# SELFY - a proposal recently accepted for funding by the EU Commission - Okayama University is the Japanese University of the Consortium and will keep on promoting leadership in cybersecurity

*In SELFY Okayama University (Pr. NOGAMI Yasuyuki group) will*
*a - provide feedback on the proposed Verification and Validation (V&V) techniques for the evaluation of the CCAM system robustness, particularly of cryptography performance level. Design-time / run-time verification can assess weak points on models or implementations of CCAM systems showing the actual robustness of embedded cryptosystems (Task 4.6)*
*b -participate in the identification and analysis of lightweight post-quantum/classical cryptographic algorithms adapted to CCAM systems*

## **SELF** assessment, protection and healing tools for a trustworth**Y** and resilient CCAM

*CCAM - Cooperative Connected Automated Mobility*

| Participant No. | Participant organisation name | Acronym | Country |
|---|---|---|---|
| 1 (Coord) | Fundació Eurecat | EUT | ES |
| 2 (Partner) | Commissariat à l'énergie atomique et aux énergies alternatives | CEA | FR |
| 3 (Partner) | Technische Hochschule Ingolstadt | THI | DE |
| 4 (Partner) | Fundación Tecnalia Research & Innovation | TEC | ES |
| 5 (Partner) | Technische Universiteit Eindhoven | TUE | NL |
| 6 (Partner) | Canon Research Centre France | CRF | FR |
| 7 (Partner) | FEV TR Otomotiv ve Enerji Arastirma ve Muhendislik Limited Sirketi | FEV | TR |
| 8 (Affiliated) | FEV Europe GmbH | FEV EU | DE |
| 9 (Partner) | Ficosa ADAS, S.L.U. | FICO | ES |
| 10 (Partner) | Idiada Automotive Technology SA | IDI | ES |
| 11 (Partner) | Virtual Vehicle Research GmbH | VIF | AT |
| 12 (Partner) | Yogoko | YGK | FR |
| 13 (Partner) | Stadt Wien | VIE | AT |
| 14 (Partner) | Asociación Española del Vehículo Autónomo Conectado | AEVAC | ES |
| 15 (Associated) | Royal Melbourne Institute of Technology | RMIT | AU |
| 16 (Associated) | OKAYAMA University | OKA | JP |

Cooperative Connected Automated Mobility (CCAM) is increasingly becoming a major cybersecurity concern and is pushing a lot developments in improved connectivity and digitalization, and evolution of solutions based on artificial intelligence and big data analytics.

CCAM related services and products will require high resilience to prevent mobility services disruption and human harm in case of fraud, cyberattack or cyberterrorism events.

Securing flows of generated and processed data between all stakeholders is vital for a correct, efficient, and robust management of the different services and systems in the CCAM context. Ensuring the veracity, quality and integrity of the data generated is essential in the process of mobility management and control, both in the stages of persistence, transmission, access and use of the information.
SELFY's strategic vision is to become the main European provider of an agnostic toolbox for the self- management of security and resilience of the CCAM ecosystem. It is expected to be easily rooled out over the CCAM environment to provide self-awareness, self-resilience and self-healing mechanisms and end-user trust.

SELFY is organised around four pillars
(i) main pillar of SELFY: convey trust to all stakeholders by increasing the acceptance and adoption of CCAM services and solutions, by developing tools to guarantee privacy, confidentiality, integrity and immutability of data in a collaborative CCAM environment.
(ii) Situational awareness, addressing which type of data must be generated and collected, and how it is used for monitoring any given CCAM ecosystem.
(iii) Data sharing, addressing advanced processing for detection of malicious events and decision-making.
(iv) Resilience, by developing new tools to increase the ability to adapt and respond to cyber- threats and cyber-attacks on assets, services and products in the CCAM domain, reducing their impact and the disruption of associated services.

In SELFY Okayama University (Pr. NOGAMI Yasuyuki group) will
a - provide feedback on the proposed Verification and Validation (V&V) techniques for the evaluation of the CCAM system robustness, particularly of cryptography performance level. Design-time / run-time verification can assess weak points on models or implementations of CCAM systems showing the actual robustness of embedded cryptosystems (Task 4.6)
b -participate in the identification and analysis of lightweight post-quantum/classical cryptographic algorithms adapted to CCAM systems