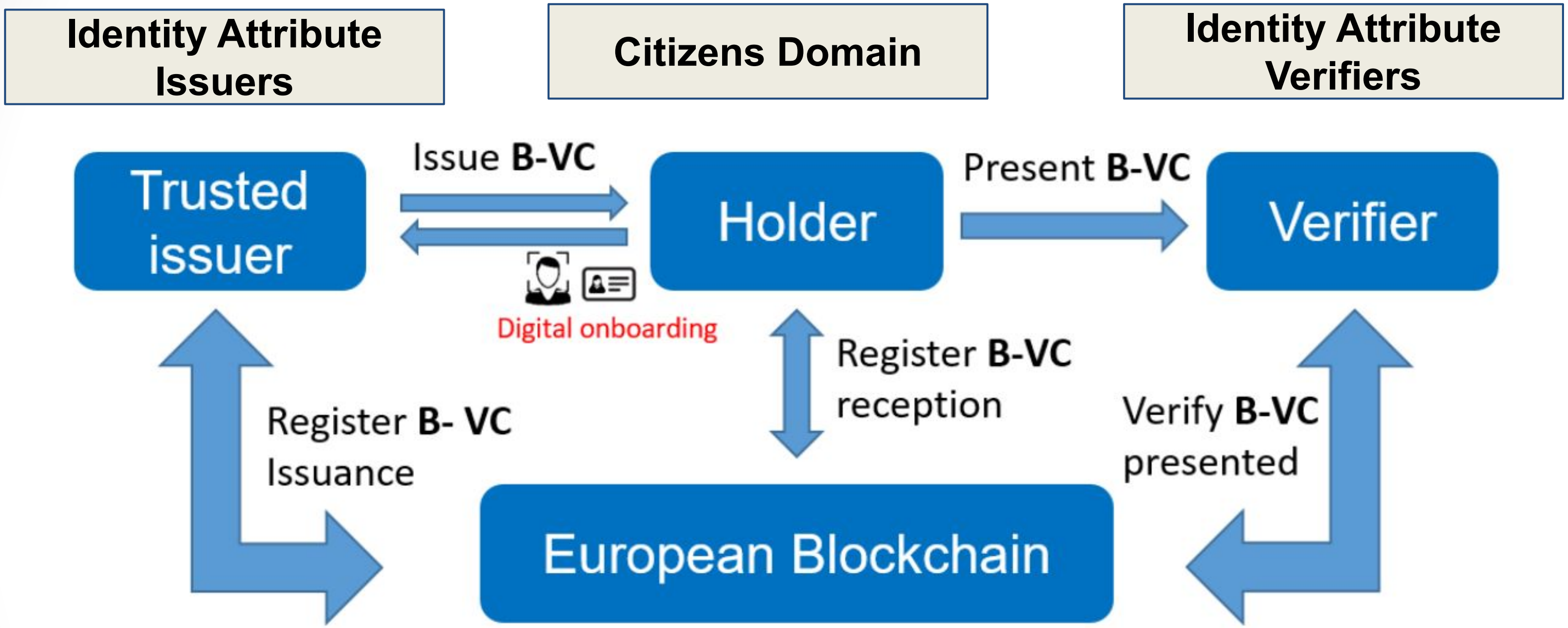
- *Dr. Santiago Macho González*
- *Santiago.macho@treetk.com*
- *TREE TECHNOLOGY (Spanish SME)*

    - *Participation in > 30 EU projects*
    - *12 on-going H2020/HEUR projects (+2 to start soon)*
        - *4 in SECURITY cluster*
    - *Expertise in Big Data, AI and cybersecurity*

- Role: *WP leader, S/T provider.*

- Proposal activity: *HORIZON-CL3-2023-CS-01-02 Privacy-preserving and identity technologies*

Proposal idea/content



Identity Attribute Issuers

Citizens Domain

Identity Attribute Verifiers

Trusted issuer

Issue **B-VC**

Digital onboarding

Holder

Present **B-VC**

Verifier

Register **B- VC** Issuance

Register **B-VC** reception

Verify **B-VC** presented

European Blockchain

Figure 1: Entities or organizations involved in the SSI scheme

B-VC : Blind verifiable credential

Proposal idea/content

- *The aim of the proposal is to create a novel platform to generate, validate and custodian the citizens' digital identity in an agile, secure and privacy preserving way. This proposal will be based on IMPULSE, an ongoing H2020 project which consists of a novel eID management system that can be integrated as a new option into online public services.*
- *The platform will include the use of:*
  - *The European self sovereign identity framework on top of European Blockchain service Infrastructure (issuer, verifier and holder)*
  - *Support for new selective disclose verifiable credentials in order to attest specific user's identity attributes in a privacy-preserving way*
  - *Zero knowledge proofs for blind users' identity attribute checking*
  - *AI-based algorithms for document verification and fraud detection, including Manipulation Attack Detection (MAD) and Presentation Attack Detection (PAD)*

Project participants

- Existing consortium:
  - Proposed coordinator: *GRADIANT*
  - Partners / Other participants:
    - *Gradiant (Spain): Distributed Identity models, Zero Knowledge proofs, privacy preserving and secure digital wallets, IA-based document validations*
    - *TREE Technology – document verification*
    - *Large company – TSP*
    - *2 possible LEAs*
- Looking for partners with the following expertise/ technology/ application field:
  - *Trust Service Providers*
  - *Multi-Biometric techs experts*
  - *Policy makers: GDPR and eIDAS experts*
  - *Use cases (verifiers and issuers)*

CS-01-02

Privacy-preserving and identity management technologies

#	Organisation	Presenter
8	SESTEK	Tuba ARLAN KIR

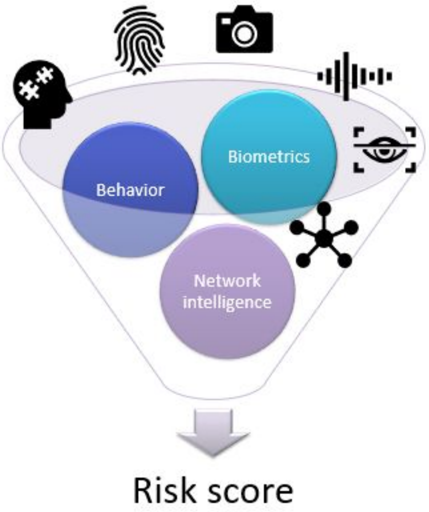
MAP:Multimodal Authentication Platform

- *Tuba ARLAN KIR, R&D&I Manager*
- *tuba.arslan@sestek.com*
- *SESTEK*
- Role: *WP leader, S/T provider*

- Proposal activity: *HORIZON-CL3-2023-CS-01-02: Privacy-preserving and identity management technologies*

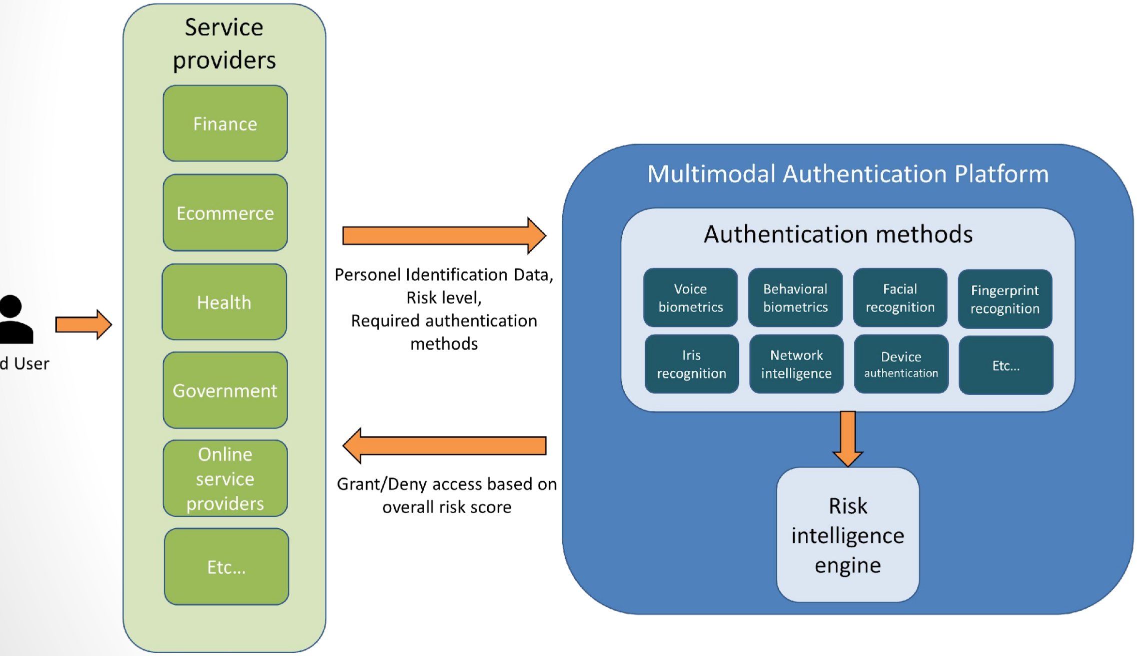
Proposal idea/content

- **deliver an intelligent & modular multimodal authentication platform**
- **expand** intelligent authentication concept **beyond authentication of a single modal**
- support real-time (often passive) use of **multiple biometric factors,** informed **by other modalities**
- orchestrate with **AI-infused decision engines**
- secure and reliable **identity management** and **privacy protection**, enabling **federated sharing** and processing of both personal and industrial data
- enhancing security-sustaining tools for **cyber threats**



Proposal idea/content

MAP Project aims to deliver an intelligent authentication platform & 3rd party services in line with the Commission's "European Digital Identity Architecture and Reference Framework" concept to be enabled by;



- Authentication of different modalities
- **Modular structure**
- Serve different verticals
- Diverse of authentication methods
- AI-infused risk intelligence engine
- End-to-end value chain
- Contribution to promotion of **GDPR compliant** European data spaces
- **Self-sovereign** identity management technologies and solutions

Project participants

- Existing consortium:
  - *Partners / Other participants: Turkey, Portugal, Finland consortiums for behavioural biometrics & authentication, facial recognition, voice biometrics, platform development, design & development of the risk scoring engine, IdM/IAM*
- Looking for partners with the following expertise/ technology/ application field:
  - *Coordinator*
  - *Technology providers: authentication of different modalities, federated learning, identity protection*
  - *Standardization*
  - *Use case providers willing to test and use final platform*

CS-01-03

Security of robust AI systems

#	Organisation	Presenter
9	KEMEA	George Kokkinis

HORIZON-CL3-2023-CS-01-03: Security of robust AI systems

(no title available yet)

- *George Kokkinis*
- *g.kokkinis@kemea-research.gr*
- Center for Security Studies (KEMEA),

  Hellenic Ministry of Citizen Protection
- *Proposal coordinator and/or WP leader*
- Proposal activity: HORIZON-CL3-2023-CS-01-03: Security of robust AI systems

George Kokkinis,
Head of Cybersecurity Sector
Center for Security Studies (KEMEA)
Hellenic Ministry of Citizen Protection

P. Kanellopoulou 4, 101 77, Athens, Greece
Tel:+302107710805
Email: g.kokkinis@kemea-research.gr
Website: www.kemea.gr/en

Proposal idea/content

1. Design and develop a Security-by-Design AI framework
2. Include SOTA context awareness in ML in this framework
3. Pilot this framework against selected areas of adversarial attacks
4. Benchmark resiliency of the developed FW against existing solutions

- Consider proposed Artificial Intelligence Act and
  - submit policy recommendations
  - Produce best practices for implementation
  - Context awareness
  - Resilience
  - Robustness

Project participants

- *KE.ME.A*
- *Hellenic Police*
- *Hellenic Ministry of Justice (contacted)*
- *Hellenic CSIRT*
- *Partners from existing CS projects will be contacted*

KE.ME.A expertise – Value added in the proposal

- *End user needs*
- *Pilot design and evaluation*
- *Dissemination, Communication, outreaching (Lead / Support)*
- *Ethical and Legal (Lead Support)*
- *Policy recommendations*

CS-01-03

Security of robust AI systems

#	Organisation	Presenter
10	Gradiant	Lilian Adkinson

Sec-AI: Security technologies for a verifiable and resilient AI

- *Lilian Adkinson*
- *ladkinson@gradiant.org*
- *Gradiant (RTO, Spain)*
- *Role: WP leader, S/T provider. Potential proposal coordinator*

- Proposal activity: *HORIZON-CL3-2023-CS-01-03 Security of robust AI systems*

gradiant
Connectivity · Intelligence · Security
for your business

Proposal idea/content

- *The aim of Sec-AI is to create a reliable platform involving a set of coordinated security technologies to build reliable, verifiable and resilient AI models*
- *The project will research the state-of-the art of novel attacks against AI models and data*
- *Sec-AI will explore the **impact of an attack on different types of AI models**, such as Federated Learning (e.g., assuming a malicious participant on the network, poisoning the exchanged parameters during the training process) or Deep Learning (e.g., reducing the accuracy of a class, weight poisoning), among others.*
- *The project will explore **possible defenses**, such as the use of:*
  - *Interpretable Machine Learning (IML) techniques for **increasing robustness** and tackling **adversarial attacks** against central and federated learning models.*
  - *Verifiable and confidential technologies for **computing AI on the edge** (Trusted Execution Environments and Zero Knowledge proofs)*
- *Sec-AI will include the validation of the developed mechanisms and the definition of metrics to assess the impact of the attacks*

gradiant
Connectivity · Intelligence · Security
for your business

Project participants

- Existing consortium:
  - Proposed coordinator: *TBD*
  - Partners / Other participants:
    - *Gradiant (Spain): IML, TEE-based verifiable computing, Zero Knowledge proofs-based techniques*
- Looking for partners with the following expertise/ technology/ application field:
  - *Machine and Deep learning experts*
  - *Security by design experts*
  - *AI regulatory and certification schemes experts*
  - *Use cases*

gradiant
Connectivity · Intelligence · Security
for your business

CS-01-03

Security of robust AI systems

#	Organisation	Presenter
11	TREE Technology	Santiago Macho Gomzáles

DETECT-AI

DEvelopment of a new tool for detTECTion of biased, erroneous or fraudulent data through AI.

- *Dr. Santiago Macho González*
- *Santiago.macho@treetk.com*
- *TREE TECHNOLOGY (Spanish SME)*
  - *Participation in > 30 EU projects*
  - *12 on-going H2020/HEUR projects (+2 to start soon)*
    - *4 in SECURITY cluster*
  - *Expertise in Big Data, AI and cybersecurity*

- Role: *Coordinator (Open)*
  - *Platform developer.*
  - *WP leader*
  - *Cybersecurity expert.*
  - *S/T provider*

- Proposal activity: HORIZON-CL3-2023-CS-01-03: SECURITY OF ROBUST AI SYSTEMS

Proposal idea/content

- **Motivation:**
  - The collection of data from different sources is becoming increasingly (health, industry and computer security).
  - This poses several challenges: biased, erroneous or event fraudulent/poisoned data.

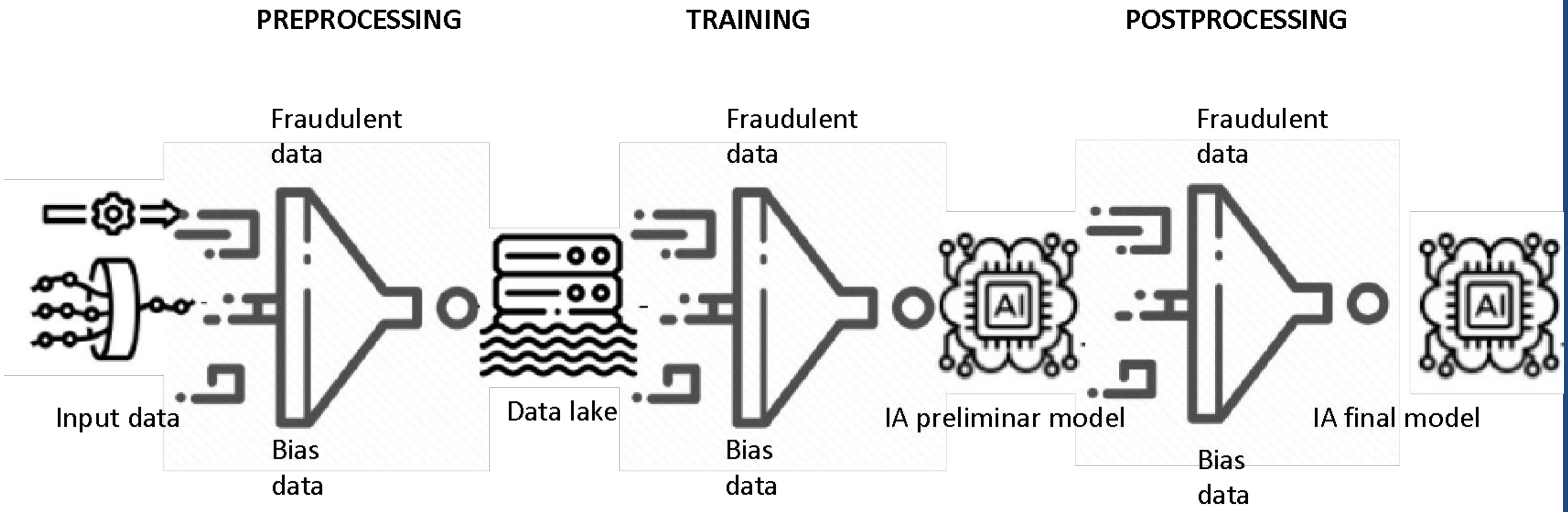
- **Consequence:**
  - Negative impact on the quality of the extract information

↓

non accurate decision-making

Proposal idea/content

- We propose the development of a new platform that enable users to automatically detect and correct attacks targeting ML models, biased, erroneous or fraudulent/poisoned data.



- This platform will be based on Machine Learning and data analytics techniques to identify anomalous patterns in the data and flag them for further review and correction and/or discard them.

Project participants

- Existing consortium:
  - Proposed coordinator: *TREE*
  - Partners / Other participants:
    - Data harmonization
    - Experts in cybersecurity for medical devices
- Looking for partners with the following expertise/ technology/ application field:
  - *Cybersecurity*
  - *Machine Learning*
  - *Platform developer*
  - *Data providers (health, industry, computer security, ….)*

CS-01-03

Security of robust AI systems

#	Organisation	Presenter
12	ZEUS consulting	Konstantinos Voukydis

New Generation AI Systems for Security

- *Konstantinos Voukydis (Researcher)*
- *info@zeusconsulting.com*
- *Zeus Consulting*
- *Proposal Coordinator*

- *Security of robust AI systems*
- *HORIZON-CL3-2023-CS-01-03*

ZEUS CONSULTING

Aratos
Group

New Generation AI Systems for Security

- Digital AI-Infrastructure for cyber-attack and hybrid-threat preventions
- Increased software, hardware and supply chain mitigation measures against cyberattacks in AI Systems
- Security of cross-border knowledge and data sharing
- Establishing a reinforcement of awareness and a common cybersecurity management and culture

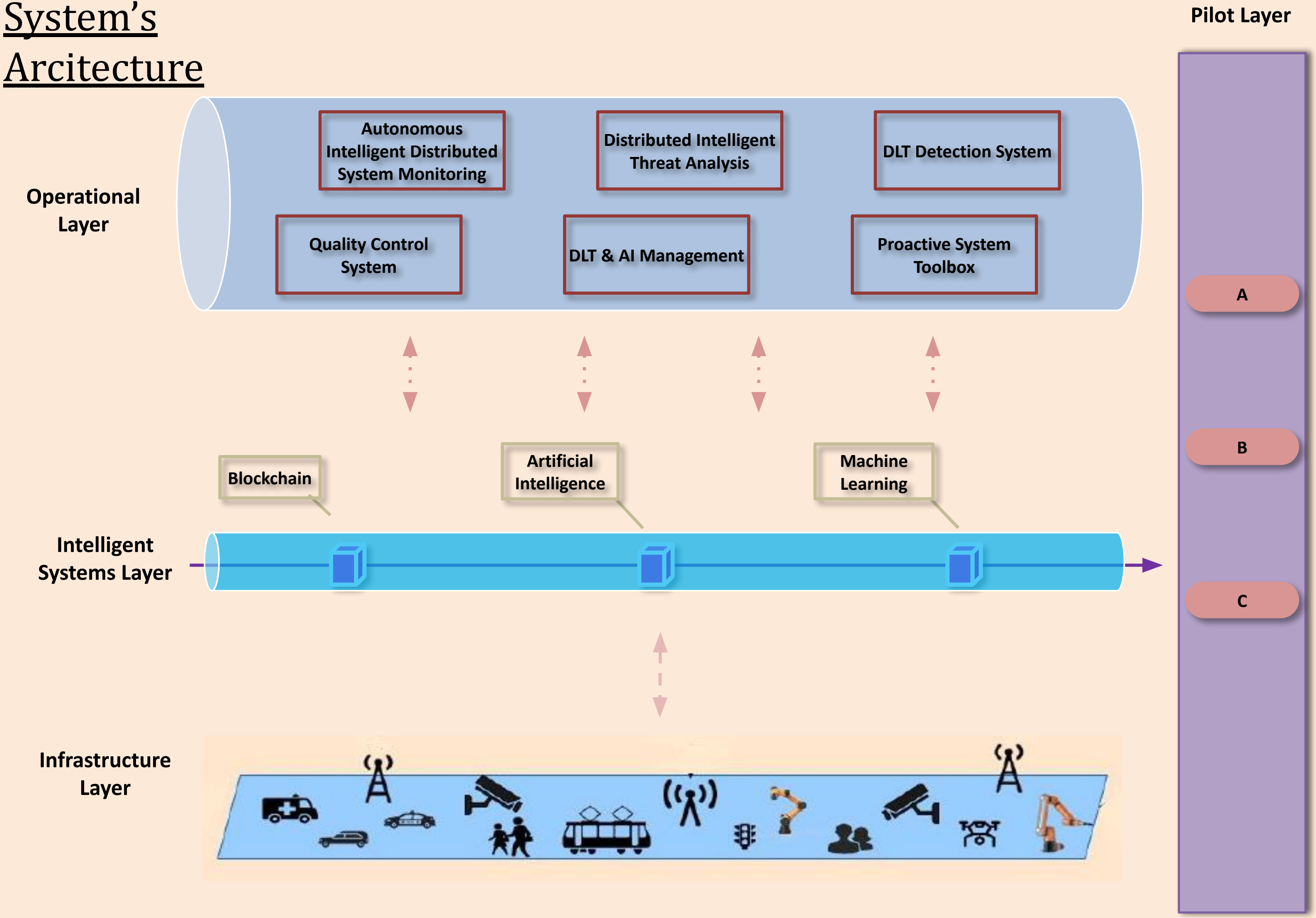
ZEUS CONSULTING

Aratos Group

Konstantinos Voukydis (voukidis@zeusconsulting.com)

New Generation AI Systems for Security

System’s Arcitecture



Pilot Layer

Operational Layer

Autonomous Intelligent Distributed System Monitoring

Distributed Intelligent Threat Analysis

DLT Detection System

Quality Control System

DLT & AI Management

Proactive System Toolbox

A

B

C

Blockchain

Artificial Intelligence

Machine Learning

Intelligent Systems Layer

Infrastructure Layer

Project participants

- Existing consortium:
  - Proposed coordinator: ***ZEUS Consulting***
  - Partners / Other participants: **CUT, University of Peloponnese, BC2050**

- Looking for partners with the following expertise/ technology/ application field:
  - ***Technical AI/ML Expert***
  - ***Big Data Analytics***
  - ***System Integrator***
  - ***Pilot Cases***

Konstantinos Voukydis (voukidis@zeusconsulting.com)

CS-01-03

Security of robust AI systems

#	Organisation	Presenter
13	AIT	Markus Wurzenberger

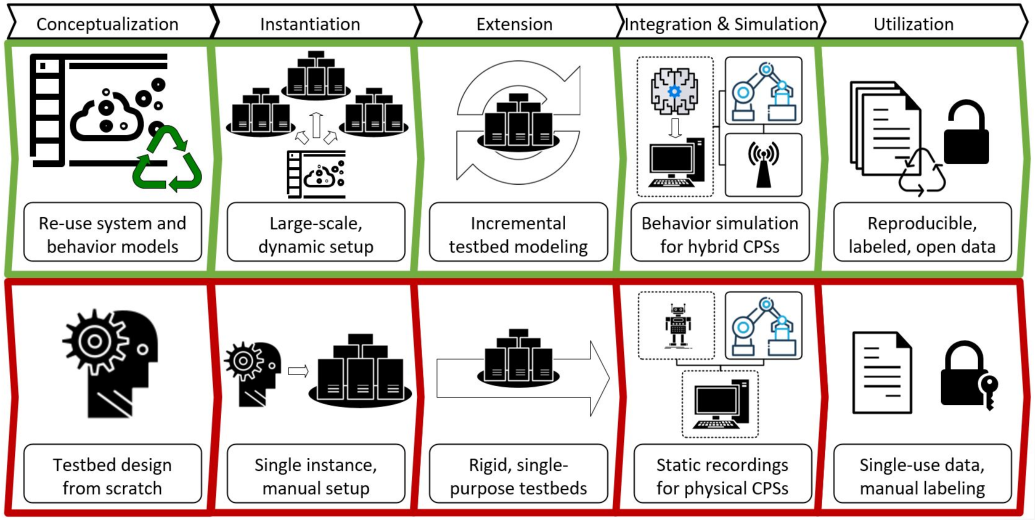
HORIZON-CL3-2023-CS-01-03

- *Markus Wurzenberger*
- *markus.wurzenberger@ait.ac.at*
- *AIT Austrian Institute of Technology GmbH*
- Role: *WP leader, S/T provider*

- Proposal activity: *HORIZON-CL3-2023-CS-01-03: Security of robust AI systems*

Proposal idea/content

- *Development of AI algorithms for intrusion and attack detection in system logs (e.g., syslog, syscalls/audit logs, application logs, web logs) and network traffic*
- *Model-driven testbed approach to generate large and realistic labelled log data sets to evaluate and test AI algorithms*
- *Study and enable certification of AI algorithms within AIT's testbed*
- *Apply the concept of digital twins to simulate attacks against CPS and OT to improve AI algorithms*
- *Detect and mitigate effects of adversarial ML*
- *Application of re-inforcement learning to improve robustness and resilience of AI intrusion detection algorithms*



Conceptualization | Instantiation | Extension | Integration & Simulation | Utilization

Re-use system and behavior models | Large-scale, dynamic setup | Incremental testbed modeling | Behavior simulation for hybrid CPSs | Reproducible, labeled, open data

Testbed design from scratch | Single instance, manual setup | Rigid, single-purpose testbeds | Static recordings for physical CPSs | Single-use data, manual labeling

Project participants

- Existing consortium:
  - None
- Looking for partners with the following expertise/ technology/ application field:
  - Looking for an appropriate consortium
- References:

Publications: https://aecid.ait.ac.at/further-information/
AECID/AMiner: https://github.com/ait-aecid
Projects:

SOCCRATES
https://www.soccrates.eu/

GUARD
https://guard-project.eu/

PANDORA
https://pandora-edidp.eu

AInception
AI FRAMEWORK FOR IMPROVING CYBER DEFENCE OPERATIONS
https://shorturl.at/eqA58

RESili8
https://resili8-project.eu/

SMI2G
Security Mission Information & Innovation Group

CS-01-03

Security of robust AI systems

#	Organisation	Presenter
14	DeepKeep	Rony Ohayon

SMI2G 2023, 10-11 May 2023, Paris

Security of robust AI systems

- *Name : Rony Ohayon, PhD*
- *Email: rony@deepkeep.ai*
- *Company: DeepKeep*
- Role: *coordinator or WP Leader*

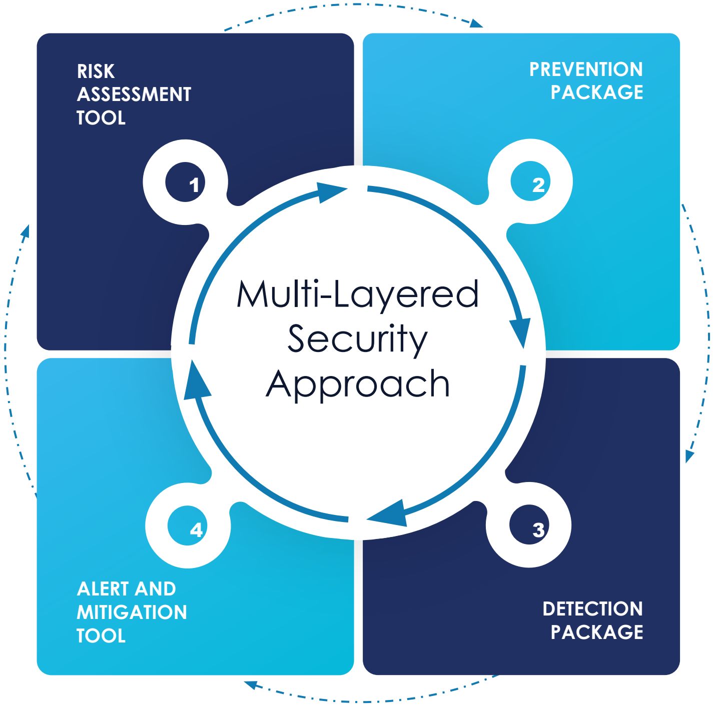
- Proposal activity: **HORIZON-CL3-2023-CS-01-03**

Proposal content

- *Create an automated software platform that will provide the following layers of AI security:*
    - *Risk analysis: run multiple tests and attacks on AI models & datasets and uncover risks and vulnerabilities. The tool will also generate a risk assessment report.*
    - *Prevention layer: fortification and prevention functions against adversarial attacks*
    - *Real-Time attacks detection & mitigation:*
        - *Detection layer: deploy a variety of detectors on AI models to detect adversarial attacks in real-time*
        - *Mitigation tool: concrete tools for tracking and mitigating attacks in real time*

Security by design approach

- Penetration testing
- Vulnerability assessment
- Protection recommendation



- Pre & post-processing
- Robust component injection
- Model reparation

- Real-time alert triggering
- Dynamic protection
- Operation center and response

- Stateful/Stateless detection
- Anomaly detection
- Explainability-based detectors`

Rony Ohayon | rony@deepkeep.ai

Project participants

- Existing consortium:
  - *2 SMEs*
  - *2 Universities*
- Looking for a WP leader or Coordinator
- Looking for the following partners:
  - ***Use cases**: Large Enterprises from the BFSI/Automotive/ Government sectors*
  - ***R&D**: Enterprises and Academic institutions with expertise in:*
    - *Adversarial AI (Evasion, Stealing, poisoning, etc.)*
    - *Trustworthy AI (weak spots, OOD, XAI, confidence, etc.)*
    - *AI ethics and regulation (AI ACT)*
    - *ML* context awareness