HORIZON EUROPE

PROJECT PARTNER SEARCH FORM

HORIZON-CL3-2026-02-CS-ECCC
Deadline: 15 September 2026, 17:00 CEST

Kaitan (ProkaitanSystems OÜ) – seeking participation as a consortium partner

Estonian deep-tech SME · cryptographic data integrity and provenance for defence, space and critical infrastructure

[x] I offer my expertise to participate as a **Partner** in a Horizon Europe project
[ ] I am planning to coordinate a project and I am looking for project partners

Call topics

HORIZON-CL3-2026-02-CS-ECCC-01 – Approaches and tools for security in software and hardware development and assessment (RIA)

Addressing in particular: *enhanced security frameworks for both hardware and software supply chains, building on root-of-trust architectures and secure lifecycle management*, and contributing to standardised assessment and cybersecurity certification.

HORIZON-CL3-2026-02-CS-ECCC-02 – Enhancing the Security, Privacy and Robustness of AI Models and Systems, SecureAI (IA)

Provenance and tamper-evident lineage of models, training data, and inference records — detecting and evidencing data poisoning and backdoor insertion, and supporting AI transparency and AI Act compliance for trusted in-house deployments.

HORIZON-CL3-2026-02-CS-ECCC-03 – Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations (RIA)

Hash-based, non-lattice quantum-resistant constructions for integrity, timestamping and evidence that must remain verifiable across a post-quantum migration.

Expertise offered

Kaitan is an Estonian deep-tech SME building cryptographic data-integrity and provenance infrastructure for mission-critical systems. What we bring to a consortium is a way to replace assumptions about data with mathematical proof: that an artefact is authentic, unaltered since a given moment, and traceable to its origin.

Contribution offered — tasks Kaitan can take

- **Root-of-trust provenance at supply-chain handover.** Cryptographic anchoring and independent verification of software and hardware artefact origin and integrity at each transfer between supplier, integrator and operator; binding SBOM/CBOM, build attestations, signing events, test evidence and release artefacts into tamper-evident records that a recipient can check against claimed or published reports.
- **Trusted lifecycle and configuration history.** Append-only, independently auditable records of component, firmware and configuration state across secure lifecycle management — usable as assurance evidence under the Cyber Resilience Act, NIS2 and cybersecurity certification schemes.
- **Integrity at the point of data capture.** Anchoring measurement, sensor and log data at the moment of digitisation, so that everything downstream can be traced back to an authenticated origin rather than trusted on assertion.
- **Security architecture, threat modelling and requirements** for the trust and provenance layer, including its interfaces to the rest of the system; contributions to standardisation and certification.
- **Work-package leadership** on the above, plus integration and pilot validation in defence, space and critical-infrastructure environments.

Keywords

Cryptographic data integrity; software and hardware supply-chain provenance; root of trust; SBOM / CBOM anchoring; tamper-evident and append-only logs; keyless hash-based signatures; quantum-resistant integrity proofs; DLT; independent and offline verification; secure lifecycle management; NIS2; Cyber Resilience Act; AI provenance and lineage; dual-use; defence, space and critical infrastructure.

Activity offered	Research · Technology development · Integration · Demonstration and validation · Standardisation and exploitation
Type of organisation	Industry / SME (deep-tech)
Country / region	Estonia — EU Member State; open to consortia across EU Member States and Horizon Europe Associated Countries

Previous experience

- **Horizon Europe:** confirmed consortium partner in a funded 2026 Cluster 3 project on cyber-resilience of autonomous systems.
- **European Space Agency:** several ongoing contracts.
- **European Defence Fund:** active consortium positioning; member of the Estonian Defence Industry Association (EKTL).
- **Heritage:** founding team and scientific advisory rooted in Estonia's pioneering work on hash-based, national-scale data-integrity infrastructure; Kaitan's own architecture is independent background IP.

Contact data

Organisation	Kaitan — legal entity ProkaitanSystems OÜ (registry code 17400815)
Organisation type	Industry / SME
Contact person	Margo Raja, Technical Innovation Manager
Email	margo.raja@kaitan.eu
Website	https://kaitan.eu