

# Séminaire LRE 14/01/25

## Platelet: Pioneering Security and Privacy Compliant Simulation for Intelligent Transportation Systems and V2X



<https://gitlab.com/Matk3z/platelet>

**Mathias Kautz**

mathias.kautz@epita.fr

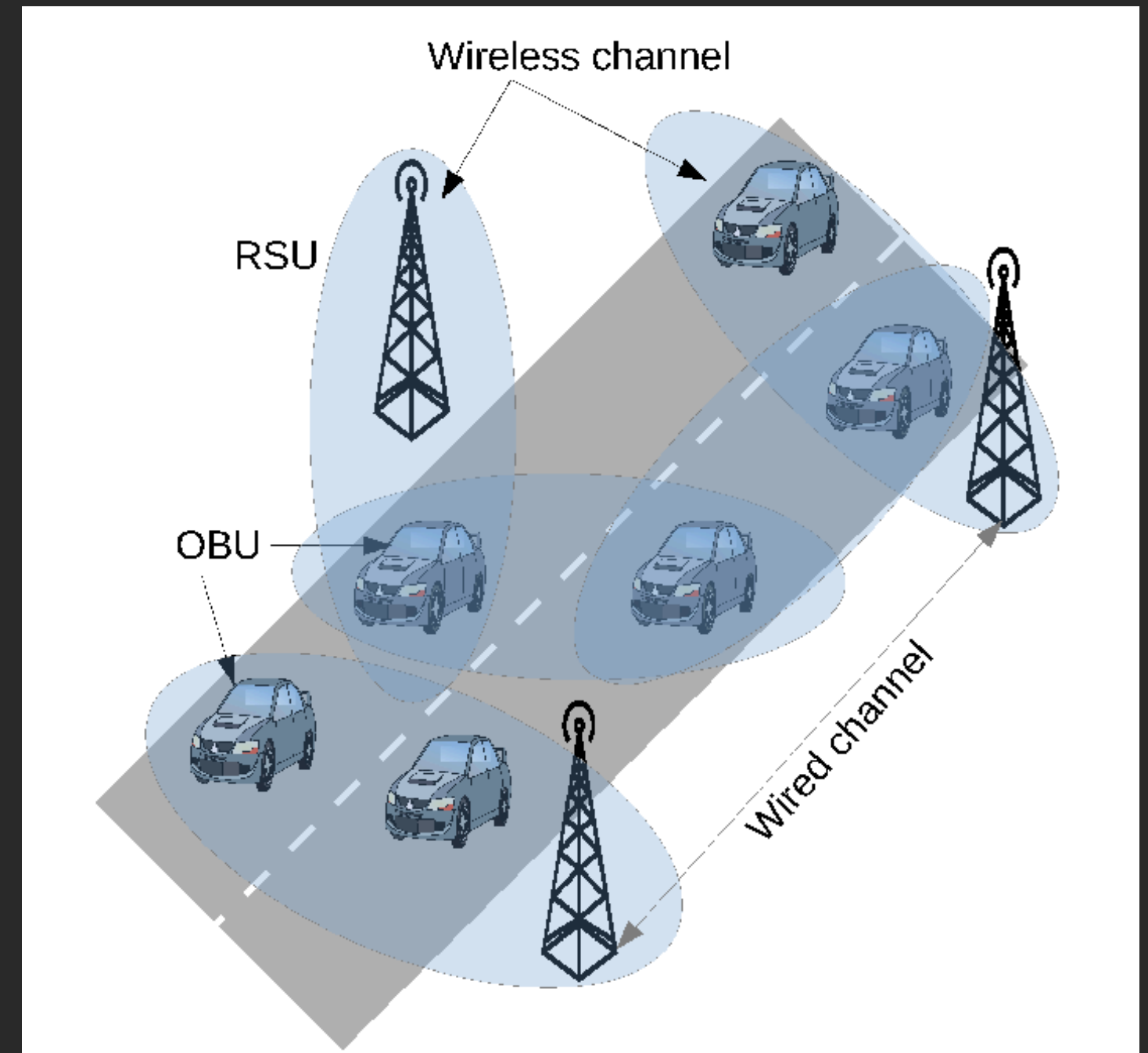
**Badis Hammi**

badis.hammi@telecom-sudparis.eu

# ITS (intelligent transportation system)

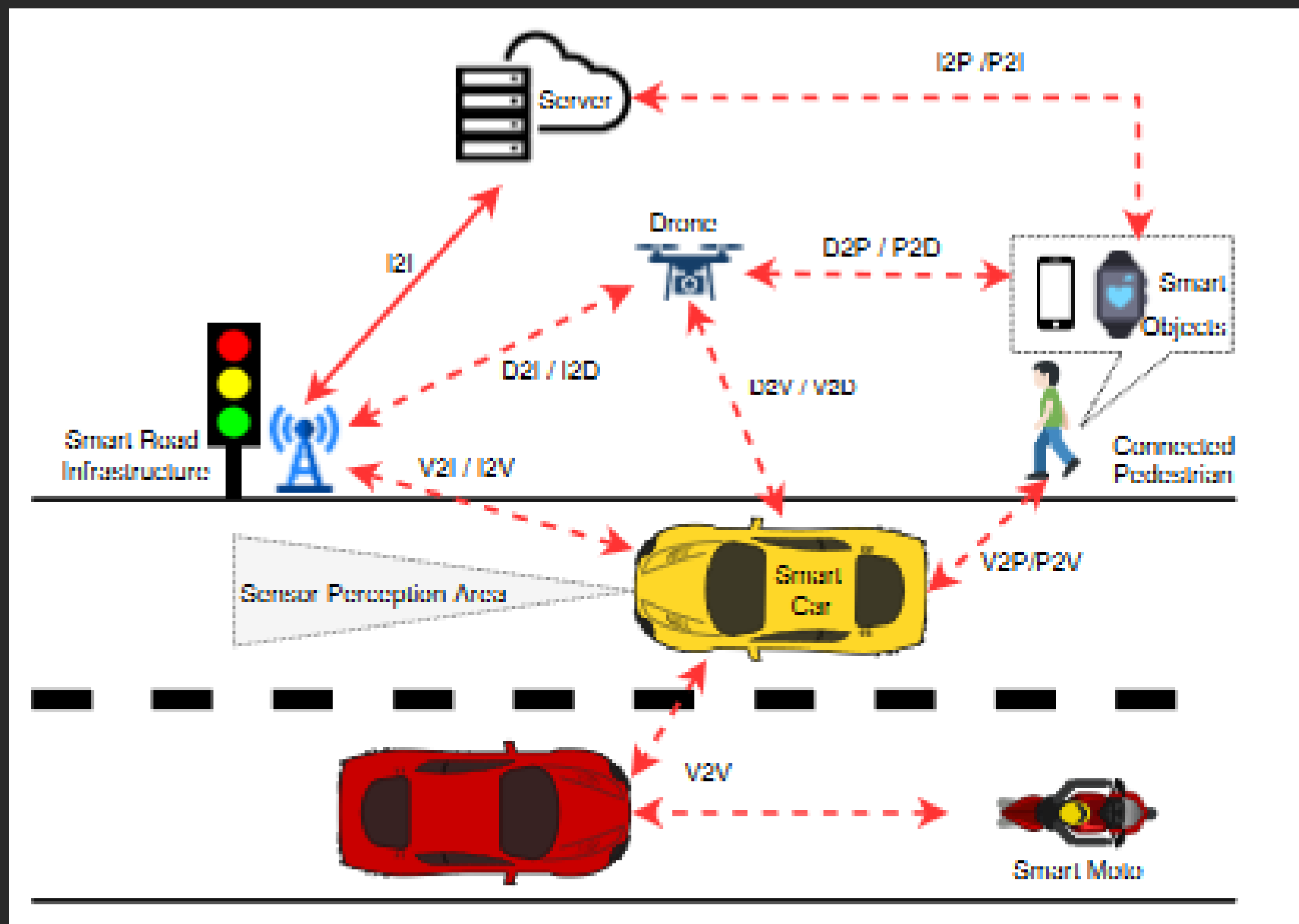
**Appliquer les nouvelles technologies  
au domaine des systèmes de  
transport**

Dans le contexte d'une ville connectée, la présence d'un réseau inter-véhicules est centrale.



Simple VANET network schematic [1]

# Réseaux C-ITS



Advanced C-ITS network [3]

Le réseau est composé de deux types de noeuds:

- RSU (road-side units)
- OBU (on-board units)

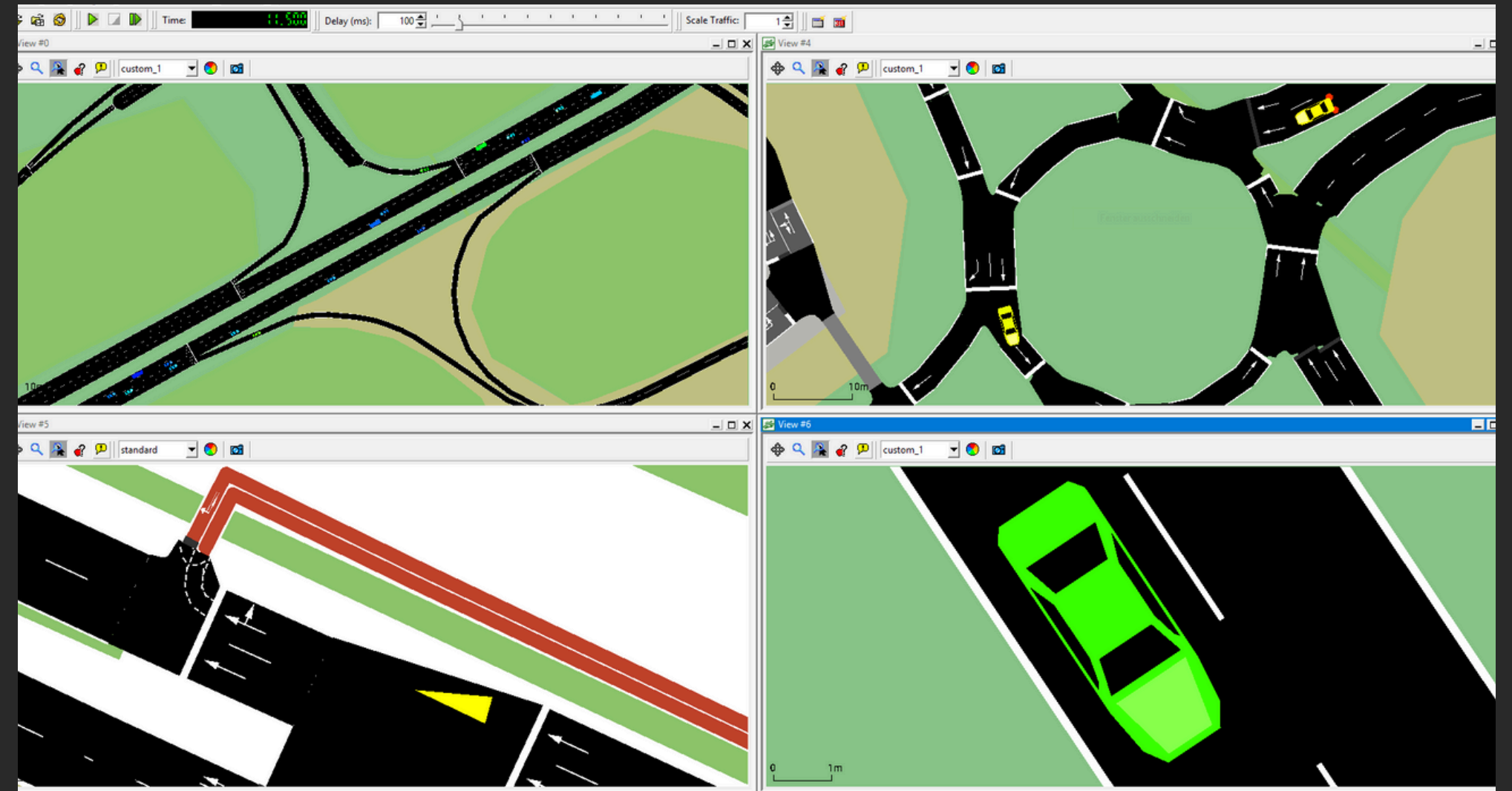
Au départ **Ad Hoc**, les solutions récentes se basent de plus en plus sur la présence **d'infrastructures existantes** (données cellulaires, serveurs centralisés, etc.).

# Simulateurs V2X

## Tester sur route = trop cher

Des simulateurs sont disponibles pour tester ces solutions dans des environnements numériques.

Les entreprises utilisent des simulateurs **closed source**, alors que les chercheurs académiques ont besoin de simulateurs **open source**.



SUMO simulation screen capture

# State of the art

Il existe beaucoup de simulateurs, mais ils sont **anciens** et répondent à des problématiques dépassées des réseaux V2X. Les simulateurs les plus récents implémentant les standards de l'ETSI sont **Artery et iTetris**.

Artery et iTetris:

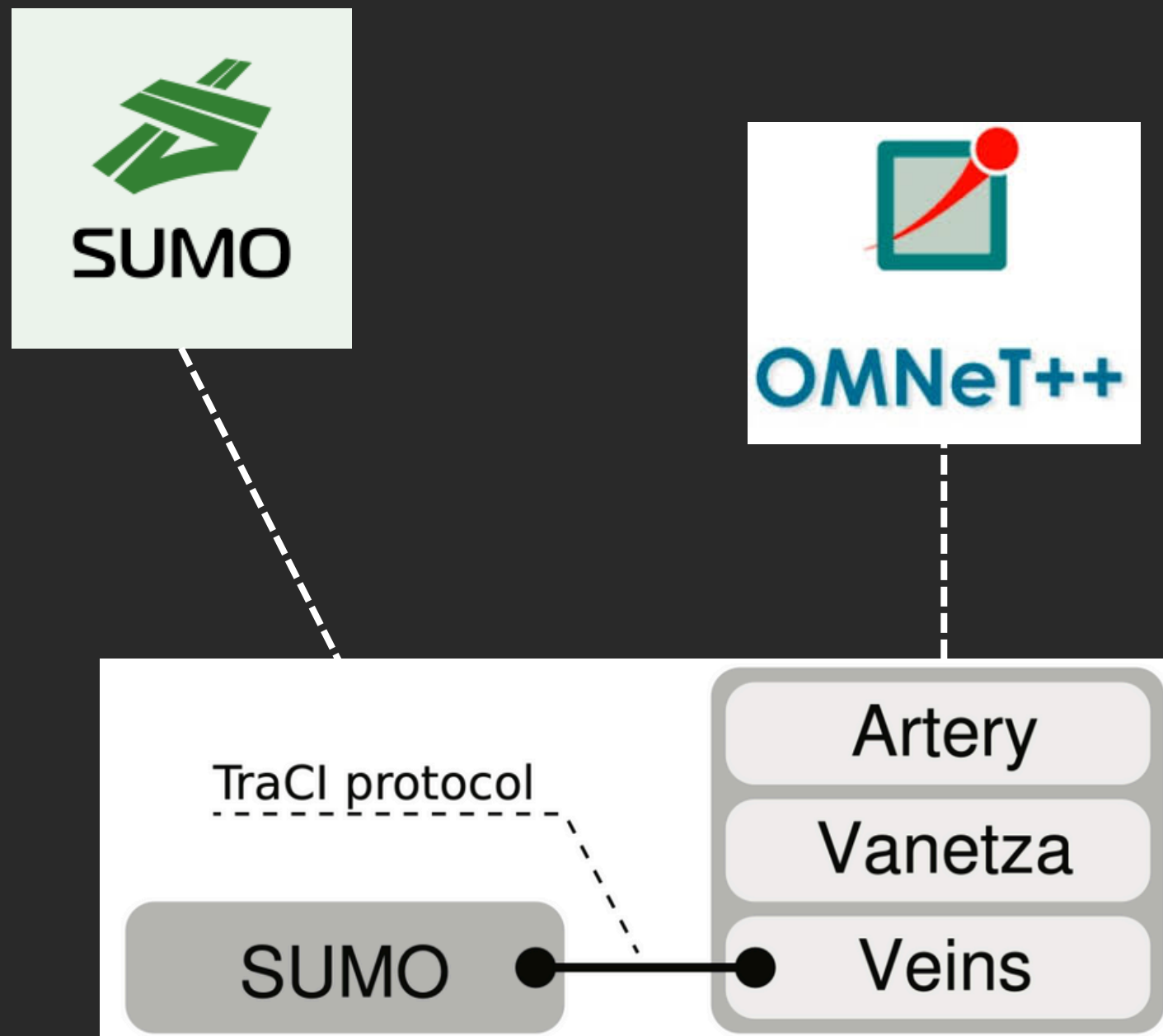
- Positif: les simulateurs les plus **performants** pour faire tourner des simulations ETSI
- Négatif: gros manque de considération pour la **sécurité** et la **confidentialité**



# State of the art

Simulator	Traffic simulation	Network simulation	ETSI-compliant	IEEE-compliant	5G and Beyond compatible	Signature implementation	Certificate renewal	pcap logging	EC and PC implementation	Certificate pool implementation
<i>TraNS</i>	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
<i>GrooveSim</i>	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗
<i>iTETRIS</i>	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
<i>Veins</i>	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗
<i>Artery</i>	✓	✓	✓	✗	✓	✓	✗	✗	✓	✗
<i>Platelet</i>	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓

# Architecture d'Artery



Artery simplified architecture [2]

Basé sur SUMO et Omnetpp

Le simulateur ITS ETSI **le plus avancé**

- Omnetpp: Network simulator
- SUMO: Traffic simulator
- Vanetza: Bibliothèque qui implémente le standard ETSI: grandement exploitée dans Artery et Platelet.



# SUMO

## SUMO

(Simulation of Urban MObility)

Simulateur de trafic routier **open source** développé dans le cadre du projet **Eclipse**

Permet d'importer des morceaux d'**Open Street Map** pour faire des simulations plus **réalistes**.



Exemple de simulation sur SUMO



# Omnet++

Framework open source de simulations de **réseaux**

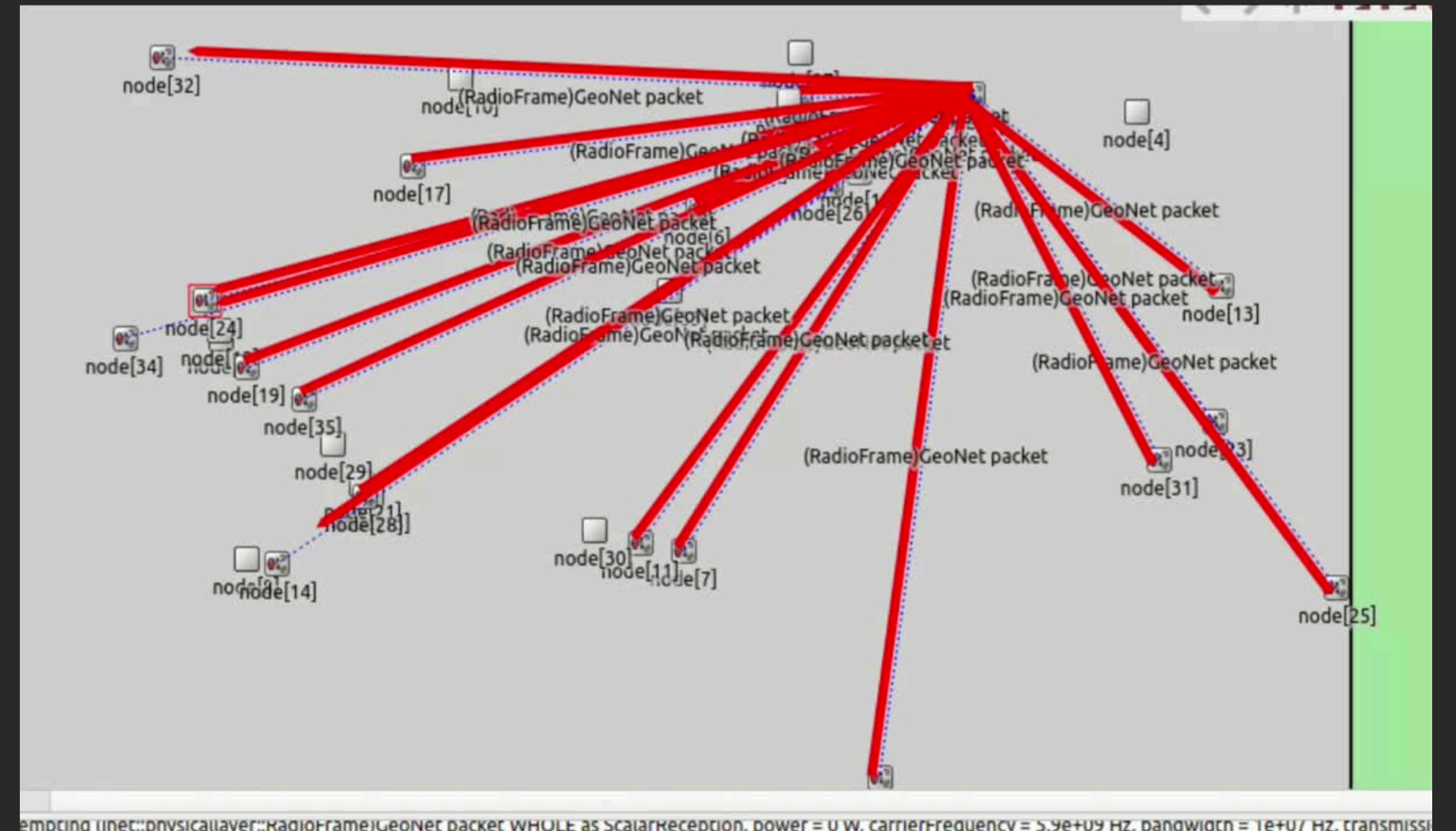
```
class Txc1 : public cSimpleModule
{
protected:
    virtual void initialize() override;
    virtual void handleMessage(cMessage *msg) override;
};

Define_Module(Txc1);

void Txc1::initialize()
{
    if (strcmp("A", getName()) == 0) {
        cMessage *msg = new cMessage("Hello World!");
        send(msg, "out");
    }
}

void Txc1::handleMessage(cMessage *msg)
{
    send(msg, "out");
}
```

Source: Documentation d'Omnet++ modifié par moi-même



Exemple de simulation omnet++

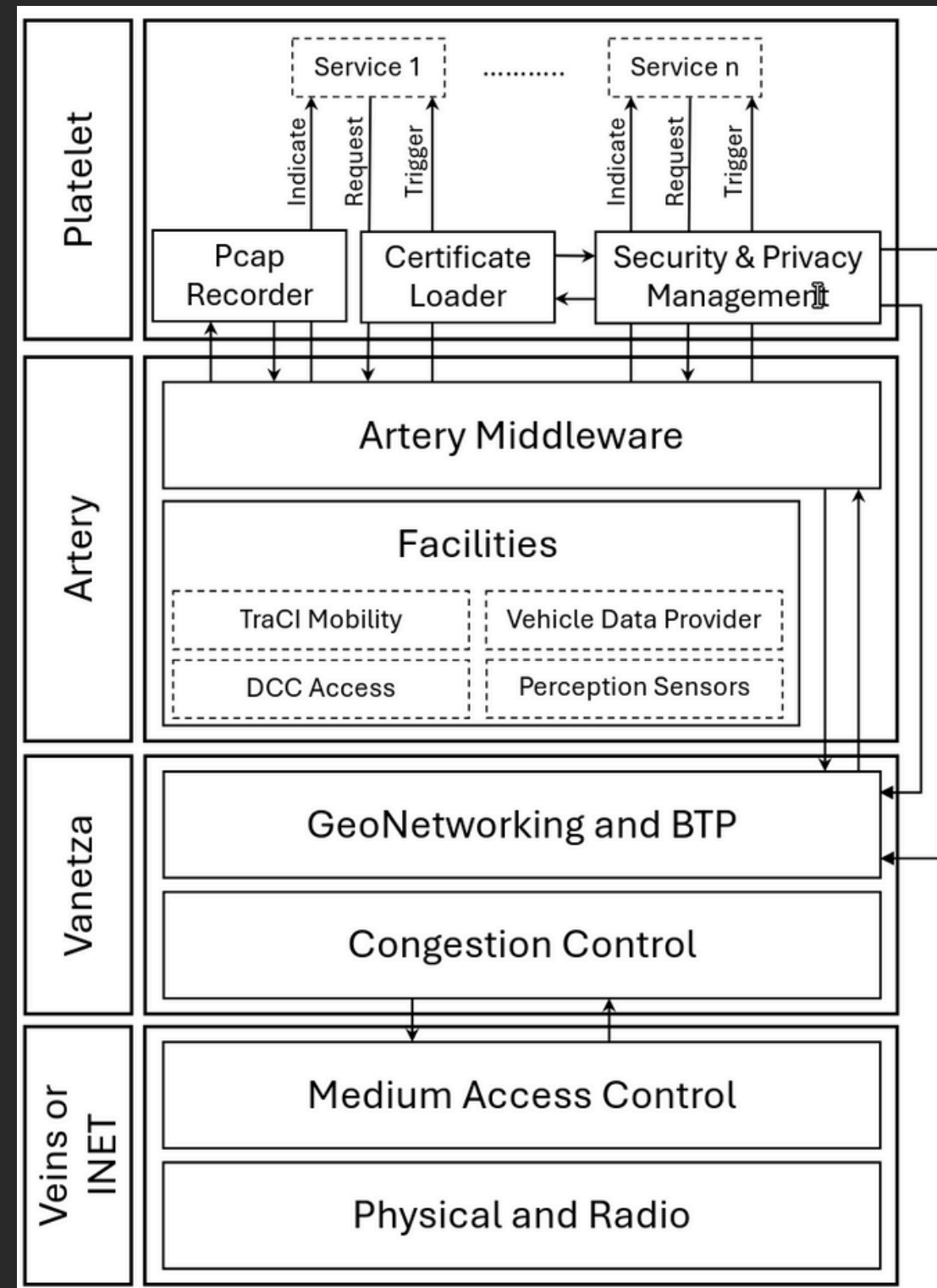
# Platelet

Premier simulateur à mettre en œuvre une gestion adéquate de la sécurité et de la confidentialité

Deux nouveaux composants:

- Un **pcap recorder** qui facilite la vérification d'un scénario complété
- Un **certificate loader** permettant aux véhicules d'envoyer des messages sécurisés

Une **application standalone** entièrement intégrée pour gérer les **scénarios sécurisés**



Platelet Architecture [6]

# StaticCertificateLoader

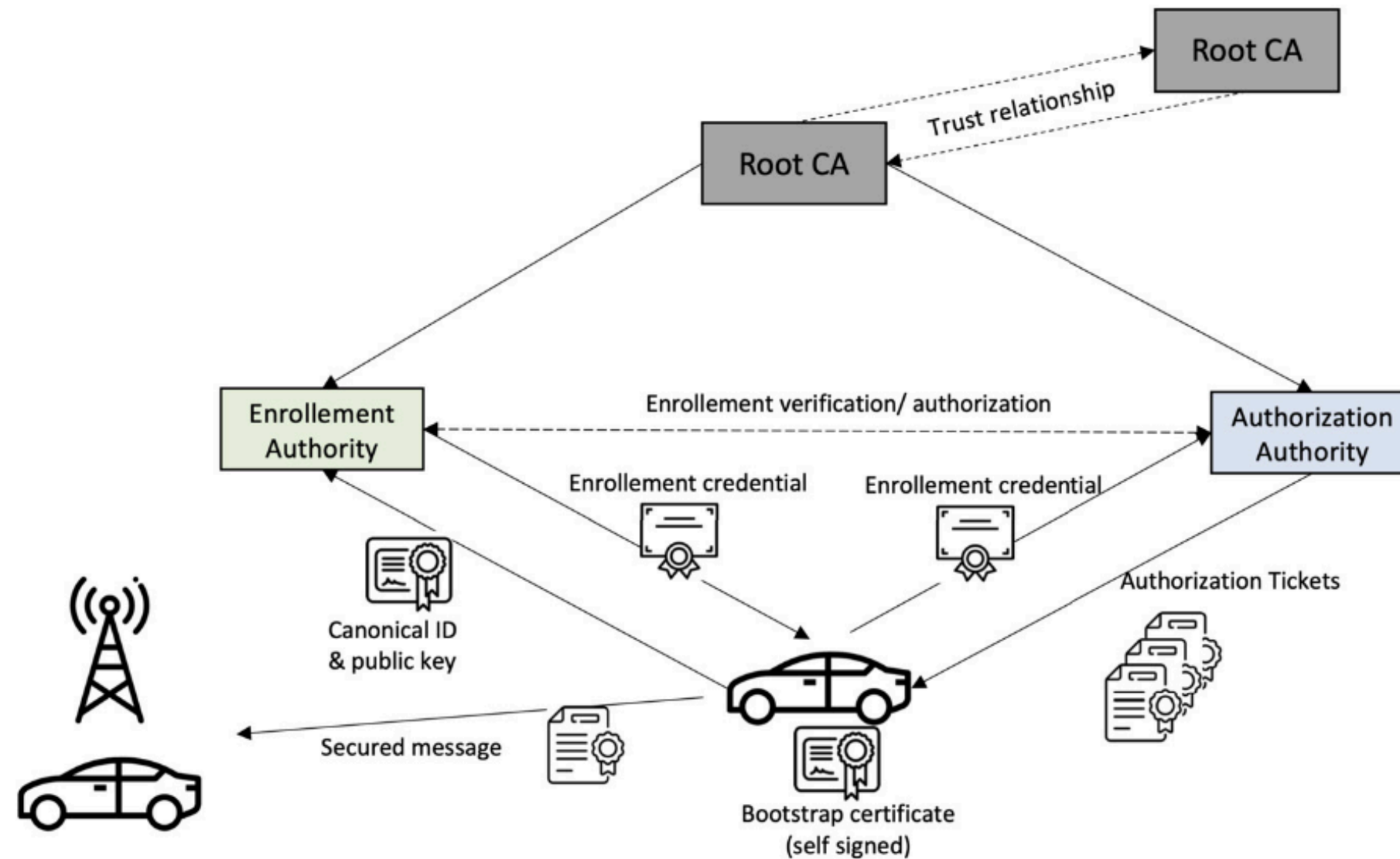
Artery n'a pas de module de chargement de certificat

Ce loader fonctionne en chargeant une pile de certificats **pré-générés** et en les distribuant pendant la simulation.

Il vérifie **l'authenticité** et **l'intégrité** du certificat lors de son chargement



# PKI, security and privacy management



Generic ETSI PKI architecture [12]

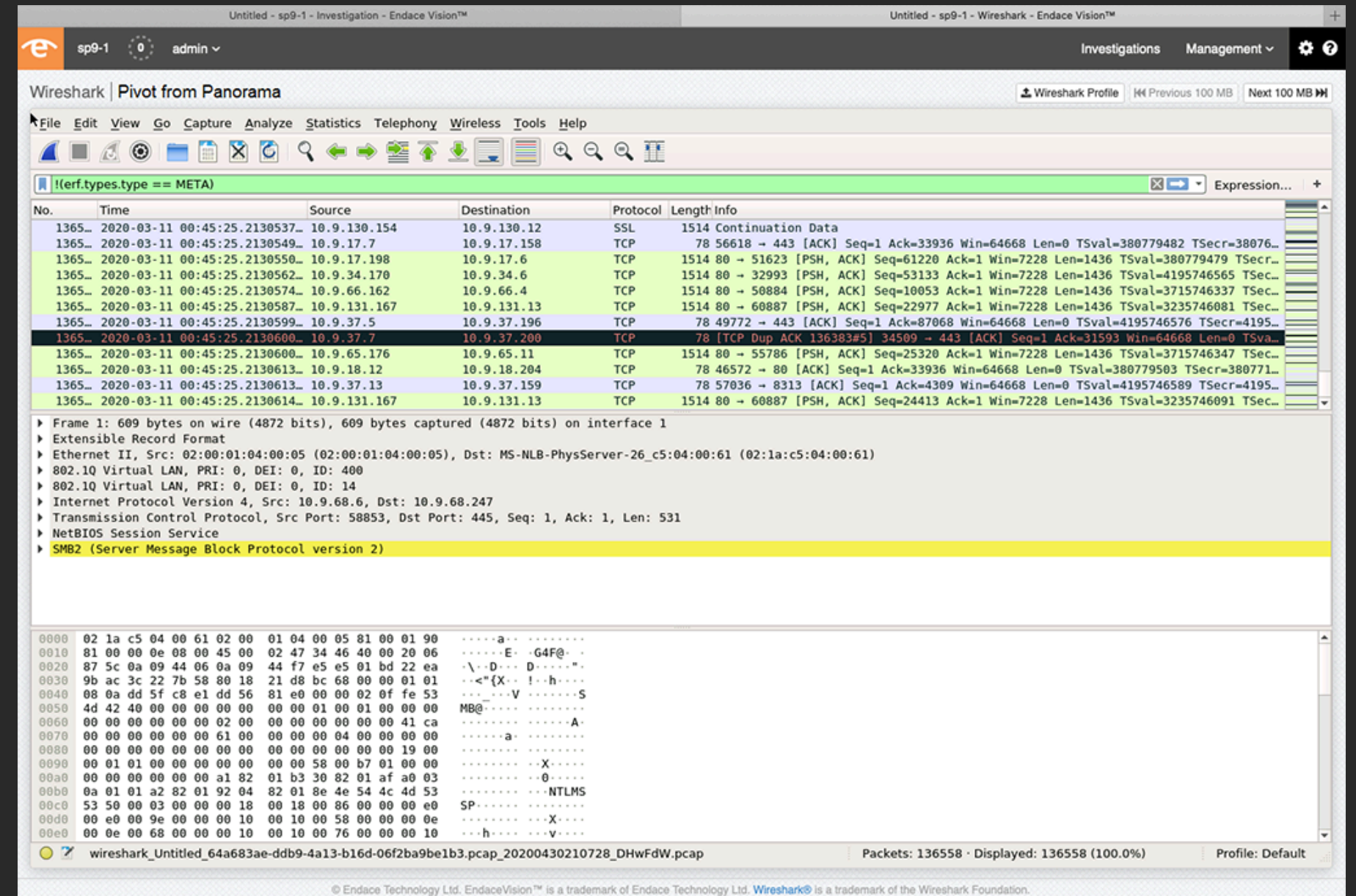


# PcapItsRecorder

Pcap: packet recording file format

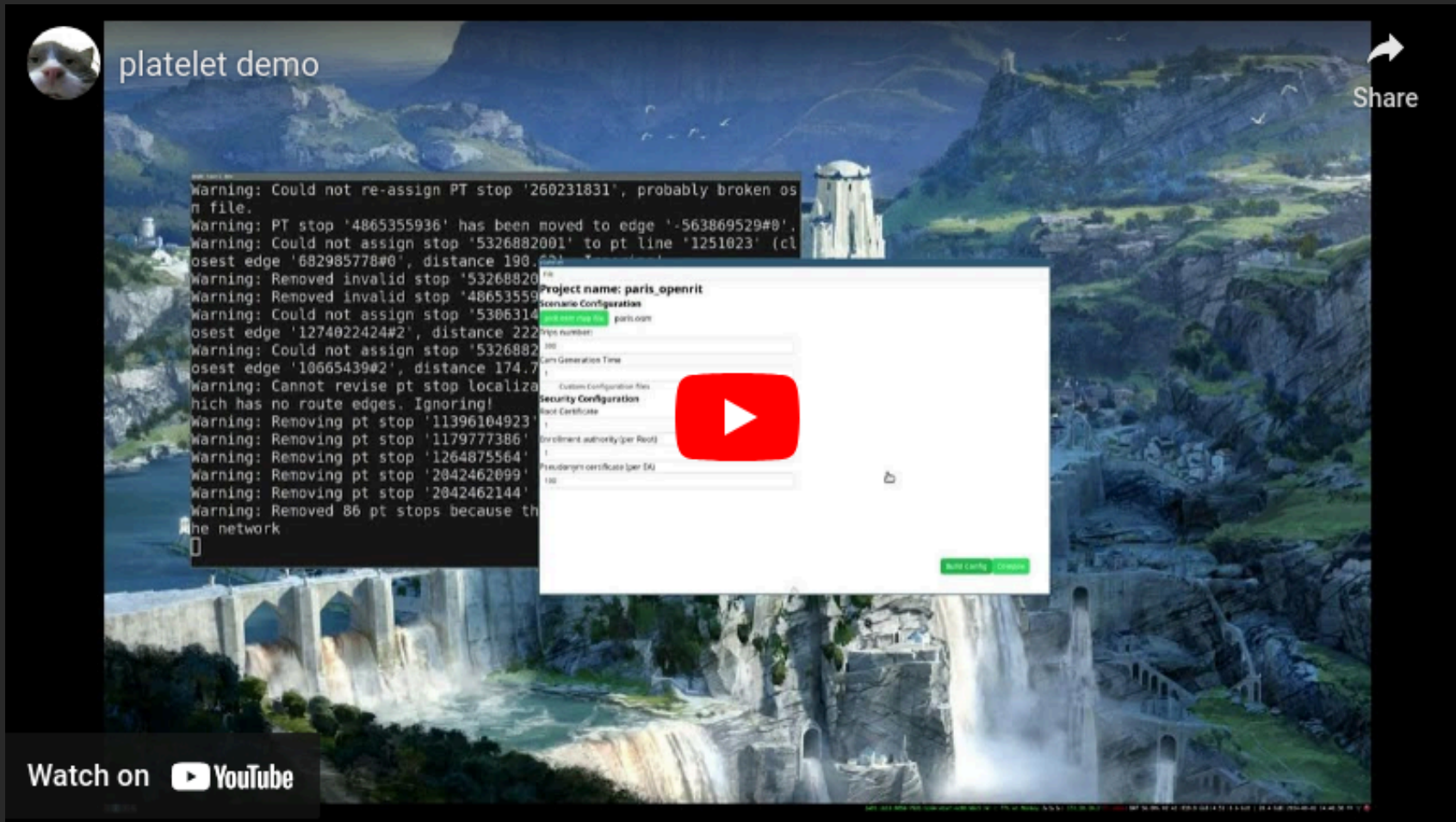
Il n'y avait **pas de recorder** auparavant dans le projet

Heureusement ! Un **packet** reader existe dans Wireshark.

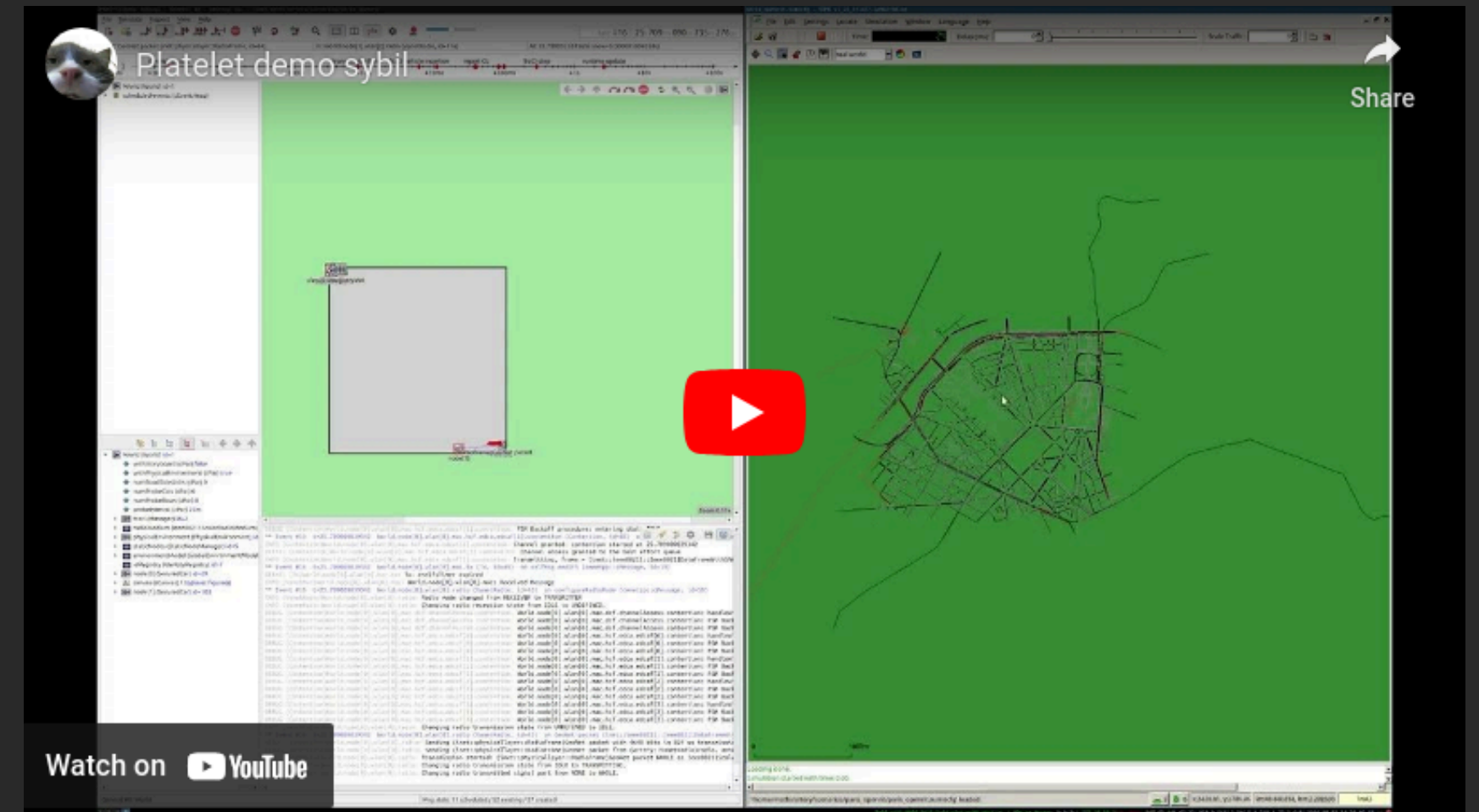


Wireshark interface

# Demo



<https://www.youtube.com/watch?v=Wu159mwxio>

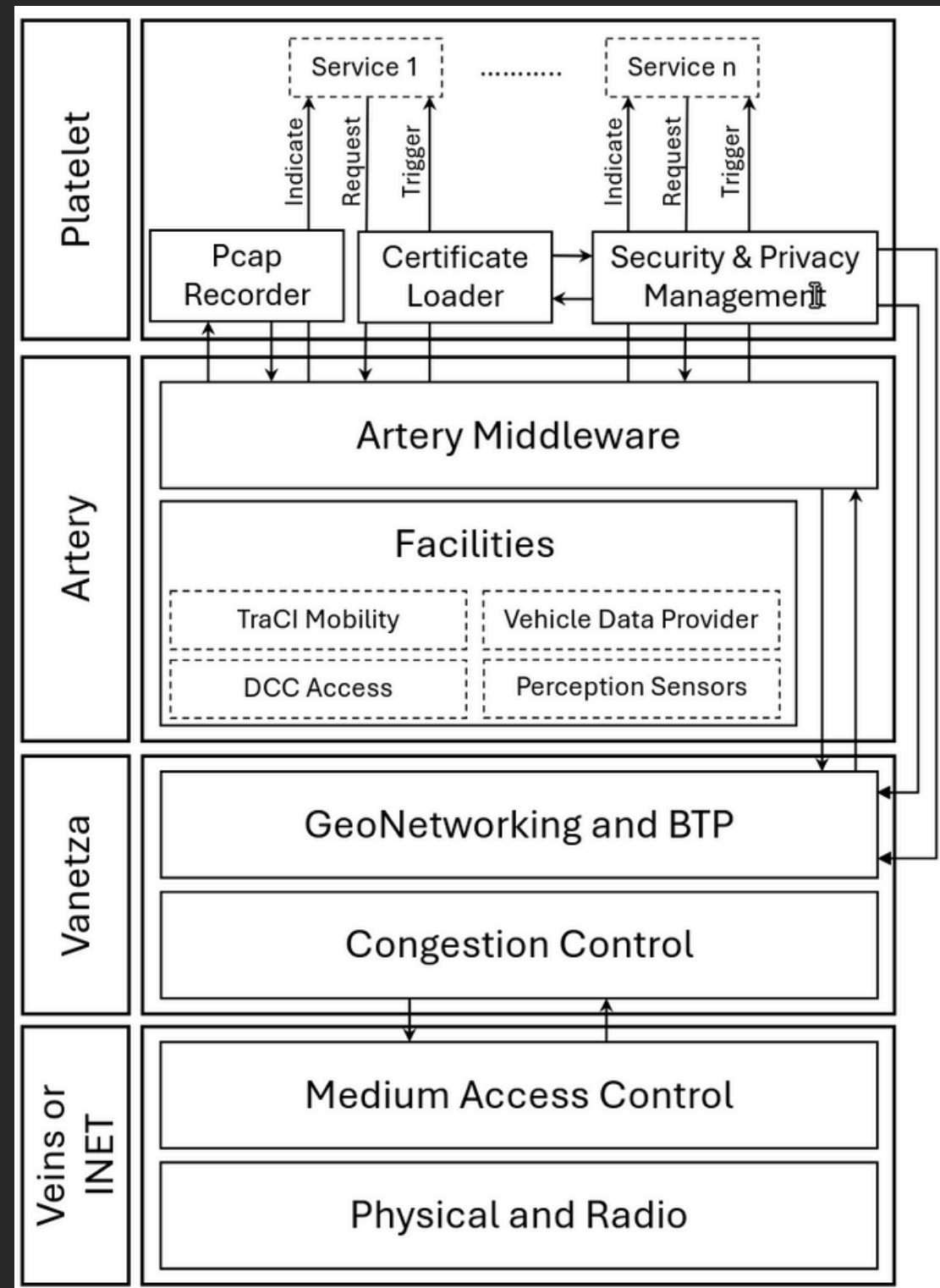


<https://www.youtube.com/watch?v=v9YIUluFh-o>

<https://gitlab.com/Matk3z/platelet>



# Pour conclure



Platelet Architecture [6]

Avant Platelet, il n'existait pas de simulateur ITS implémentant une couche de gestion de la **sécurité** et de la **confidentialité**.

Platelet permet la simulation de **scénarios sécurisés** et fournit des composants qui permettent de la **faciliter**.

Pour rendre la vie des chercheurs plus **simple**, on a **centralisé** tous les outils dans une **seule** application standalone.



# Bibliographie

- Mukesh Saini, Abdulhameed Alelaiwi, Abdulmotaleb El Saddik, 2015, How Close are We to Realizing a Pragmatic VANET Solution? A Meta-Survey
- R. Riebl, H. Gunther, Christian Facchi, L. Wolf, 2015, Artery: Extending Veins for VANET applications
- Badis H, Jean-Philippe M, Jonathan P, 2022, PKIs in C-ITS: Security functions, architectures and projects: A survey
- Agachai S, H.W. Ho, 2017, Smarter and more connected: Future intelligent transportation system
- Jonathan P, Florian S, Michael F and Frank K, 2014, Pseudonym Schemes in Vehicular Networks: A survey
- Mathias K, Badis H, Joaquin G, 2024, Platelet: Pioneering Security and Privacy Compliant Simulation for Intelligent Transportation Systems and V2X
- Artery Documentation, <http://artery.v2x-research.eu/>
- Omnet++ documentation, <https://omnetpp.org/documentation/>
- Vanetza documentation, <https://www.vanetza.org/>
- Institut européen des normes de télécommunications, ETSI TS 103 096
- Institut européen des normes de télécommunications, ETSI EN 302 637-2
- Institut européen des normes de télécommunications, ETSI TS 102 940