
# Building Trust in AI: Highlights from the European AI & Cybersecurity CrossTalk Event

**The European AI Cybersecurity Network (EASINET) CrossTalk** event brought together leading European projects, policymakers, and industry representatives to explore advancements and challenges in AI and cybersecurity. HARPOCRATES participated as one of several projects contributing to discussions on secure and trustworthy AI systems, particularly in healthcare.
Representing HARPOCRATES, **Antonis Michalas from Tampere University (TUNI)** shared insights on the project's progress and its approach to building privacy-preserving AI frameworks.
The event featured projects such as **FLUTE, ENCRYPT, HARPOCRATES, ONCOVALUE, TRUMPET, EOSC TITAN, EOSC SIESTA, AI4EOSC, PAROMA-MED, and KATY**, alongside contributions from **ENISA and the European Commission.**

## EUROPEAN PROJECTS AT THE CROSSTALK

AI4 EOSC | encrypt | EOSC TITAN | EOSC SIESTA | flute | HARPOCRATES | KATY | oncovalue | PAROMA-MED | TRUMPET

## Event Highlights

**Antonis Michalas Represents HARPOCRATES**
Antonis Michalas provided an overview of HARPOCRATES' efforts in developing secure and transparent AI solutions. His presentation focused on:

- **Functional and Hybrid Homomorphic Encryption:** Tools to securely process sensitive data while maintaining privacy, with relevance to healthcare applications.
- **Privacy-Preserving Machine Learning:** Ensuring confidentiality in AI model training and usage.
- **Building Trust in AI Systems:** Developing methodologies that align with European data protection and cybersecurity standards.

Antonis highlighted **HARPOCRATES' collaborative approach, emphasizing the importance of working alongside other projects to address shared challenges.**

## SOLUTIONS PRESENTED

### Privacy Enhancement Technologies

Many projects focus on developing privacy-preserving data processing technologies, such as encryption, data watermarking, and secure, privacy-preserving frameworks

## Contributions from European Projects

The event highlighted the diverse efforts of participating in projects, each addressing different aspects of AI and cybersecurity:

- **FLUTE:** Addressing secure processing for large-scale data streams.
- **ENCRYPT:** Developing privacy-first AI workflows with advanced encryption.
- **ONCOVALUE:** AI-driven oncology innovations with a focus on transparency and secure data handling.
- **TRUMPET:** Advancing data-centric AI applications in industrial and scientific contexts.
- **EOSC TITAN and EOSC SIESTA:** Enhancing secure data sharing and interoperability in scientific research.
- **AI4EOSC:** Focusing on scalable and secure AI solutions for research ecosystems.
- **PAROMA-MED:** Supporting personalized medicine with ethical and secure AI frameworks.
- **KATY:** Predictive analytics and decision-making tools in healthcare applications.

Each project offered unique insights into advancing AI technologies while ensuring security and privacy.


## Key Themes

**HARPOCRATES and Secure AI**
Antonis Michalas' presentation aligned with broader event themes, highlighting HARPOCRATES' contributions to:

- Developing AI models that prioritize transparency and explainability.
- Using advanced encryption techniques to ensure data security.
- Collaborating with other projects to address interoperability and standardization challenges.

**The Role of Collaboration**
The event emphasized the importance of collaboration among European projects, industry, and policymakers. HARPOCRATES contributed to discussions on how shared knowledge can:

- Drive innovation in secure AI technologies.
- Establish common cybersecurity standards.
- Balance regulatory compliance with the need for flexibility in AI development.

**Policy and Industry Perspectives**
Representatives from ENISA and the European Commission stressed the importance of unified cybersecurity frameworks and the role of public-private partnerships in advancing AI technologies. HARPOCRATES' methodologies reflect these priorities, particularly in sensitive sectors like healthcare.

## HARPOCRATES in Healthcare

HARPOCRATES highlighted its work on secure AI for healthcare, focusing on:

- **Protecting Patient Data:** Leveraging encryption methods to safeguard sensitive information.
- **Reliable AI Models:** Ensuring AI systems are accurate and explainable to users.
- **Compliance with Regulations:** Aligning AI development with European data protection and cybersecurity standards.

These efforts support the growing need for secure AI systems in healthcare, where trust and data protection are crucial.

## Key Takeaways

HARPOCRATES contributed to meaningful discussions on AI and cybersecurity at the EASINET CrossTalk event. Key outcomes include:

1. **The Importance of Trust:** Secure, transparent AI systems are essential for adoption, particularly in healthcare.
2. **Collaboration is Key:** Working with other projects and stakeholders enhances the scope and impact of secure AI solutions.
3. **AI for Healthcare Requires Focus:** Tailored approaches are necessary to meet the specific demands of the healthcare sector.

## Closing Remarks

The EASINET CrossTalk event highlighted the collective efforts of European projects to address the challenges of secure AI development. **HARPOCRATES' contributions, particularly in the healthcare domain, reflect their commitment to advancing privacy-preserving and trustworthy AI systems.**
Through collaboration with other projects and stakeholders, HARPOCRATES continues to play an important role in shaping the future of secure AI. For updates and more information, visit our website or contact us directly.

STAY TUNED!
Stay updated on all our latest news, developments, research and general information regarding the HARPOCRATES project.

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101069535.

UK participant in Horizon Europe Project HARPOCRATES is supported by UKRI grant number 10048312