Approaches and tools for security in software and hardware development and assessment

HORIZON-CL3-2026-02-CS-ECCC-01

Program:	Horizon Europe Cluster 3
Típus:	Research & Innovation Action
TRL szint:	-
Támogatás projektenként:	3-5 M EUR
Támogatott projektek száma:	4-5
Pályázati felület megnyílik:	2026 március 3
Beadási határidő:	2026 szeptember 15
Felhívás linkje:	LINK

This topic aims to develop innovative tools, methods, and processes to secure the entire ecosystem of software and hardware development.

Proposals should address at least one of the following:

A. Secured hardware systems over trusted Chips

This subtopic aims to develop robust security solutions for trusted hardware platforms, focusing on secured microprocessors, secure boot mechanisms, and cryptographic acceleration. Proposals are expected to address the risks of hardware-based vulnerabilities and backdoors, taking into account emerging threats..

B. Software Supply Chain security

This subtopic focuses on mitigating security risks in software supply chains, including secure code provenance, automated vulnerability detection, and secure software development lifecycle methodologies.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu

Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI)

HORIZON-CL3-2026-02-CS-ECCC-02

Program:	**Horizon Europe Cluster 3**
Típus:	**Innovation Action**
TRL szint:	**-**
Támogatás projektenként:	**3-5 M EUR**
Támogatott projektek száma:	**4-5**
Pályázati felület megnyílik:	**2026 március 3**
Beadási határidő:	**2026 szeptember 15**
Felhívás linkje:	LINK

This topic aims to strengthen the resilience of AI systems and algorithms against various threats and attacks, such as enhancing their resilience against adversarial attacks, backdoor injections, and data poisoning. Proposals should develop real-time anomaly detection, mitigation techniques to defend against adversarial attacks and robust federated learning techniques, in synergies with leading efforts on AI transparency, and in compliance with the AI Act.

The topic is expected to:

- Develop robust AI models resistant to adversarial attacks.
- Advance methodologies to identify and mitigate compromised datasets.
- Develope mechanisms that enable AI models to be trained, deployed and operated in privacy-preserving environments.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu

Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations

HORIZON-CL3-2026-02-CS-ECCC-03

Program:	**Horizon Europe Cluster 3**
Típus:	**Research & Innovation Action**
TRL szint:	**-**
Támogatás projektenként:	**3-5 M EUR**
Támogatott projektek száma:	**2-3**
Pályázati felület megnyílik:	**2026 március 3**
Beadási határidő:	**2026 szeptember 15**
Felhívás linkje:	LINK

Proposals should address one of the following technology areas:

A. **Design and implementation of PQC advanced primitives for enhanced security and privacy**, also including schemes beyond lattice-based approaches. Proposals should also include recommendations that balance security, performance, and usability in practical applications and be based on open-source reusable software libraries, which can be formally verified.

B. **Development of a unified specification language to formalise and document conditions on safety and security in software implementations;** development and improvement of tools and methodologies that can be used to evaluate both the implementation and the usage of cryptography in software applications and provide formal machine-checked guarantees of correctness and security. Proposals should also consider improving existing HACS tools and their integration in such software implementations.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu

Artificial Intelligence for Cybersecurity applications

HORIZON-CL3-2027-02-CS-ECCC-01

Program:	**Horizon Europe Cluster 3**
Típus:	**Research & Innovation Action**
TRL szint:	**-**
Támogatás projektenként:	**3-5 M EUR**
Támogatott projektek száma:	**4-5**
Pályázati felület megnyílik:	**2027 március 2**
Beadási határidő:	**2027 szeptember 15**
Felhívás linkje:	LINK

This topic aims to advance AI-based cybersecurity applications while ensuring that AI-driven solutions remain resilient, transparent, and compliant with regulatory frameworks such as the AI Act. In this context, the topic explores the role of all types of AI, including generative AI, in cybersecurity applications, including automated threat detection, adaptive cyber defence, and AI-driven cyber threat intelligence. Proposals should develop solutions for trustworthy AI in cybersecurity contexts including addressing adversarial AI risks, in compliance with the provisions of the AI Act.

The topic is expected to:

- Develop AI-driven solutions and tools for real-time cyber threat detection.
- Develop adaptive AI systems capable of evolving with dynamic cybersecurity challenges.
- Developing AI-enhanced frameworks that integrate predictive analytics, automation, and threat intelligence to strengthen proactive defence measures.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu

Secure Computing Continuum (IoT, Edge, Cloud, Data spaces)

HORIZON-CL3-2027-02-CS-ECCC-02

Program:	**Horizon Europe Cluster 3**
Típus:	**Innovation Action**
TRL szint:	**-**
Támogatás projektenként:	**3-5 M EUR**
Támogatott projektek száma:	**5-7**
Pályázati felület megnyílik:	**2027 március 2**
Beadási határidő:	**2027 szeptember 15**
Felhívás linkje:	LINK

This topic aims to advance security across the entire computing continuum, spanning IoT devices, edge computing, cloud infrastructures, and data spaces. Proposals should address critical challenges such as ensuring data integrity in highly distributed and dynamic environments, implementing robust zero-trust architectures to secure interconnected and heterogeneous systems, and enabling comprehensive protection for sensitive data and processes.
Privacy should be considered a core element of these approaches, ensuring that data confidentiality is preserved throughout its lifecycle, in compliance with relevant data protection frameworks, such as GDPR. Solutions are expected to deliver tangible and measurable security improvements across all layers of the continuum, prioritizing scalability, interoperability, security and resilience against emerging threats.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu

Secure PQC implementations, Cryptanalysis and Post-quantum Digital Trust

HORIZON-CL3-2027-02-CS-ECCC-03

Program:	**Horizon Europe Cluster 3**
Típus:	**Research & Innovation Action**
TRL szint:	**-**
Támogatás projektenként:	**4-5,5 M EUR**
Támogatott projektek száma:	**3-4**
Pályázati felület megnyílik:	**2027 március 2**
Beadási határidő:	**2027 szeptember 15**
Felhívás linkje:	LINK

Proposals should address one of the following technology areas:

A. **Development of solutions to prevent implementation attacks**, balancing security, performance and cost; research in new attacks, including AI-powered ones, and/or combination of attacks, to inform secure design; creation of testing frameworks for automated security evaluations; improvement of formal verification methodologies.

B. **Quantum hardness analysis**, via development of new quantum algorithms or improvement of existing quantum algorithm implementations, also leveraging AI if relevant and combining with AI-capabilities; analysis of cryptanalysis results; design of new post-quantum cryptosystems using these advances/ fine-tuning of parameters set for existing PQC schemes. Design of quantum-resistant algorithms supporting the field of electronic identities and other advanced cryptographic blocks for verification protocols; new digital signature schemes and key encapsulation mechanisms for scalable and performant PQC implementations to be demonstrated in real world scenarios; implementation of formal verification techniques for post-quantum digital identity and digital trust systems.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu

New primitives for functionalities of future hybrid quantum-classical and quantum networks

HORIZON-CL3-2027-02-CS-ECCC-04

Program:	**Horizon Europe Cluster 3**
Típus:	**Research & Innovation Action**
TRL szint:	**-**
Támogatás projektenként:	**4 M EUR**
Támogatott projektek száma:	**1**
Pályázati felület megnyílik:	**2027 március 2**
Beadási határidő:	**2027 szeptember 15**
Felhívás linkje:	LINK

The action supports research on new quantum primitives and protocols for security and trust-based applications, by combining different cryptographic approaches and exploiting insights from quantum information science, to demonstrate quantum cryptographic advantage and obtain foundational results on the unique features of quantum protocols. The goal is to build the cryptographic foundations of hybrid quantum-classical and future quantum networks, where the latter may require entirely new paradigms whose design requires different expertise.

Proposals should include quantum scientists as well as researchers from PQC with interest in quantum protocols and from other fields.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu