Ministero delle Imprese e del Made in Italy

SSSTLC Scuola Superiore di Specializzazione in Telecomunicazioni

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

UNIVERSITÀ DEGLI STUDI DELL'AQUILA

DISIM Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica

EXEMERGE CELLENCE

**Automotive e cybersecurity: vulnerabilità, sistemi di protezione e quadro normativo**
**Webinar – 2024-04-11**

# Il cluster automotive dell'Abruzzo – L'esperienza del Centro di Eccellenza ExEmerge


**Prof. Fortunato SANTUCCI**
**Dott. Walter TIBERTI**

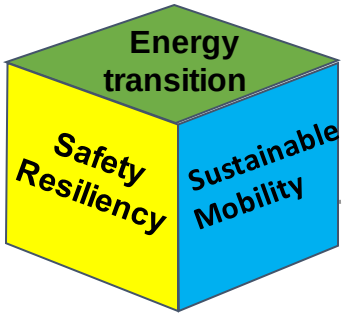
**University of L'Aquila – DISIM ExEmerge Centre of Excellence**
fortunato.santucci@univaq.it - walter.tiberti@univaq.it

# Agenda

- Scenari di riferimento
- Un ecosistema per l'innovazione
- Il progetto EMERGE
- Focus sulla sicurezza nelle comunicazioni intra-veicolari
- Il *Crypto-Engine*
- Il ruolo del Crypto-Engine in EMERGE e SHINE-ON

# Reference Scenario

Towards a connected, cooperative, secure and de-carbonised transport system




**Connected, secure and integrated mobility,**
**More sustainable powertrains**

**Digital Railways, Autonomous Vehicle**
**Accessibility and modal integration**
**Eco-sustainability of rail transport**

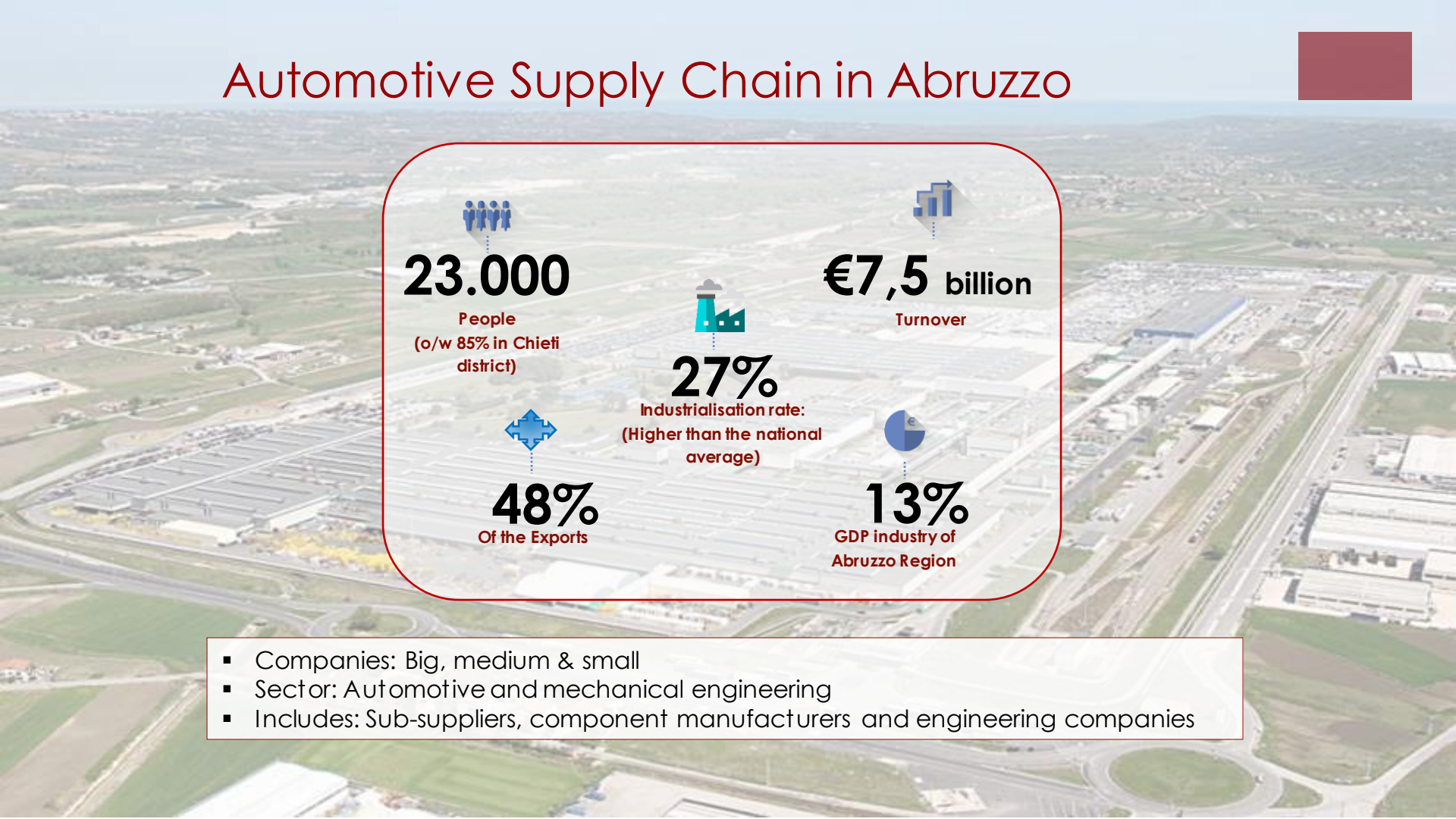

**Efficient, environmentally sustainable and integrated ship and infrastructure**
**New services**
**(e.g. assisted berthing, autonomous navigation)**

**ITS**

***MaaS*: from vehicle-centered to service-centered**

Innovation creates **new models of mobility** and cannot be left to market forces alone but must be accompanied by a national support policy that focuses on sustainable growth, **made in Italy** and the creation of **new jobs with high skills**

# Automotive Supply Chain in Abruzzo




- Companies: Big, medium & small
- Sector: Automotive and mechanical engineering
- Includes: Sub-suppliers, component manufacturers and engineering companies

# Abruzzo Smart Specialization 2021-27

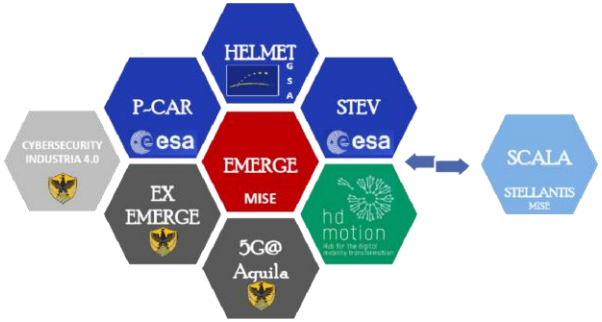
Abruzzo Region S3 development goals include
**Automotive and Aerospace**

| Domini S3 | S3 2021-2027<br>Traiettorie di sviluppo S3 |
|---|---|
| Automotive | ▪ Veicoli commerciali multienergy e con motopropulsori più sostenibili e allestiti per l'ultimo miglio<br>▪ Materiali e tecnologie per il miglioramento del rapporto tra prestazioni, qualità, pesi e costi<br>▪ Materiali a basso impatto ambientale, materiali smart e processi produttivi correlati a favore di un'economia circolare<br>▪ Green factory<br>▪ veicoli connessi e servizi per la mobilità connessa<br>▪ smart e digital factory |
| Aerospazio | ▪ Progettazione, sviluppo e realizzazione di sistemi elettronici, micro e nanotecnologie applicate alla sensoristica e alla elettronica di potenza<br>▪ Sistemi ed applicazioni per il monitoraggio e controllo di sistemi e ambiente e tracciamento di persone ed oggetti<br>▪ Sistemi di comunicazione e osservazione della terra anche mediante satelliti e droni<br>▪ Cyber Security<br>▪ Sviluppo di piattaforme di elaborazione e storage sicure e orientate alla logica cloud e multiaccess edge computing<br>▪ Sviluppo di piattaforme satellitari e di Payload innovativi |

***Satellite technology advancements will be critical to achieve the Sustainability, safety and security goals***

# Abruzzo Region Innovation Ecosystem

## Public-Private Entrepreneurship




### January 2020

**EMERGE Navigation**

RadioLabs

**Elital, Leonardo, Telespazio, UnivAQ**

Prototyping on light commercial vehicles of KET for CCAM and on-field trials

**MIMIT & Abruzzo Region**

### December 2019

Phase 1 - March '21
Phase 2 - October '24

### January 2024

**MIMIT - PNRR**

**HD-Motion**

+CIM4.0

**9 Italian Partners Plus 5 Affiliated Entities**

Support to SMEs and PAs in the Digital Mobility Transformation

### January 2019

**SCALA**

STELLANTIS

**In synergy with EMERGE Navigation**

Advanced applications for connected. geo-localized and cybersecure vehicles

**MIMIT & Abruzzo Region**

**Centre Ex-EMERGE**

UNIVERSITÀ DEGLI STUDI DELL'AQUILA

**Research infrastructure connected with the University**

Advanced research on connected vehicles

**Specific action of Italian Government (RESTART)**

**P-CAR**

RadioLabs

**UnivAQ & Polo Automotive Abruzzo**

Lab for safety and performance evaluation of GNSS-based positioning for CCAM.

**ESA-NAVISP EI3**

**SHINE-ON**

RadioLabs

**UnivAQ, Cyber 4.0, Drivesec**

Cybersecurity for vehicle on-board ECUs

**MIMIT**

**CYBORG**

RadioLabs

**UnivAQ, Cyber 4.0, Drivesec**

Test-bed for acquiring GNSS data for CCAM applications.

**MIMIT**

**AS-ITc**

TIM

**EagleProjects, Radiolabs, NITEL, ADPM Drones, ASPI**

Test-bed for acquiring GNSS data for CCAM applications.

**ESA ARTES**

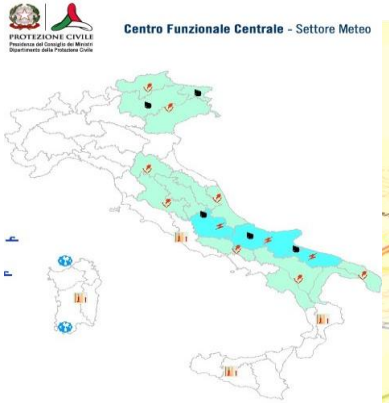
# *EMERGE*: a first project for Abruzzo automotive sector

Innovation agreement by **MISE**, **Radiolabs**, **Leonardo**, **Telespazio University of L'Aquila**, **ELITAL** and with the contribution of **Regione Abruzzo**

***Connected, Geo-localized*** *and* ***Cyber-secure*** *vehicles*

- **Target applications:**
- Transport logistics
- Emergencies

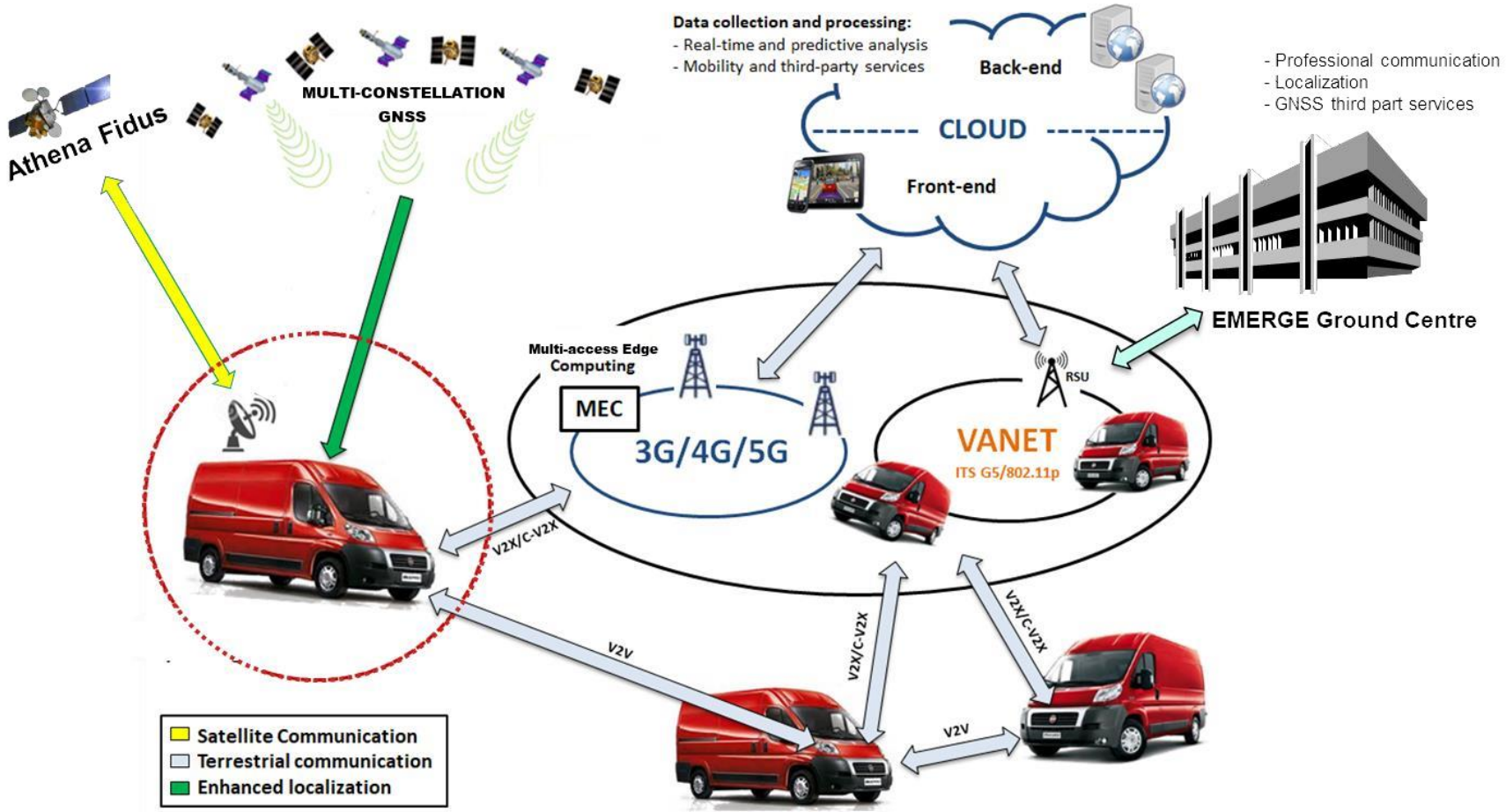
**Security *margin***: anticipate and notify road dangers and obstacles





**Dynamic Navigation**: on-map dynamic events, pre-trip planning and fleet management.
***"Last mile"*** preferred corridors for urgent transportations

# *EMERGE*: project overview

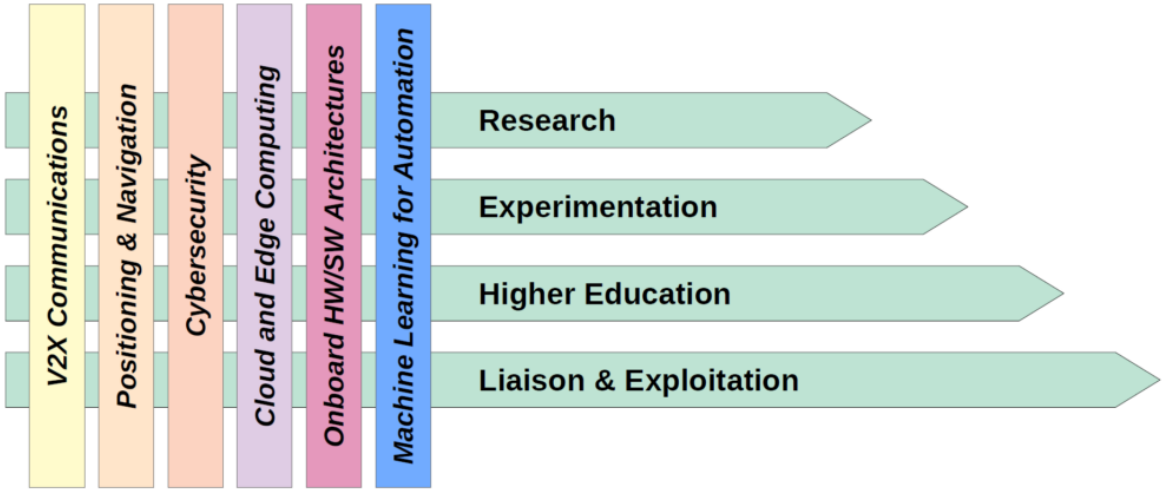


# The ExEmerge Centre of Excellence

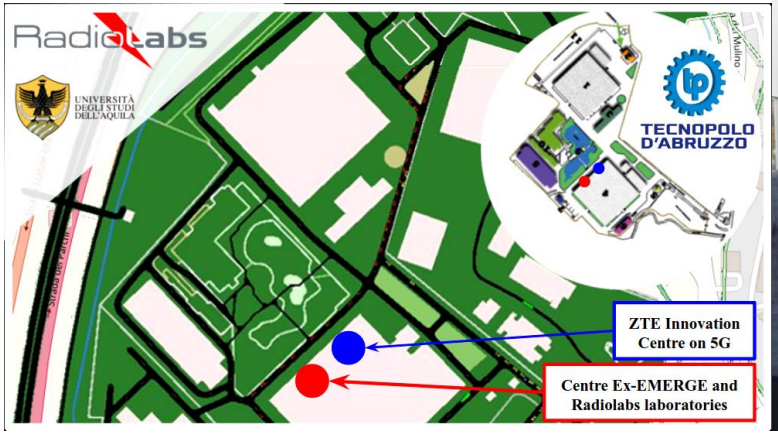
http://exemerge.disim.univaq.it

| ExEmerge board | |
|---|---|
| Vittorio Cortellessa | vittorio.cortellessa@univaq.it |
| Alessandro D'Innocenzo | alessandro.dinnocenzo@univaq.it |
| Gabriele Di Stefano | gabriele.distefano@univaq.it |
| Norberto Gavioli | norberto.gavioli@univaq.it |
| Costanzo Manes | costanzo.manes@univaq.it |
| Patrizio Pelliccione | patrizio.pelliccione@univaq.it |
| Marco Pratesi | marco.pratesi@univaq.it |
| Fortunato Santucci | fortunato.santucci@univaq.it |

**Centre of EXcellence (EX) on Connected, Geolocalized and Cybersecure vehicles (*EX-EMERGE*)**



# Center of Excellence ExEMERGE and Radiolabs laboratory





# Dedicated mobile laboratories

For the purposes of the project, the preparation of 5 vehicles in 3 different configurations is envisaged:

1. **full** *(1 vehicle)* - GEO SATCOM on-the-move, SATNAV, IMU, 4G/5G/V2X Comms, IP cameras
2. **medium** *(2 vehicles)* - SATNAV, IMU, 4G/5G/V2X Comms, IP cameras
3. **small** *(2 vehicles)* - 4G/5G/V2X Comms, IP cameras


A ***full*** vehicle has been configured and approved as mobile laboratory according to the Italian regulation.

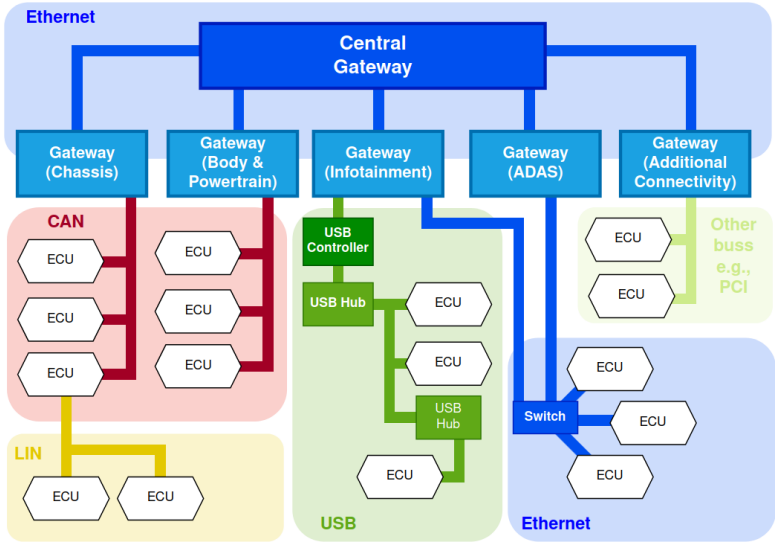
# *Focus on* Cyber-Security - Securing intra-vehicle communications

**Objective**: securing intra-vehicle communications (e.g., CAN bus, Automotive Ethernet, etc.)

**Challenges**: vendor/platforms heterogeneity, complexity, slow adoption, real-time requirements

## Cybersecurity **Requirements**

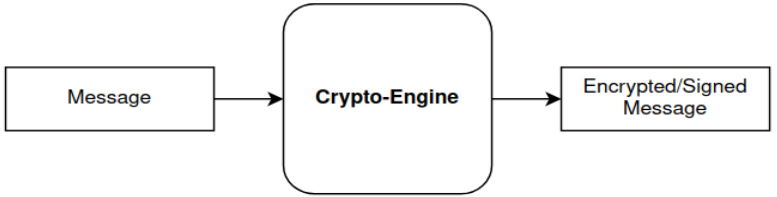
- Defined according **ISO 31000:2018** "Risk Management"
- Definition of the **minimum** security features required in terms of *BUY* and *MAKE*
- Other relevant standards:
  - **ISO 26262**
  - **ISO/SAE 21434** (Cybersec. Requirements for Road Vehicles HRA)
  - **SAE J3061**



# Our solution: *Crypto-Engine*

- The **Crypto-Engine** is a logically-centralized component that aims **to provide cyber-security functions** in a large number of automotive platforms, including those **having no cyber-security features** at all
  - The Crypto-Engine provides:
    - **Confidentiality** via hybrid public-key encryption
    - **Authentication** via public-key signature
    - Key exchange and management services

- ***Main features:***
- Cryptography-as-a-service via **ECTAKS**
- **Independence** from the communication bus
- Supports **hardware accelerators**
- Embeddable in ECUs




Using **ECTAKS**, the Crypto-Engine provides cryptographic services without **storing the full cryptographic keys**

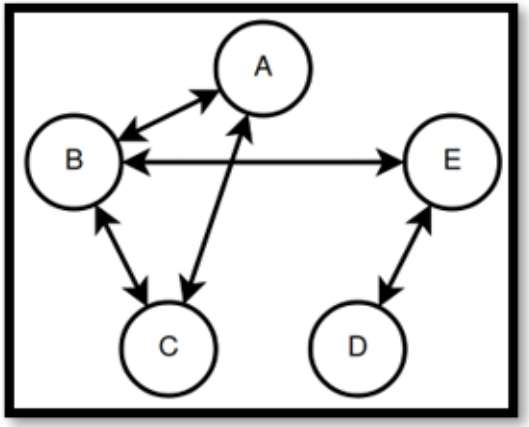
# TAKS & ECTAKS

- **TAKS [4,5,6]**– *Topology-Authenticated Key Scheme*: cryptographic scheme designed for Wireless Sensor Networks. Features:
  - Limited requirements (**8 KiB** of RAM, **48 KiB** of storage)
  - Key exchange mechanism: the cryptographic keys are constructed/reconstructed by defining an ***Authenticated Topology***

- **ECTAKS [1,2,3]** – evolution of TAKS towards Elliptic Curve Cryptography
  - Provides customized ECIES and ECDSA
  - Verified to be as secure as the ECDPL problem. Security proof in **[3]**
  - Curve-independent (prime and binary* curves)
  - Can **natively protect multicast communications** without key distribution or additional overhead
  - State-of-the-art algorithms for symmetric encryption and hashing

# ECTAKS: background

An **Authenticated Topology** is a directed graph ANT = (V, E) where V is the set of the network nodes and E is the set of edges between nodes entitled to communicate




**Key Components: e**ach node *i* is assigned with a Local Configuration Data (LCD) containing:

- A private **Local Key Component** $k_i$
- A private **Transmit Key Component** $t_i$
- For each edge *(i, j)* in the ANT, a public **Topology Vector** $m_{i->j}$
- $k_i$, $t_i$, and the $m_{i->j} \in (\mathbb{F}_p)^2$ , i.e., they are 2-dimensional vectors over a prime field with *p* elements

In the example:

- Each node has a $k_i$ and a $t_i$.
- Node A has a $m_{A->B}$ and $m_{A->C}$;
- Node B has a $m_{B->A}$, $m_{B->C}$ and $m_{B->E}$ ..and so on

# ECTAKS: background

When Node *i* wants to send data to Node *j*, it generates the **ECTAK** (shared secret). This secret is then fed into the KDF to generate the AES symmetric key

$$\mathrm{ECTAK}_{i\_j} \stackrel{\mathrm{def}}{=} \alpha \mathbf{k}_i \cdot (\mathbf{m}_{i\_j} G).$$

α = nonce
**G** = Generator (Point) of the selected EC

Node i sends the point $\alpha \mathbf{t}_i G$ along the encrypted message

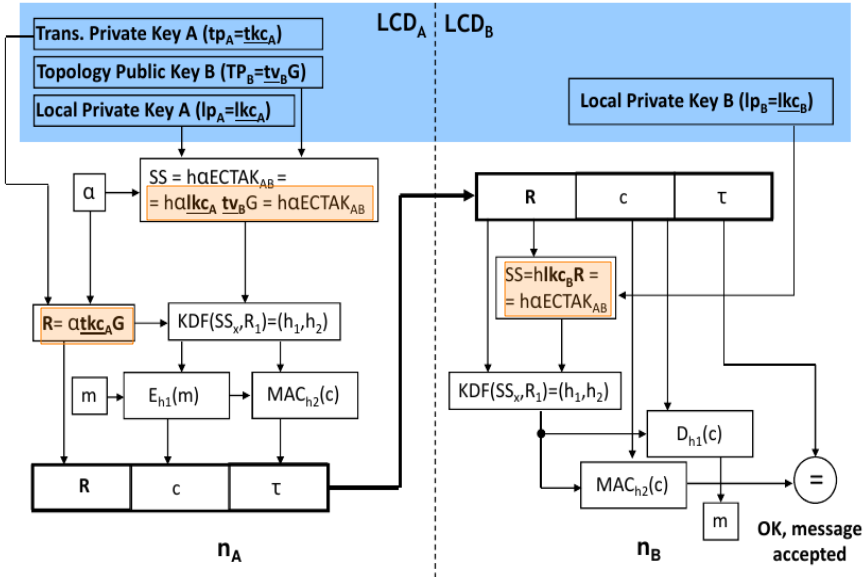
To recover the secret, Node *j* computes:

$$\mathbf{k}_j \cdot (\alpha \mathbf{t}_i G) = (\mathbf{k}_j \cdot \alpha \mathbf{t}_i) G = (\alpha \mathbf{k}_i \cdot \mathbf{m}_{i\_j}) G = \alpha \mathbf{k}_i \cdot (\mathbf{m}_{i\_j} G) = \mathrm{ECTAK}_{i\_j}$$

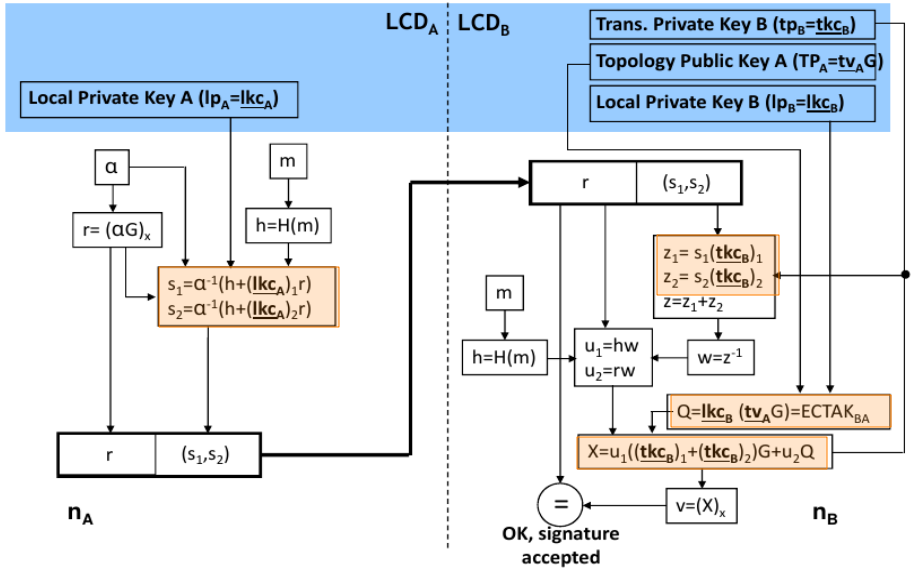
And uses the shared secret in the KDF to obtain back the AES key to decrypt the message

# ECTAKS: protocols

## ECTAKS-ECIES




## ECTAKS-ECDSA

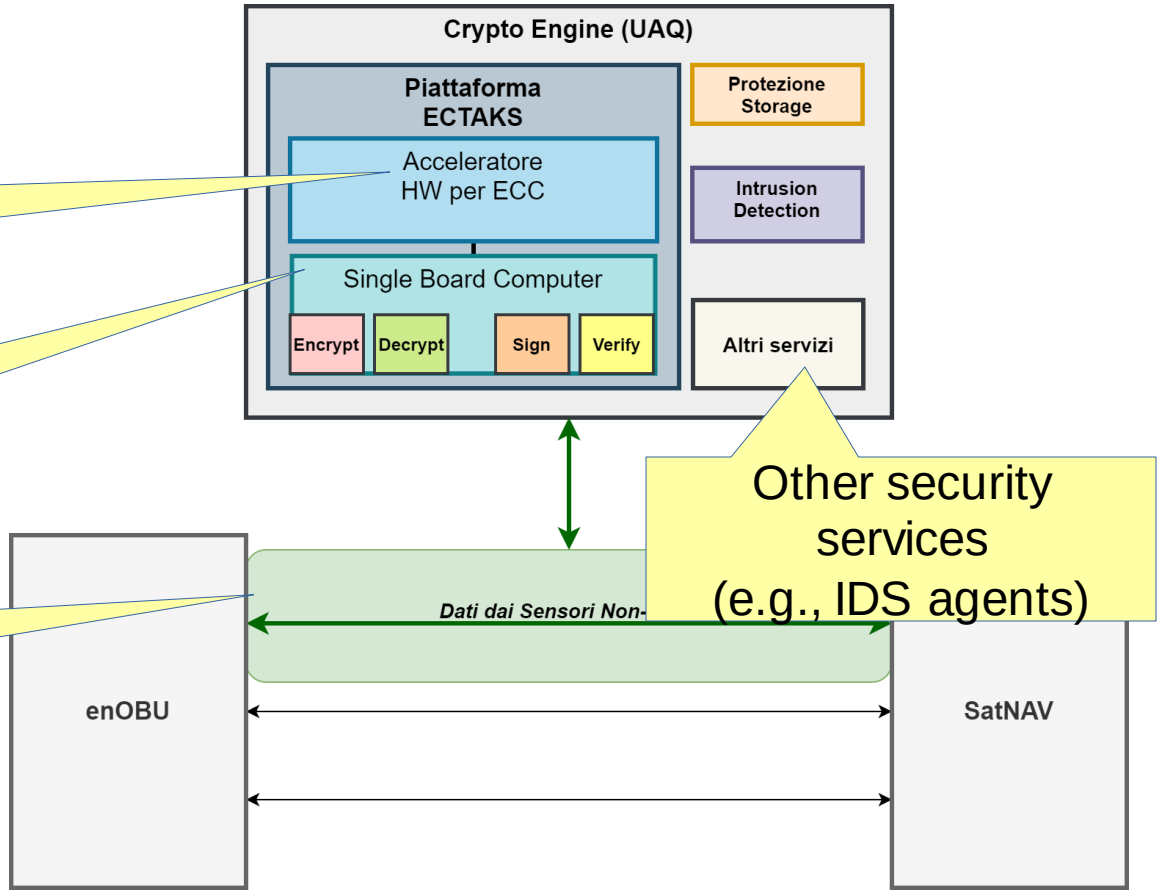


# The Crypto-Engine in EMERGE

Optional custom ECC Hardware acceleration

HW, SW or Virtual (VM/Container) platform

Non-GNSS data ecnryption & sign

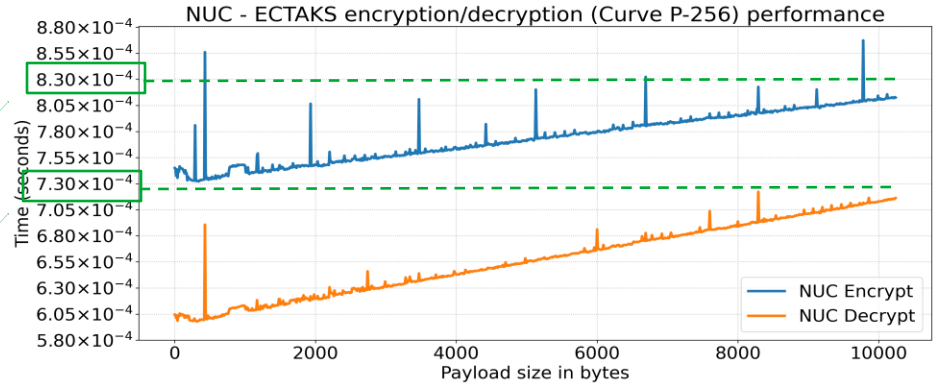


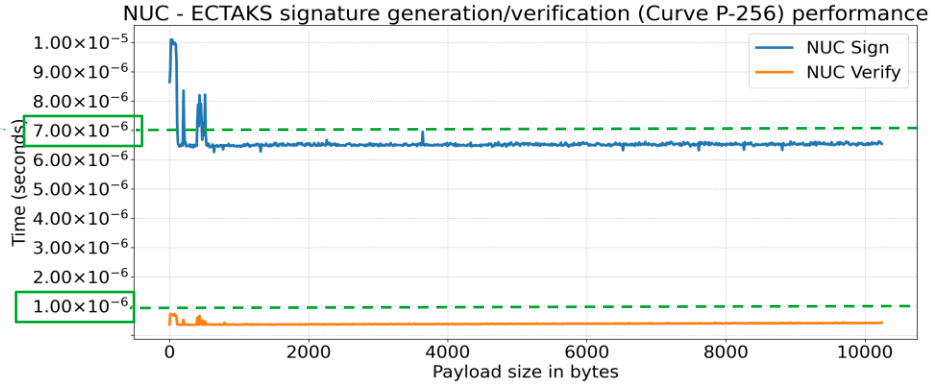
# Crypto-Engine: ECTAKS performance

- Payload: 1 Byte to 10KiB
- Plataform: Intel NUC N100
- Elliptic curve: NIST P-256

  - Encrypt: $t_{ENC}$ < 830 us
  - Decrypt: $t_{DEC}$ < 730 us

  - Sign: $t_{SIGN}$ < 7 us
  - Verify sign: $t_{VER}$ < 1 us

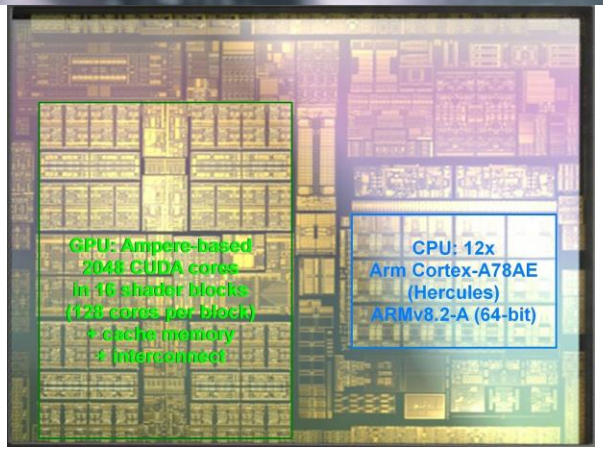


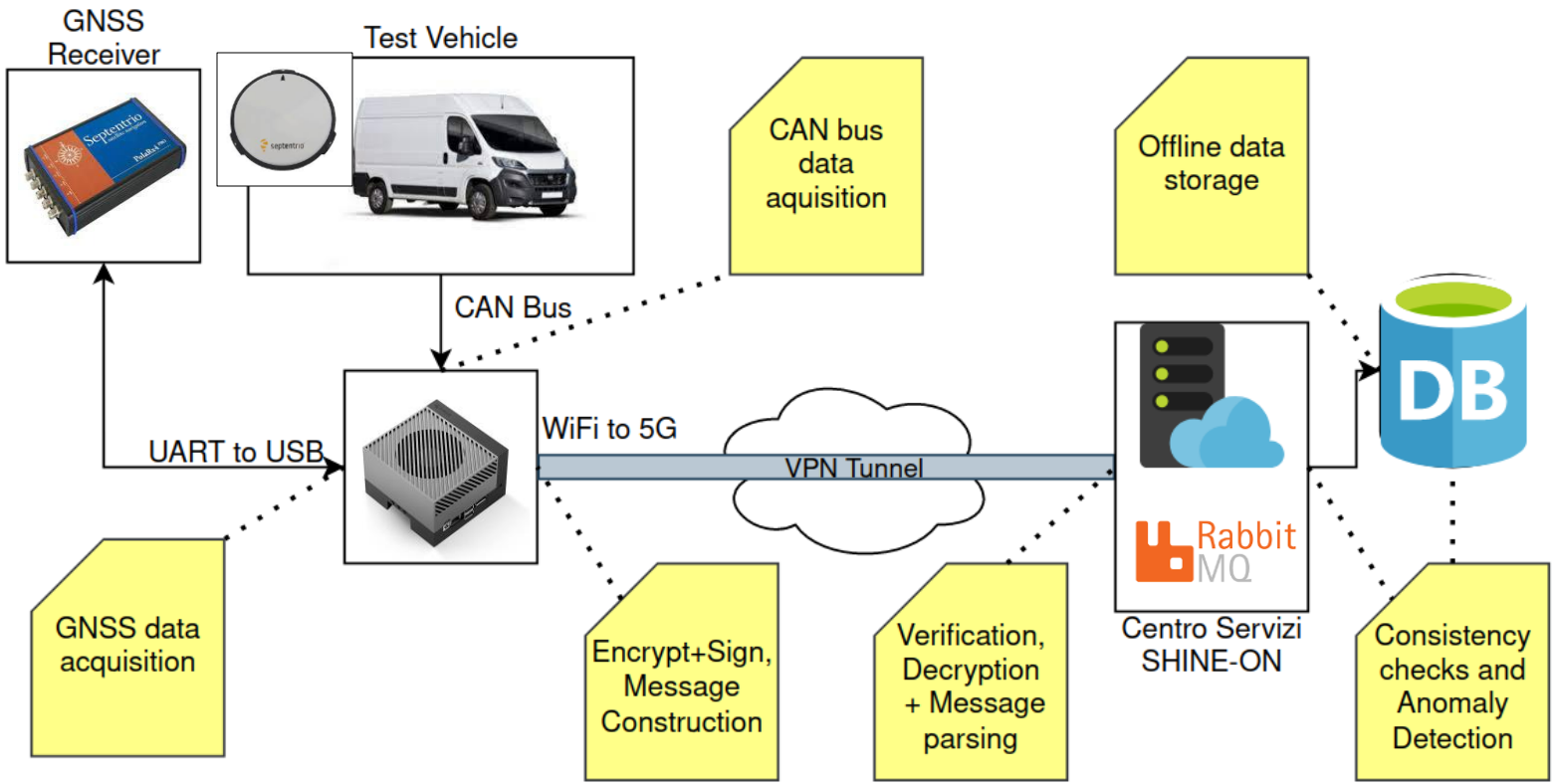
# SHINE-ON

*Secured HIgh accuracy localizatioN Equipment for autOmotive applicatioNs*

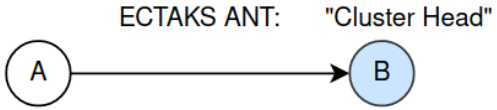
- Project founded by the **CYBER4.0 National Compotence Centre**
- Collaboration between Radiolabs and UnivAQ: *WP2 ECU "Secured GNSS Augmentation Module" SGAM* to improve the **Crypto Engine HW module**
- **Target TRL = 5**
- Exploitation of **NVIDIA-based GP-GPU platforms** for improving GNSS augmentation and security computations

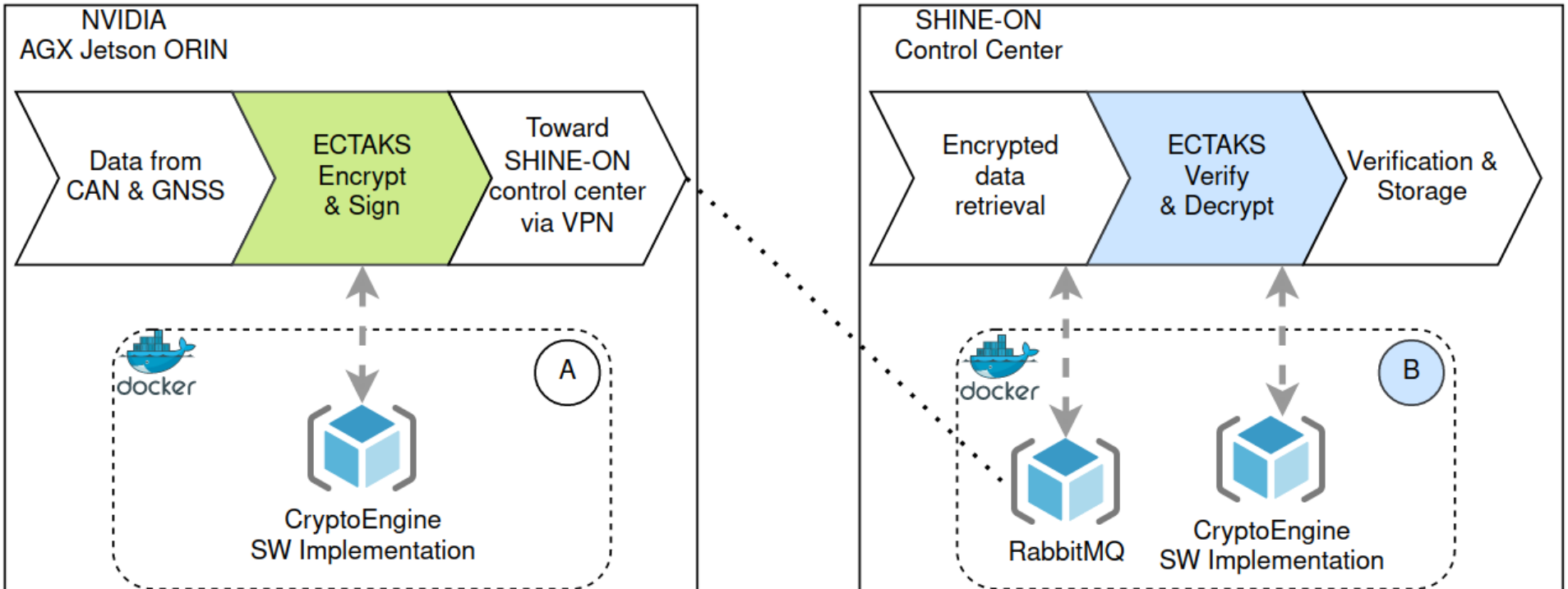


# The Crypto-Engine in SHINE-ON



# The Crypto-Engine in SHINE-ON



Ministero delle Imprese e del Made in Italy

SSSTLC Scuola Superiore di Specializzazione per le Telecomunicazioni e le Tecnologie dell'Informazione

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

# Gallery

Gallery

# References


1) Tiberti, W.; Civino, R.; Gavioli, N.; Pugliese, M.; Santucci, F. *A Hybrid-Cryptography Engine for Securing Intra-Vehicle Communications*. Appl. Sci. **2023**, 13, 13024. https://doi.org/10.3390/app132413024

2) Aragona R., Civino R., Gavioli N., Pugliese M., *An Authenticated Key Scheme over Elliptic Curves for Topological Networks*, Journal of Discrete Mathematical Sciences and Cryptography, Taylor & Francis, May **2021**.

3) Civino, Roberto, and Riccardo Longo. *Formal security proof for a scheme on a topological network.* Adv. Math. Commun 17 (**2023**): 562-571.

4) Marchesani S., Pomante L., Pugliese M., Santucci F., *Definition and Development of a Topology-based Cryptographic Scheme for Wireless Sensor Networks*, 4th International Conference on Sensor Systems and Software (S-CUBE2013), Lucca, Jun. **2013**

5) Pomante L., Pugliese M., Bozzi, L. Tiberti W., Grimani D., Santucci F., *SEAMLESS Project: Development of a Permorming Secure Platform for IEEE 802.15.4 WSN Applications*, EUROMICRO Conference on Digital System Design (DSD2020), Portorož, Aug. **2020**

6) Tiberti W., Caruso F., Pomante L., Pugliese M., Santic M., Santucci F., *Development of an extended Topology-based Lightweight Cryptographic Scheme for IEEE 802.15.4 Wireless Sensor Networks*, International Journal of Distributed Sensor Networks, SaGe Publishing, Oct. **2020**