DIAS

SMART ADAPTIVE REMOTE DIAGNOSTIC ANTITAMPERING SYSTEMS

Solutions and demonstrators (WP4 & WP5)

25th October 2022, Brussels

HORIZON 2020
LC-MG-1-4-2018
Grant agreement ID: 814951

DIAS
Smart Adaptive Remote Diagnostic Antitampering Systems

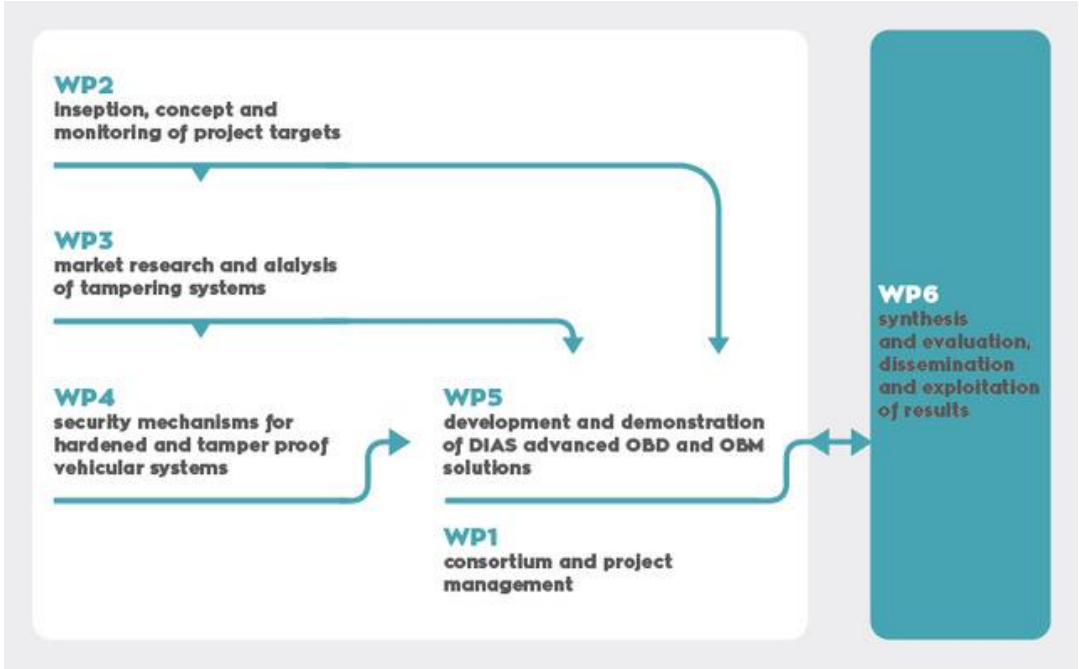
EUROPEAN COMMISSION
HORIZON 2020
LC-MG-1-4-2018
Grant agreement ID: 814951

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 814951.

Contents

- **Countermeasures based on market/system analysis**
  - Security solutions
  - Diagnostic Solutions

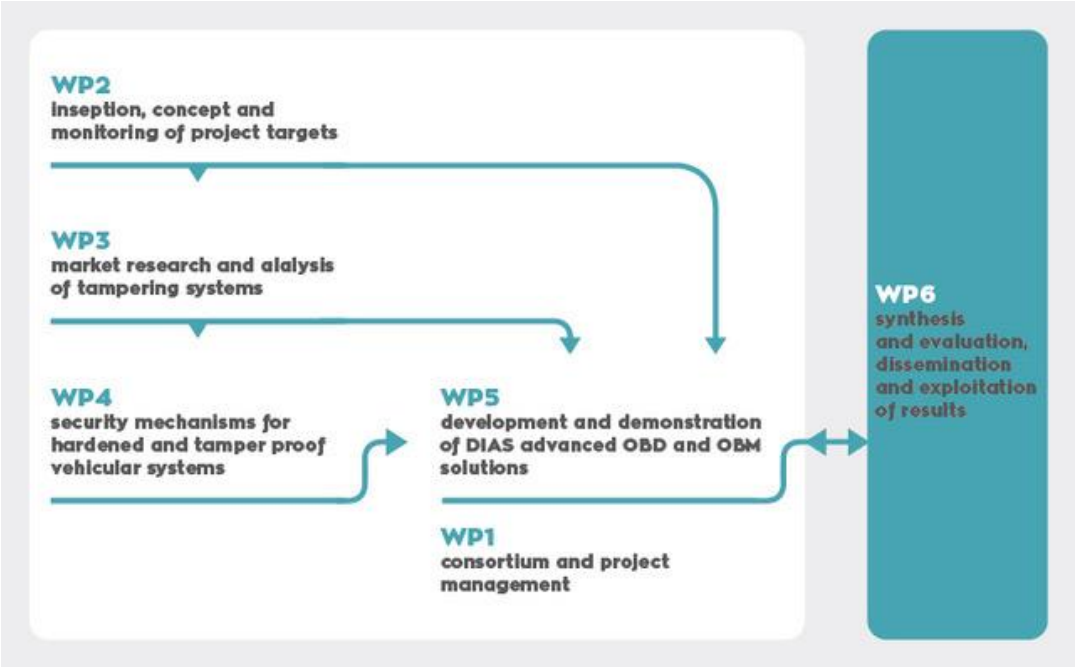
  --> Overall Diagnostic System
- **Remote Tampering Reporting**
  - Trusted data exchange Self Sovereign Identities
  - Digital Emission Certificates & Visualization
- **Summary**
- Q&A



Contents

- **Countermeasures based on market/system analysis**
  - Security solutions
  - Diagnostic Solutions

  --> Overall Diagnostic System
- **Remote Tampering Reporting**
  - Trusted data exchange Self Sovereign Identities
  - Digital Emission Certificates & Visualization
- **Summary**
- Q&A



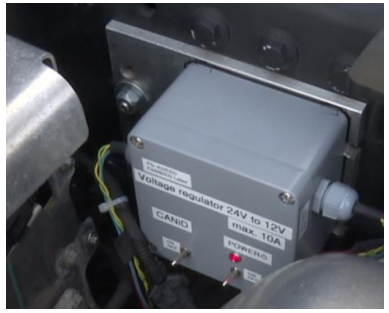
DIAS: Security and Diagnostic Solutions Demonstrators

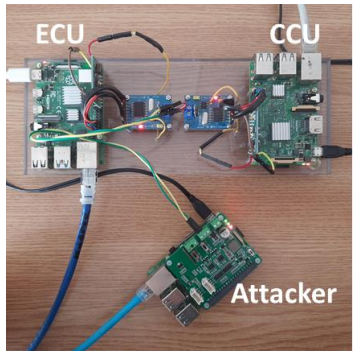
WP2
Inseption, concept and monitoring of project targets

WP3
market research and alalysis of tampering systems

WP4
security mechanisms for hardened and tamper proof vehicular systems

WP5
development and demonstration of DIAS advanced OBD and OBM solutions





Prototypes and Demonstrators for Testing and Validation

FMAX – Security Requirement/Solutions with MD1

Sl. No	Section	Generic Requirement	Status	RB Remarks
1	5.2	Secure boot must be provided	OK	RB Authenticated Boot (RTMD Once)can be a practical solution. Is it OK? RTMD performed Once is sufficient or Cyclic check needed? Authenticated Boot: Checks memory in parellel to Boot up process but does not prevent boot up until complete memory check is completed.
2	5.2	Secure software update	OK	RB Secure Flashing: CVC with ECC256 - NIST curves No Customer specific concept shall be implemented. Only CB Programming is open with CVC&ECC256 - NIST curves.
3	5.2	Code signing	OK	Same as Sl.No. 2 Only RB will be Signing.
4	5.2	Authentication of the communication partners	OK	Authentication for In vehicle communication: No procedure, successful Integrity check shall be assumed as authentication(as the sender has appropriate/valid key for generating MAC). Authentication for Tester communication: Secure Access procedure shall be in place with Symmetric Keys (AES 128) **Asymmetric Keys (ECC P256)** in offline mode shall be used. Access Protection shall be implemented for improved protection. Will FO Tester be available and support for hacking event or should we use our own? FO Tester will not be used.
5	5.2	Integrity of data transmitted on CAN	OK	Integrity Check shall be done with MAC verification (SecOC or SecOC Light based on the opposite node). Implemented for demonstration: Communication with CCU - SecOC (Implemented in intermediate; R.pi-based CCU) Communication with NOx sensor - SecOC Light (Implemented in Truck)
6	5.2	Secure key generation	OK (not on MD1 but on separate demonstrator)	Prototype NOx SCU & CCU with part specific, pre-shared key. ECU is capable of generating derived keys but KMS is customer specific. For demonstration: Separate demonstrator for KMS for CAN (FEV)
7	5.2	Secure key storage	OK	Sufficient Key storage is available from ECU releated to known security solution in DIAS
8	5.2	Secure key exchange	OK (not on MD1 but on separate demonstrator)	KMS is customer specific. For demonstration: Separate demonstrator for KMS for CAN (FEV)

DIAS specific security concept was agreed on between Bosch as implementing partner and WP4 lead.

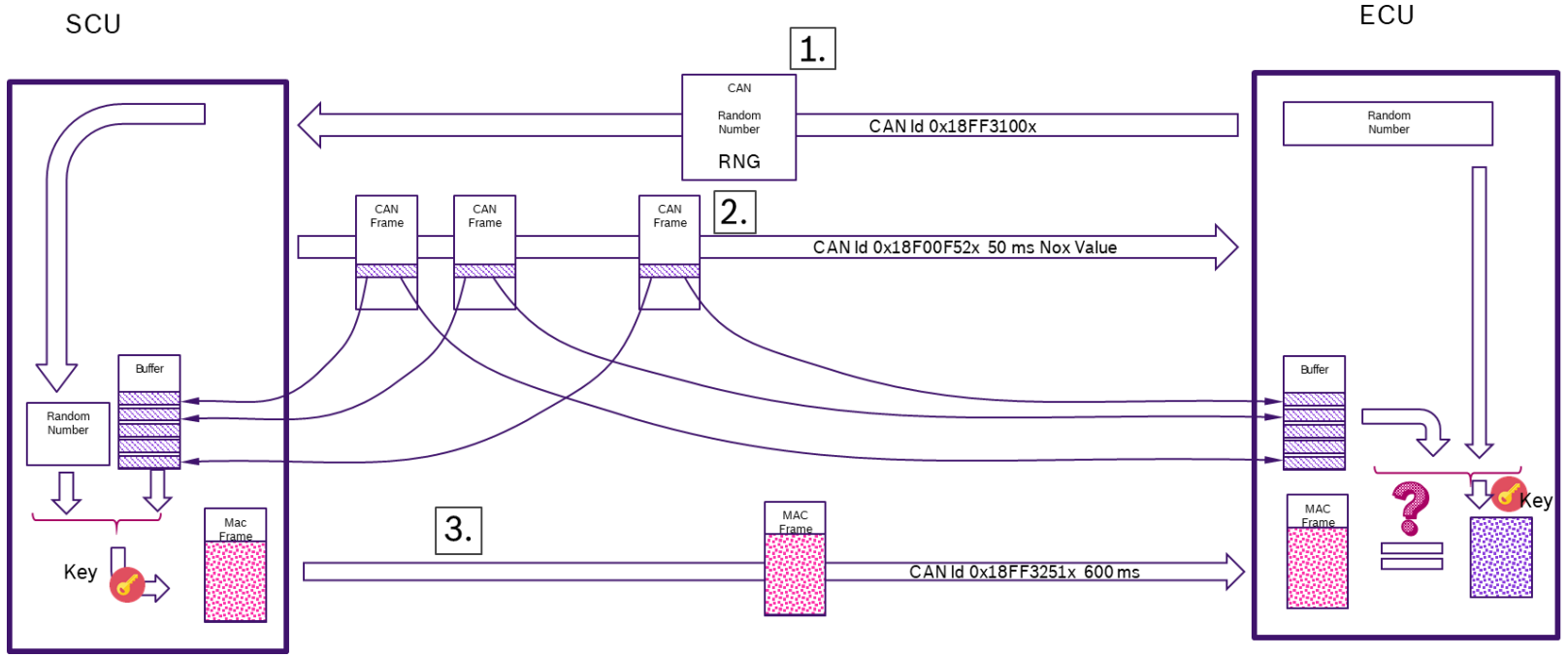
- Vehicle was converted from EDC17 to MD1
- Implementation acc. requirements from D4.1
- Huge efforts for calibration of driveability and emissions (cmp. new ECU project)

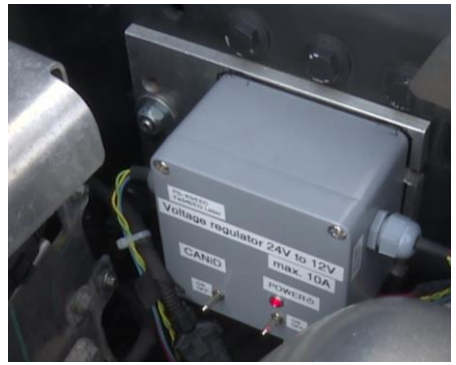
Recommended minimum requirement: "Secure flashing", as it is the attack path most commonly used.

1.Requirements are extracted from DIAS-D4.1-v1.0 (submitted).pdf

FMAX – Authenticated Sensor Communication

- An authentication concept was developed specifically for Small Control Units, not having enough resources to handle standardized Secure Onboard Communication (SecOC) → “SecOC light“

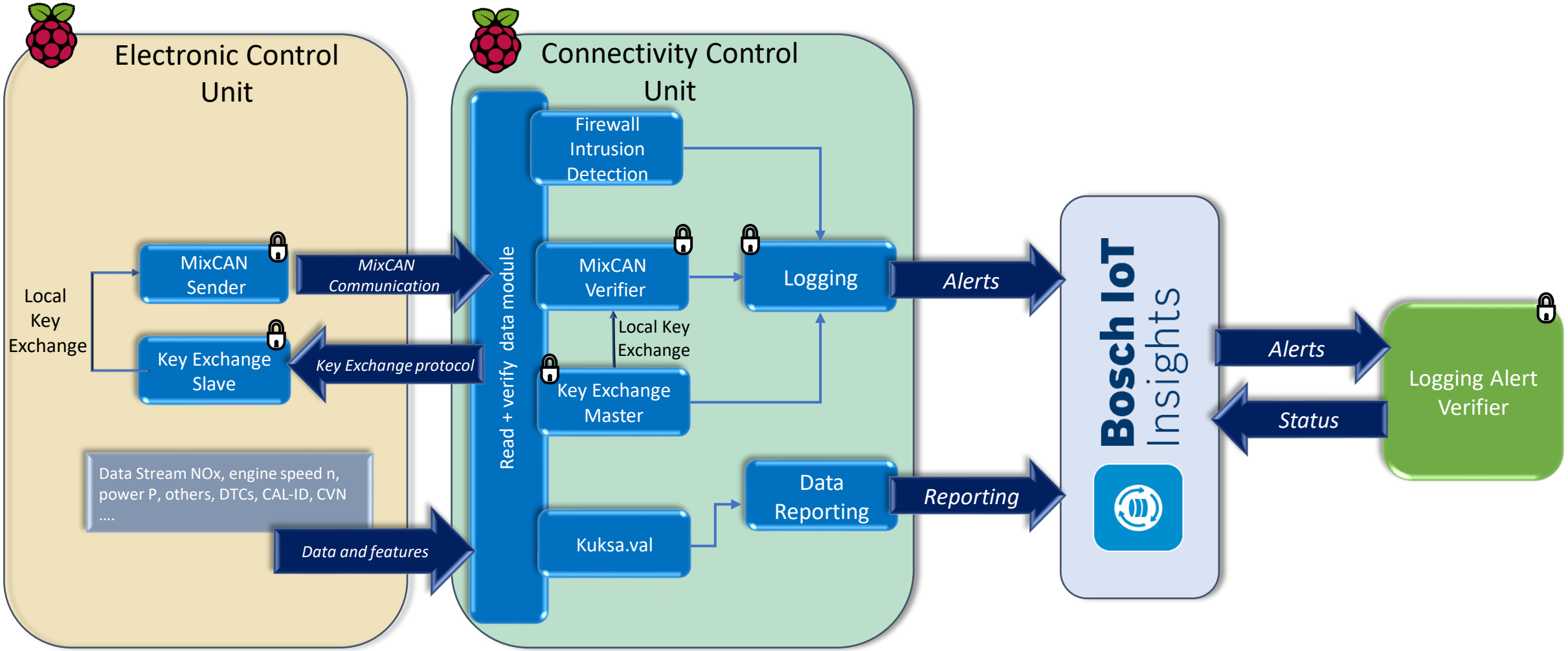




- Truck equipped with sensor sample featuring “SecOC light”
- Solution penetration tested by WP4 partners

Recommended minimum requirement: Continuous authentication for µC-based tailpipe exhaust sensors for direct emission sensing of regulated species acc. Emission regulation (e.g. tailpipe NOx and PM)

Testbed: In-Vehicle Security

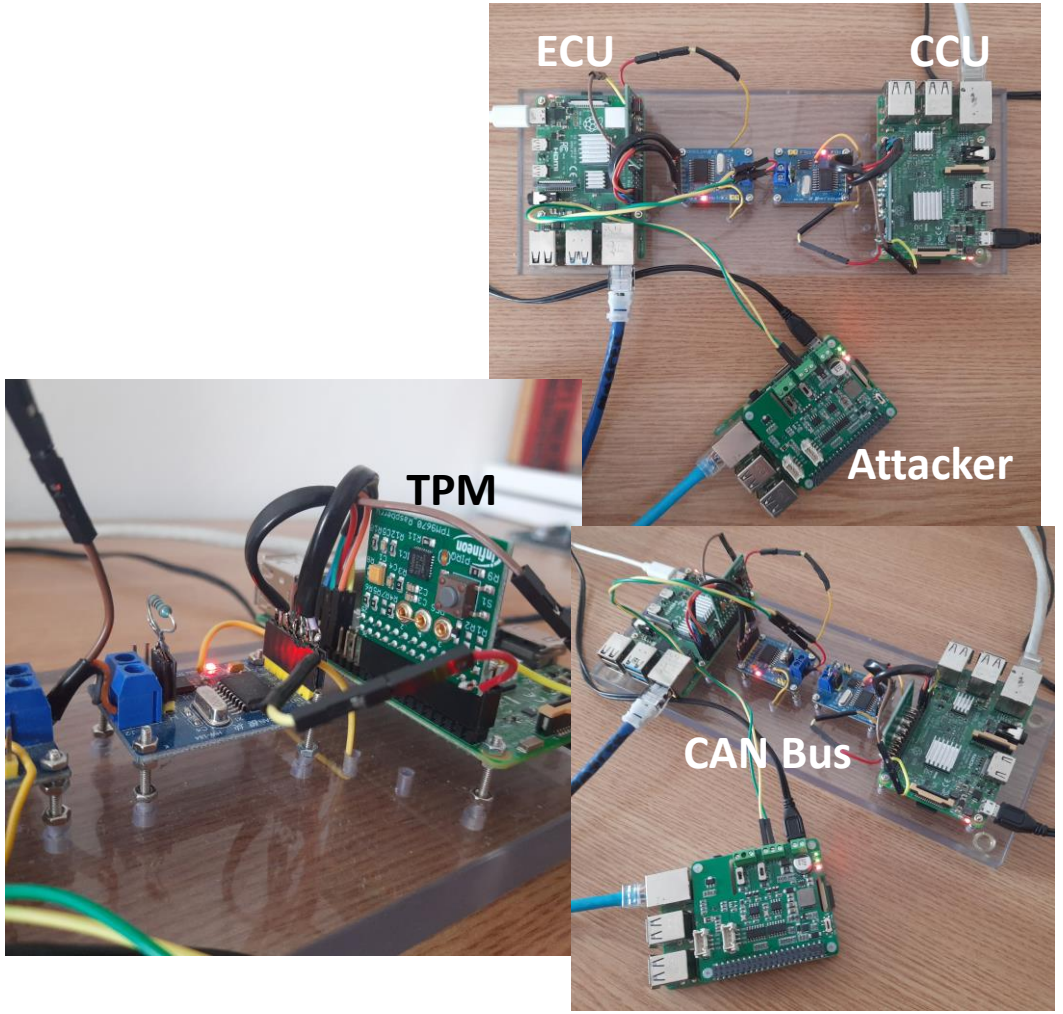


Testbed: DIAS Security Solutions

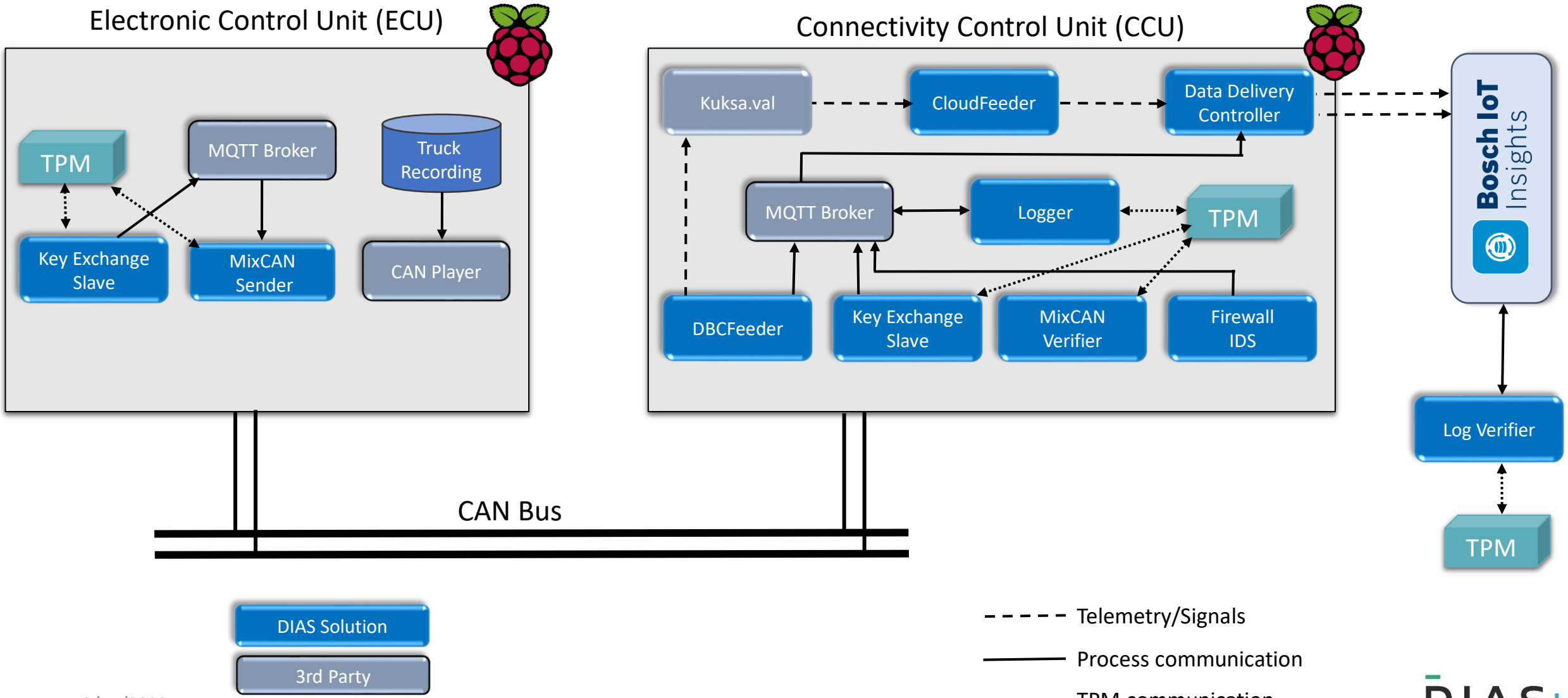
DIAS Solution	Requirements	Description
Secure Key Generation and Storage Using Trusted Platform Module (TPM)	• Key storage on ECU/CCU • Key distribution over CAN	• Asymmetric long-term key • Symmetric short-term keys • Key Storage using TPM sealing and hierarchies
MixCAN Data Authentication	• Data authentication of CAN frames	• Authentication of multiple aggregated CAN frames using Bloom Filters
Stateful Firewall	• xCU and CAN network protection against known CAN attacks	• Restricts known un-authorized CAN network traffic coming from one CAN network to another
Intrusion Detection System	• CAN frame inspection	• Performs deep packet inspection at CAN frame data level. The IDS is able to detect known sequences of tampered frames, and deviations from expected frame cycle times
Secure Logging + Logging Verifier Using Trusted Platform Module	• Signing and reporting events • Generating verifiable alerts	• Signs events using the TPM digital signature engine • Reports and attests alerts using Platform Configuration Registers

Testbed: Hardware Setup

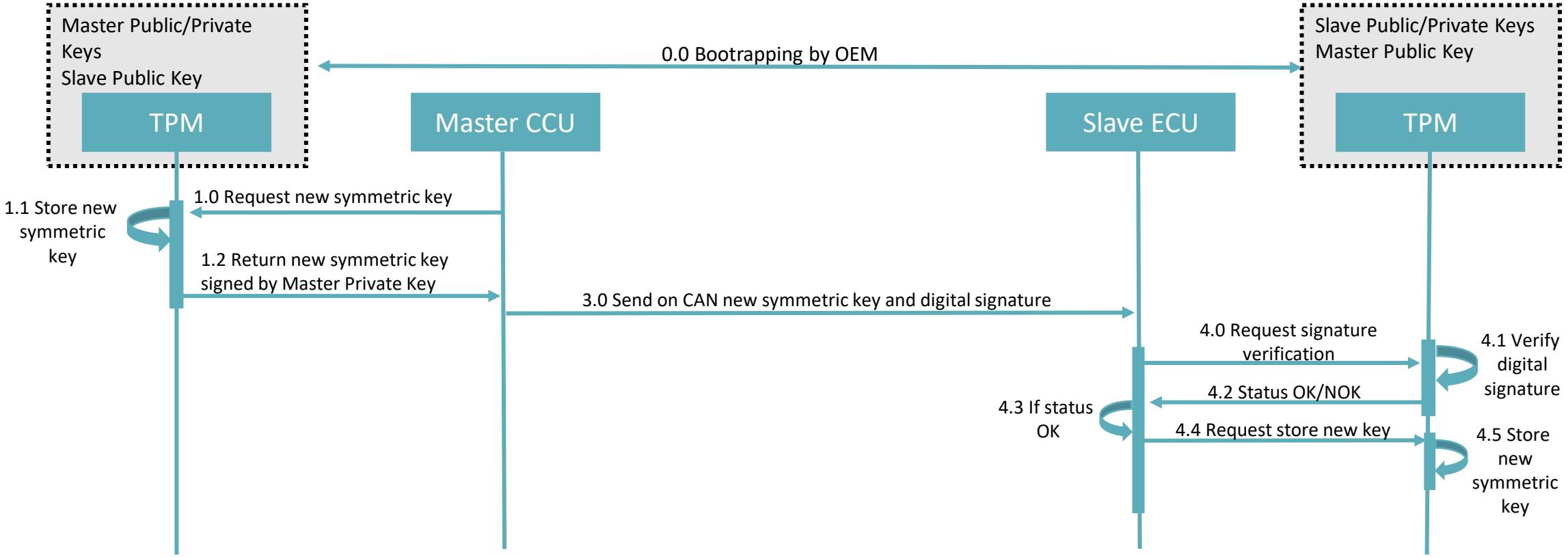
- In-Vehicle:
  - ECU/CCU:
    - Raspberry Pi's 3 model B or 4
    - Iridium 9670 Optiga IoT Security, TCG TPM 2.0
    - MCP2515 CAN Controllers with TJA1050 CAN Transceivers
  - Attacker:
    - Raspberry Pi 3 model B
    - Seeed 2-Channel CAN-BUS(FD) Shield
- Cloud:
  - Bosch IoT Insights
  - Virtual environment



Testbed: Implementation



Long-Term Key Generation and Storage Using TPM

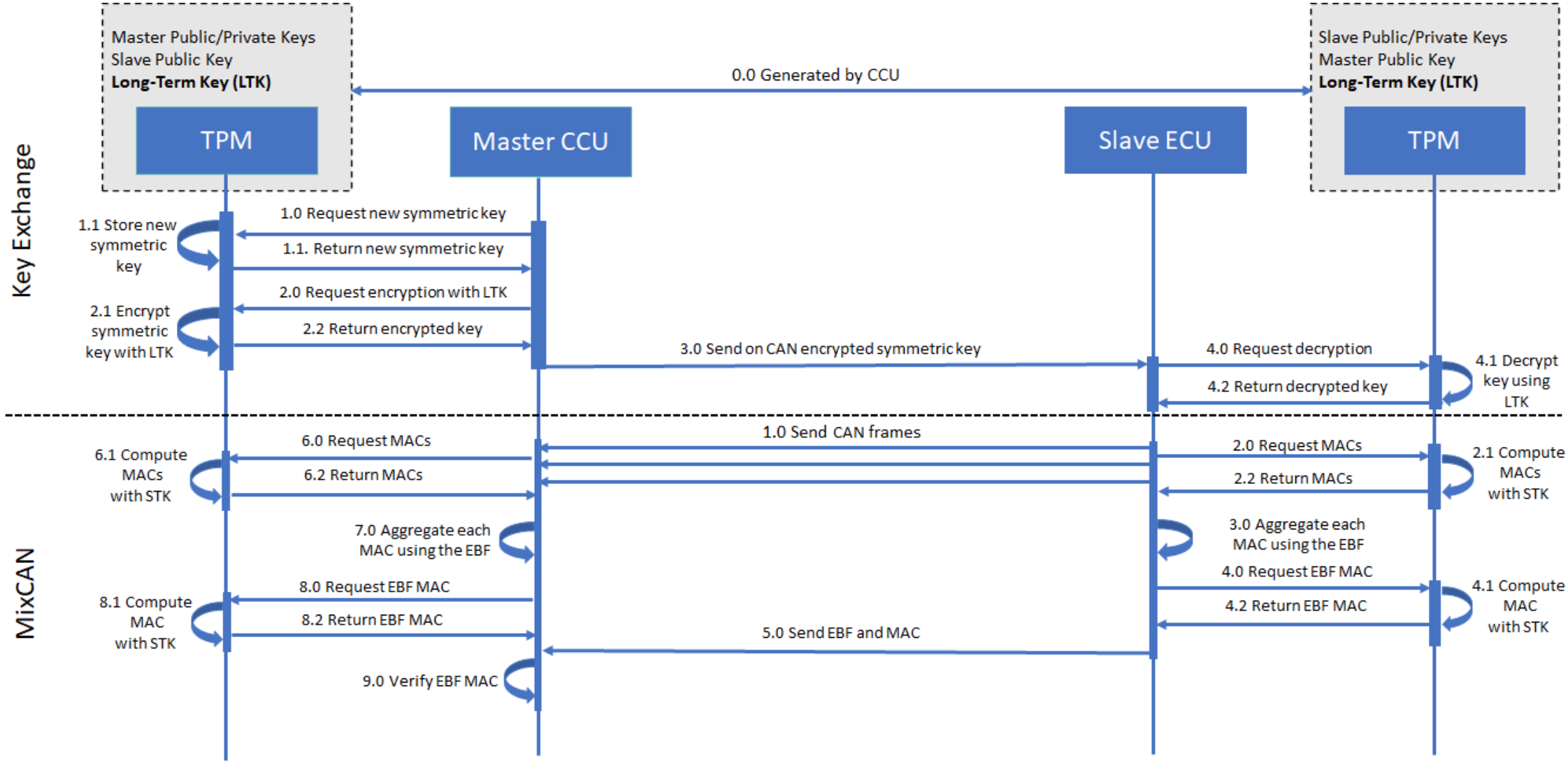


- Asymmetric key distribution protocol used to generate Long Term Keys (LTKs)
- LTKs are derived from a set of bootstrapped asymmetric keys
- Private keys are stored securely using Trusted Platform Module Sealing

MixCAN Data Authentication

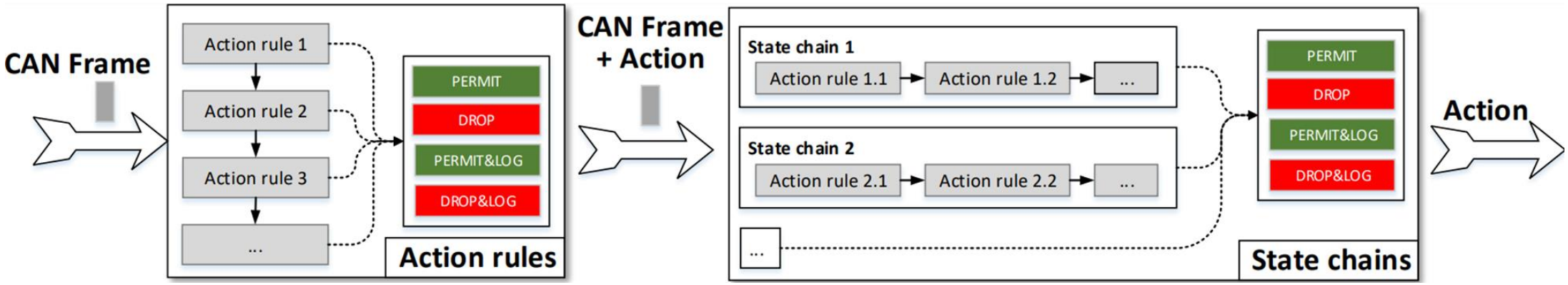
- Leverages a LTK to distribute periodically symmetric Short-Term Keys (STKs)
- STKs are further used for data authentication
- Proposed MIXCAN protocol is an alternative to other secure CAN protocols
- Enables xCU/CCUs to compute a mix of authentication tags for a set of frames where each tag can be verified independently
- Uses symmetric cryptography to compute authentication tags
- Uses Encrypted Bloom Filters (EBF) to aggregated tags
- Has low bus impact, the mix of authentication tags fits in one CAN frame
- Data authentication failure events are logged internally and reported on request

Short-Term Key Generation and Data Authentication

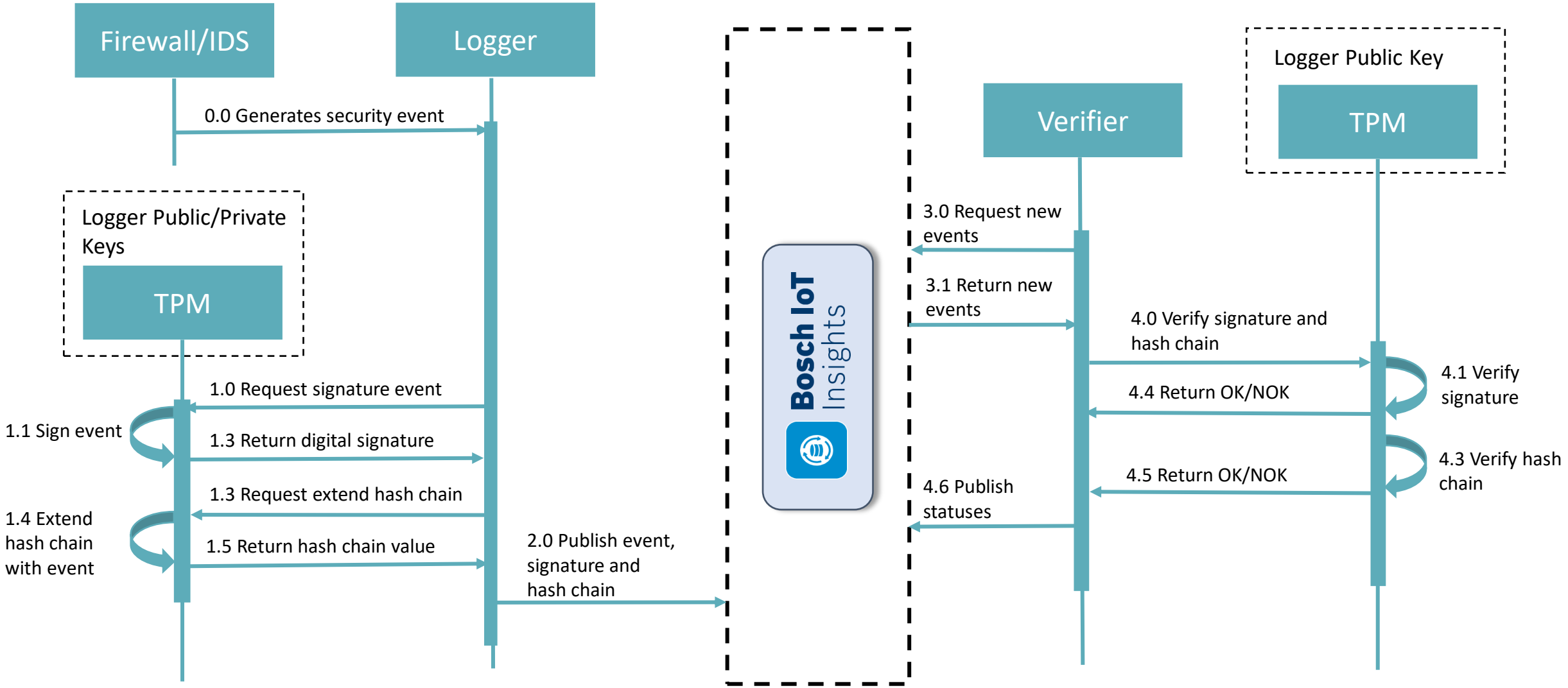


Statefull Firewall and Intrusion Detection System

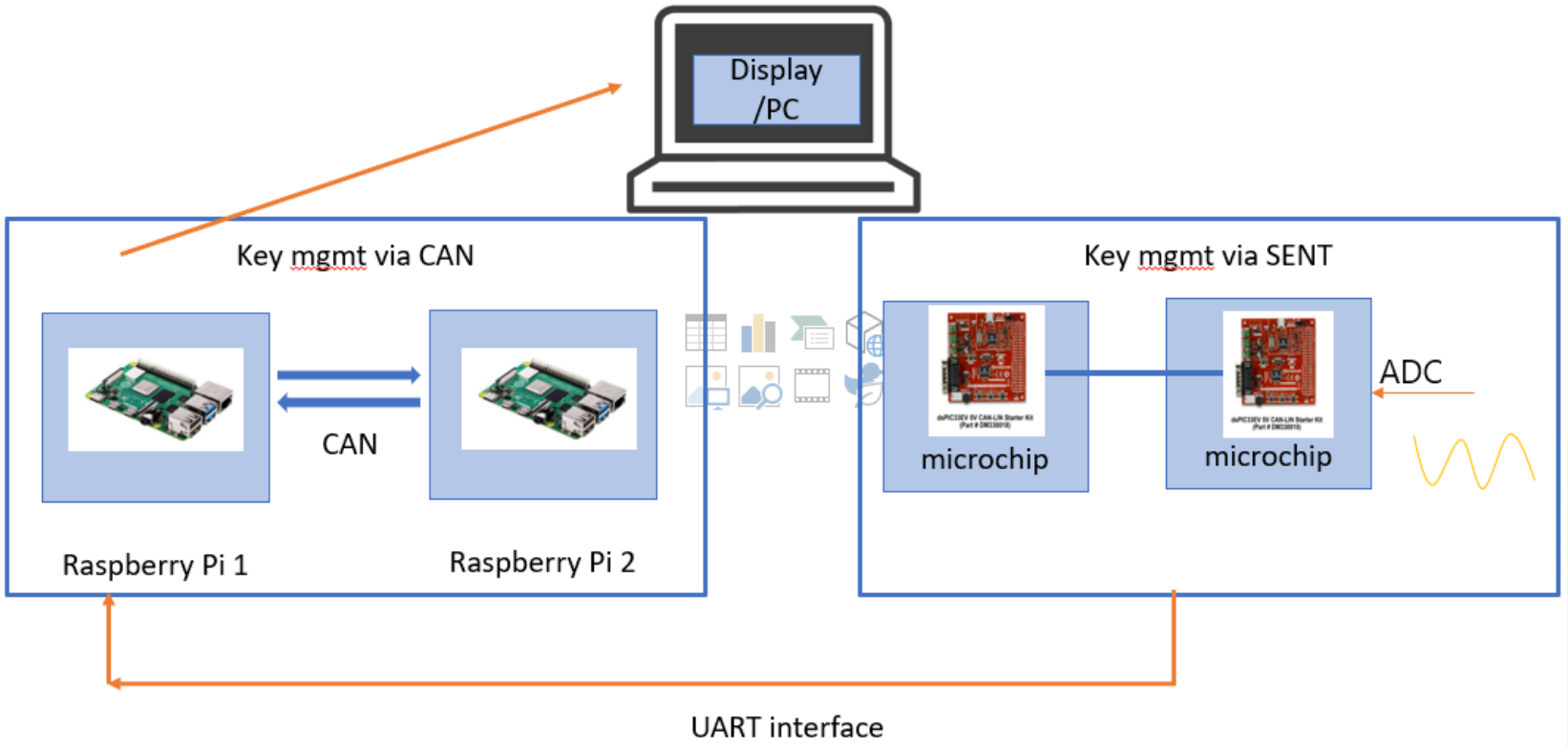
- The Statefull Firewall monitors CAN frames based on:
  - The CAN Identifier frame field
  - CAN frame transmission frequency
- The Intrusion Detection System inspects CAN frames based on:
  - The CAN Data frame field
  - Byte level values and range of values
  - Logical operations between CAN Data bytes
- Alerts are generated if:
  - A known pattern/sequence of frames is detected
  - Transmission frequency of frames is disturbed over/under normal values



Secure Logging Using TPM

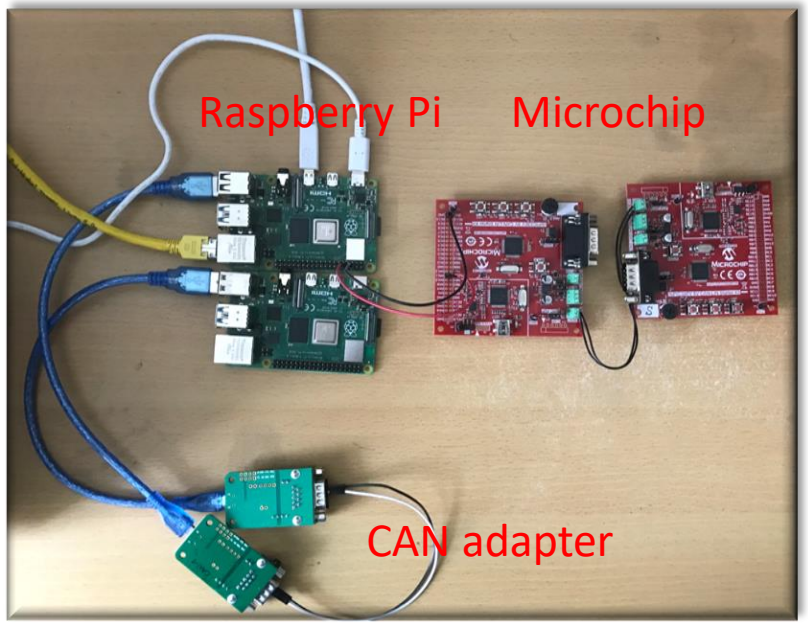


Demonstrator FEV (1/4)



Demonstrator setup:

- **Two Raspberry Pis** to demonstrate the xCUs
- **Two CAN adapters** for CAN communication
- **Two Microchips** to demonstrate the transmitter/receiver of SENT



The FEV desktop demonstrator includes two parts:

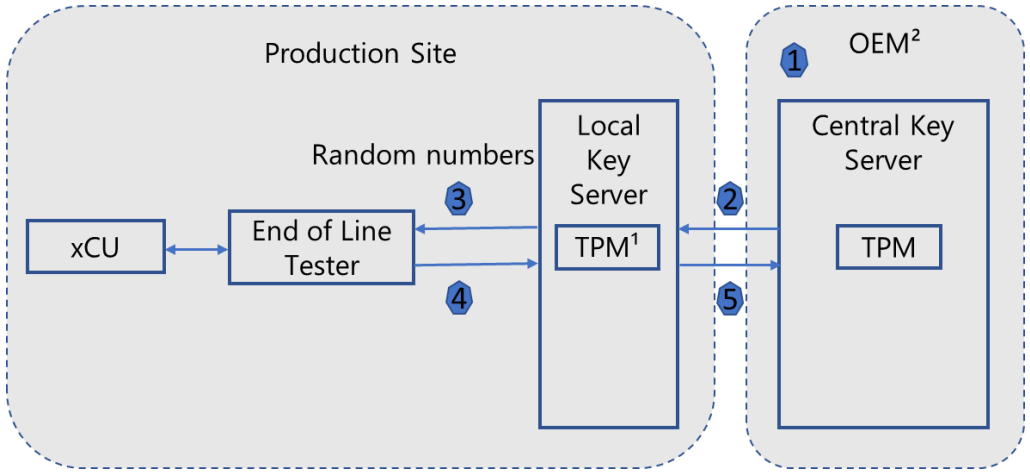
- A key management scheme for xCUs of different suppliers using CAN
- Key exchange and secure onboard communication of SENT

Key Management Schemes for CAN and SENT (2/4)

- A key management scheme for xCUs of different suppliers using CAN
  - Requirement of **secure key exchange supported on the end nodes of CAN bus**
    - **Elliptic curve Diffie-Hellman (ECDH) key exchange** is used for its moderate key size but strong security strength
  - The scheme considers that the xCUs are produced by **different suppliers**, also the lifecycle of xCUs requires **key update**
    - Use case 1: **during production**
    - Use case 2: **in workshop**
- Key exchange and secure onboard communication of SENT
  - Novel solution for **two layers (internet layer and hardware layer) secure communication**
    - Requirement of **secure communication of SENT** from initial risk analysis of DIAS
    - SENT is **unidirectional protocol** and the sensors are **resource constrained**
  - According to the market analysis the tampering devices using SENT interface is not found, also the potential threat is lower than the initial threat analysis. The proposed scheme is **currently not suitable for serial production of SENT sensors**.
  - The key exchange scheme **can be used for other applications** where lightweight cryptography is required due to limitation of the hardware

A Key Management Scheme for xCUs of Different Suppliers (3/4)

- Use case 1: during production

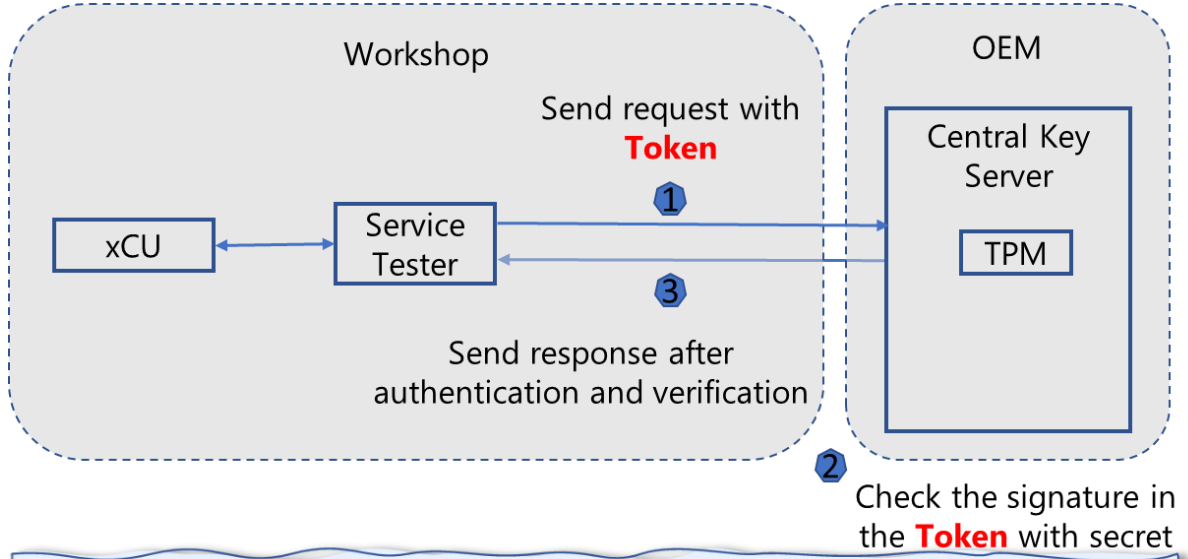


1. TPM: Trusted Platform Module; OEM: Original Equipment Manufacture

- Steps:

1. Generate sets of the pre-shared random numbers
2. Distribute the pre-shared random numbers to different local key servers as requested by the supplier production sites
3. Flash the pre-shared random numbers into the xCUs during production
4. Log which random numbers have been introduced to each xCU
5. Send the log files back to the central key server

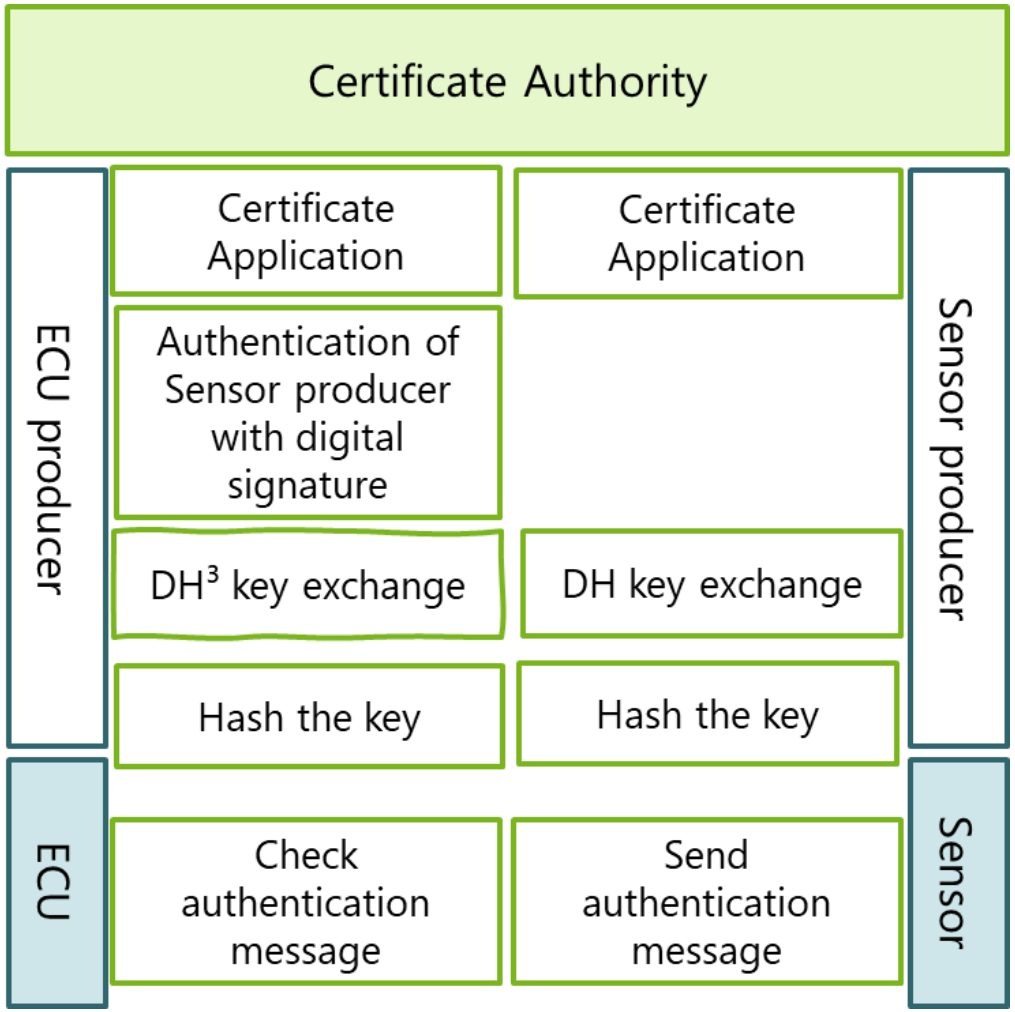
- Use case 2: in workshop



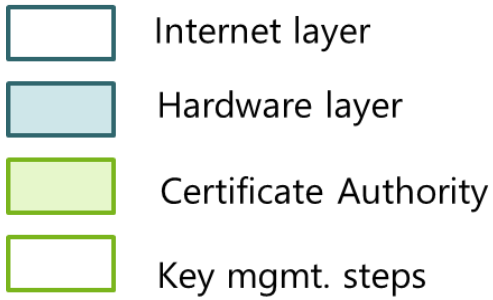
- Steps:

1. Send the request to the central key server for updating the random numbers with a valid token
2. Verify the signature
3. Send a response with new random numbers to the service tester when the authentication is successful

Key Exchange and Secure Onboard Communication of SENT (4/4)



- Architecture
  - The top layer of this architecture is CA[1]
  - ECU[2] and sensor producer request certificates at CA
  - The certificates are used for authentication at the beginning of key exchange
  - The final key is saved on the device
  - At the bottom is the secure on-board communication
  - PRESENT is used to encrypt/decrypt the authentication information



1. CA: Certificate Authority; 2. ECU: Engine Control Unit; 3. DH: Diffie-Hellman

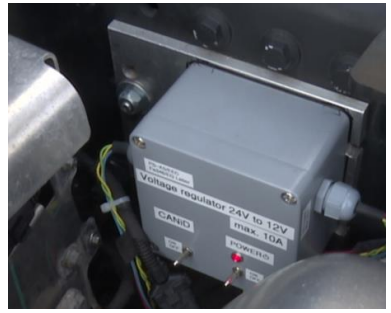
DIAS: Security and Diagnostic Solutions Demonstrators

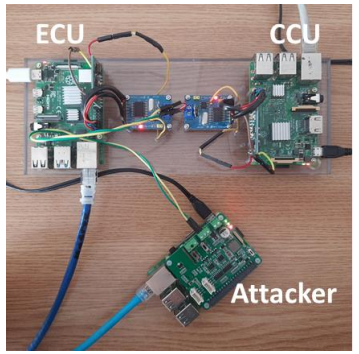
WP2
Inseption, concept and monitoring of project targets

WP3
market research and alalysis of tampering systems

WP4
security mechanisms for hardened and tamper proof vehicular systems

WP5
development and demonstration of DIAS advanced OBD and OBM solutions





Prototypes and Demonstrators for Testing and Validation

Dedicated detection functions

- Emulators for tampering of SCR* were found to use common/similar attacks.
- Dedicated functions were developed to detect these specific attacks.
- These functions have been implemented in the SW of the updated ECU** of our demonstrator truck.
- **All known SCR emulators would have been robustly detected by at least one of the newly developed function.**

Subset of functions was implemented and validated in FMAX demonstrator vehicle:

Emulator Attack	Diagnostic approach
Periodical erasing of Fault Codes prevents detected malfunctions from being confirmed and triggering MIL and inducement	A new DTC is reported when the following condition is fulfilled: Number of driving cycles per FCM clear command < Threshold1 **&** ((Mileage per FCM clear commands < Thr.2) or (time engine running per FCM clear commands < Thr.3))
Deactivation of DEF-Dosing results in constant DEF level and no refilling events	Expected urea consumption is calculated with a rather simple model based on the Diesel fuel consumption. DTC is reported, when the modelled urea consumption exceeds the DEF tank capacity and no refill is detected.
DEF pump disconnected → Pressure is (poorly) emulated based on pump actuation	Improved hydraulic plausibility check, considering DEF injections

Recommended minimum requirement

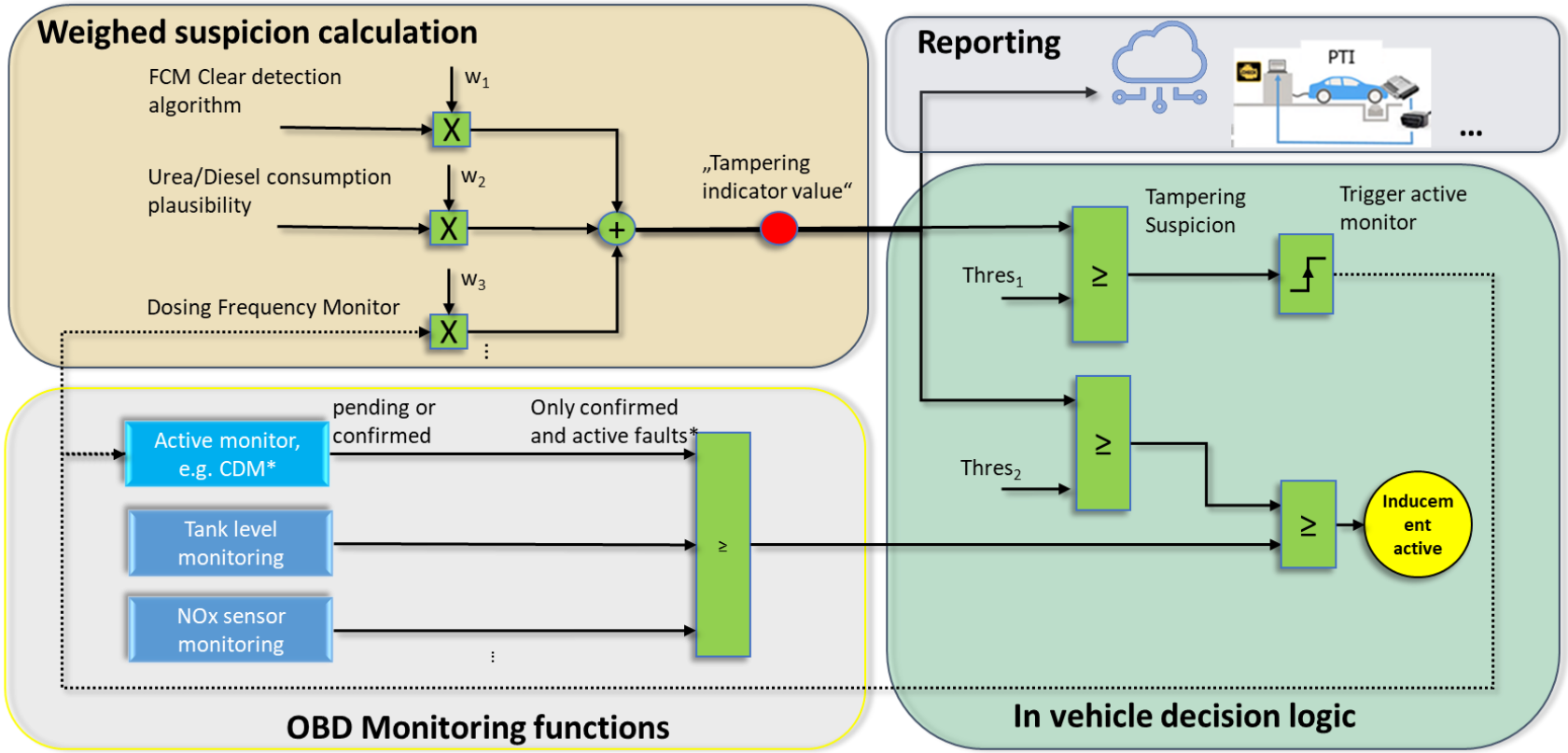
* SCR Selective Catalytic Reduction
** ECU Engine Control Unit

FMAX Diagnostic Solutions “Level1”

A tampering coordinator collects information from tampering detection functions and calculates a “tampering probability”/tampering indicator value (cmp. deliverable D5.1).

Input is modular (e.g. “advanced functions” can be added → see following slides).

Output can be used for various use cases (e.g. precondition for remote data, pre-cursor for road side checks etc.)

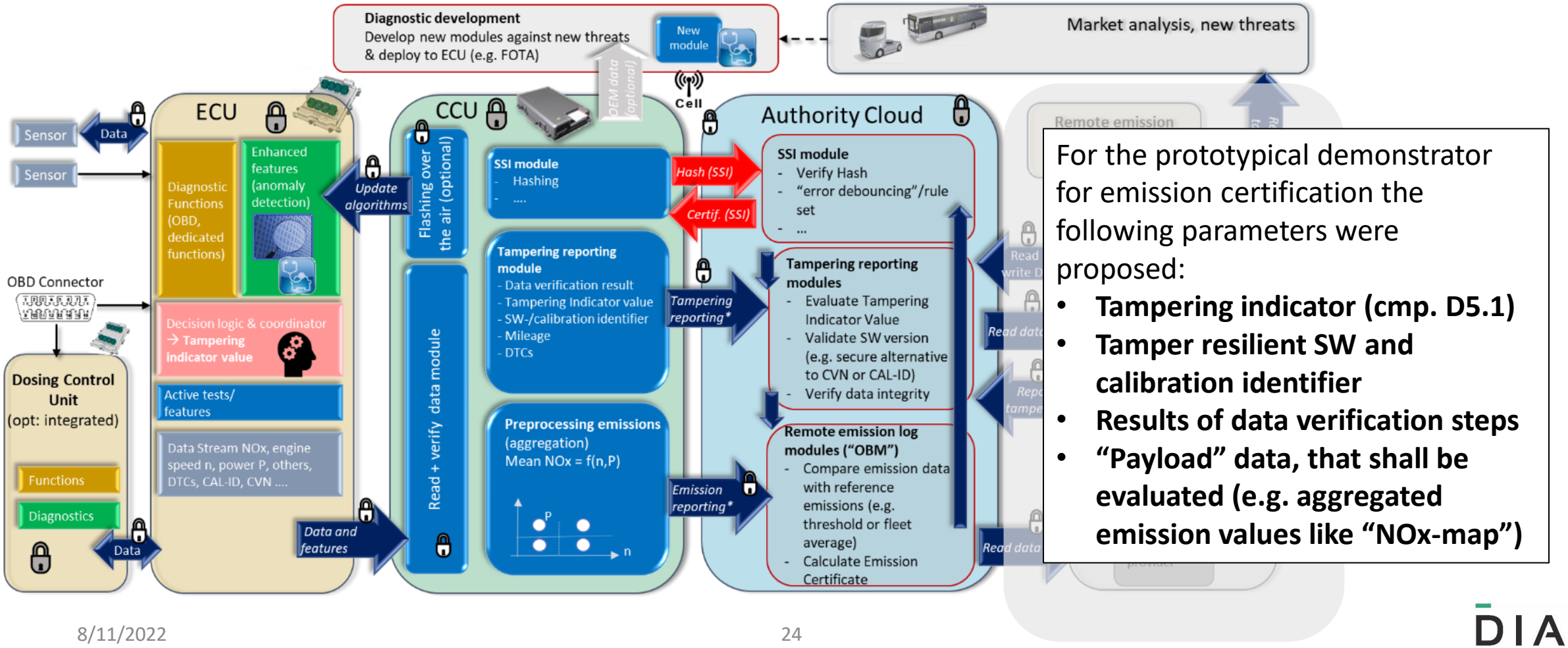


Recommended minimum requirement: Tampering indication

* **C**onsumption **D**eviation **M**onitoring

Overall Diagnostic System (ODS)

A connected system comprising complementary security and diagnostic solutions was updated after the developments of intra-vehicular measures concluded with the assumption, that the tampering devices identified in DIAS work packages WP2 and WP3 can either be prevented from working or detected (cmp. Deliverable D5.2).



For the prototypical demonstrator for emission certification the following parameters were proposed:

- **Tampering indicator (cmp. D5.1)**
- **Tamper resilient SW and calibration identifier**
- **Results of data verification steps**
- **"Payload" data, that shall be evaluated (e.g. aggregated emission values like "NOx-map")**

Need a break?

Advanced detection system against unknown tampering

- Objectives
  - successful detection, regardless if the manipulation attempt has been foreseen or not
  - preserve the integrity of the existing system
  - combine different detection methodologies
  - open path for further improvement of the detection algorithms
  - develop a prototype of the system in MATLAB environment
- Approach
  - extensive analysis of the signals collected from the real truck
  - model identification from historical values not susceptible to manipulation
  - measured signals are continuously monitored and compared with predicted values
  - propose a diverse palette of detectors and combine their outputs
  - analyze the performance of the proposed complex detection system

DIAS

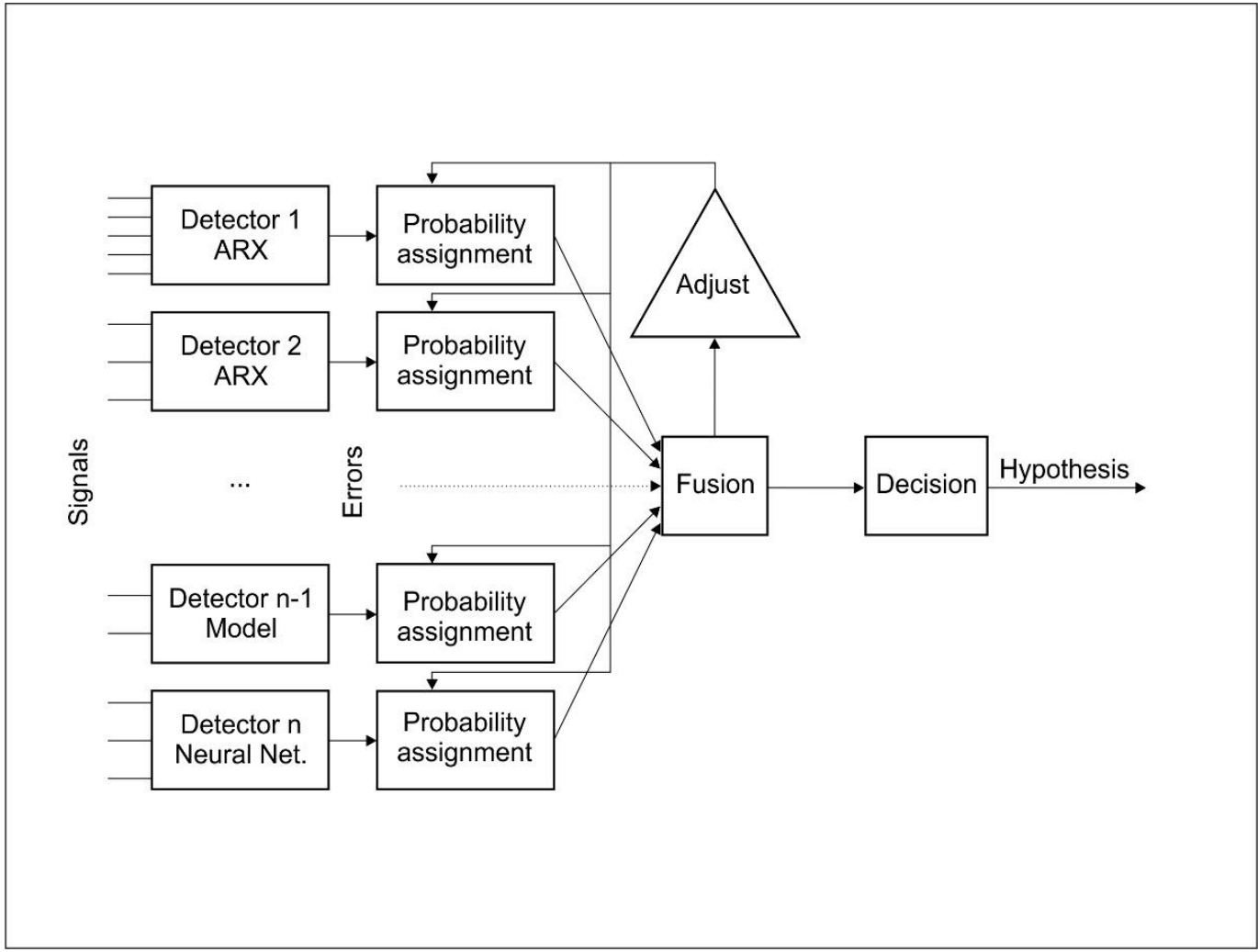
Vehicle data analysis

- Ford-Otosan FMAX (BOSCH)
  - equipped with EDC17 at the beginning and with MD1 engine control unit (ECU) after
  - test drives have been carried out on public roads, covering city, rural and highway with the ambient temperature ranging from -7°C to +20°C
  - total 37 measurement files covering a total distance of approximately 2800 km
- Signal analysis (UMFST + CERTH)
  - statistical analysis, correlation analysis, visual analytics
  - selection of resilient group of inputs, outputs - Granger causality
- Based on the real measurements create the dedicated aftertreatment model simulating different tampering scenarios (TNO)
- Create a simulation model for heavy-duty vehicles in the Exothermia suite (LAT)
  - test the transferability of the proposed detection system to other vehicles

DIAS

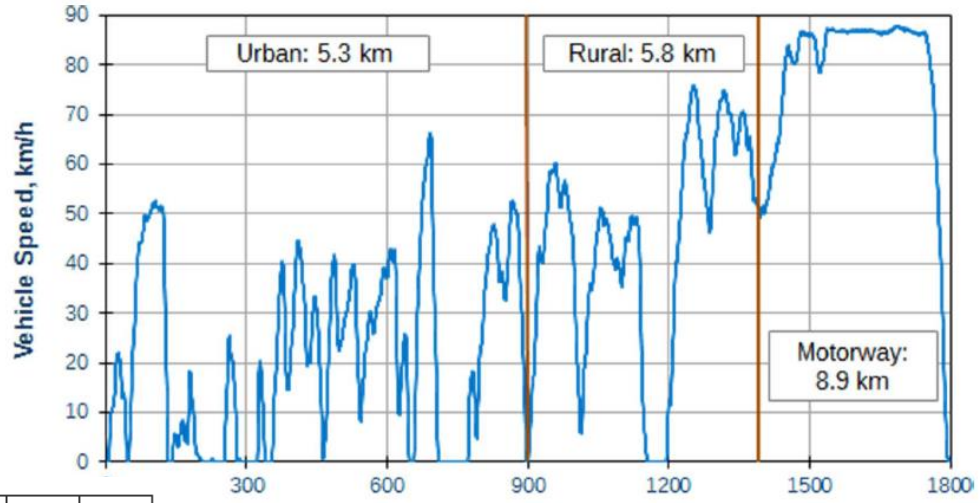
Proposed detection system architecture

- Detectors:
  - Heterogeneous structure of predictors.
    - Autoregressive models.
    - Nonlinear process models.
    - LSTM Neural networks.
    - … other (future).
- Prediction error, relative prediction error aggregation:
- Detector fusion:
  - Dempster-Shafer hypothesis-based fusion.
    - Advantage: ability to include uncertainty.
- Closed-loop adjustment:
  - Probability is adjusted to favour minority reports on abnormal behaviour.



Experimental results based on data provided by JRC

- Vela7 Heavy Duty chassis dyno laboratory
- Tampering device: Emulator 14-019 Renault
  - Injecting false NOX, AdBlue values on CAN bus



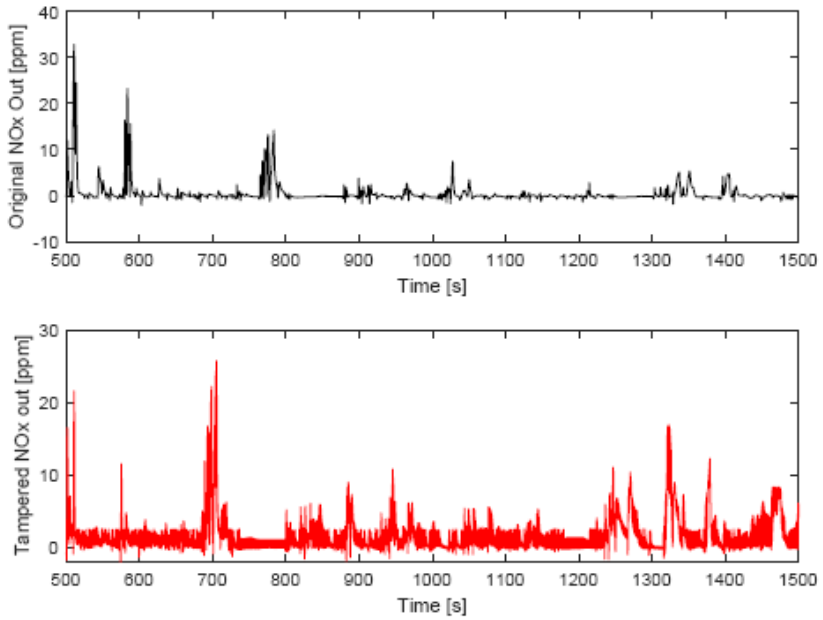


Figure 3: NOx output (downstream) in the absence and presence of the emulator.

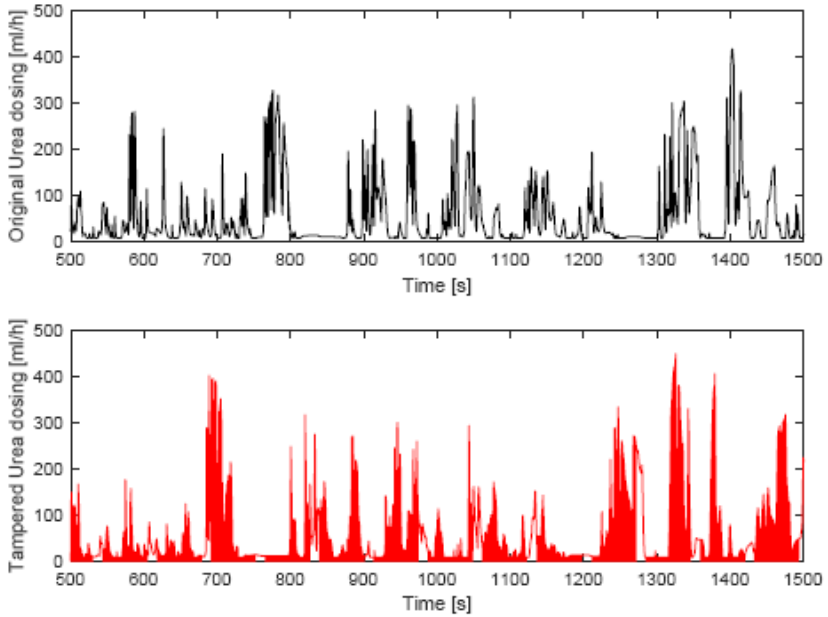


Figure 4: AdBlue (Urea) dosing in the absence and presence of the emulator.

Renault MDA2C
Category: N2
Engine: Volvo Powertrain Corp.
Code: DTI 5 210 EURO VI-D
Size: 5132 cc
Power rate: 158 kW
Fuel: Diesel

DIAS

ARX based detectors and output fusion system

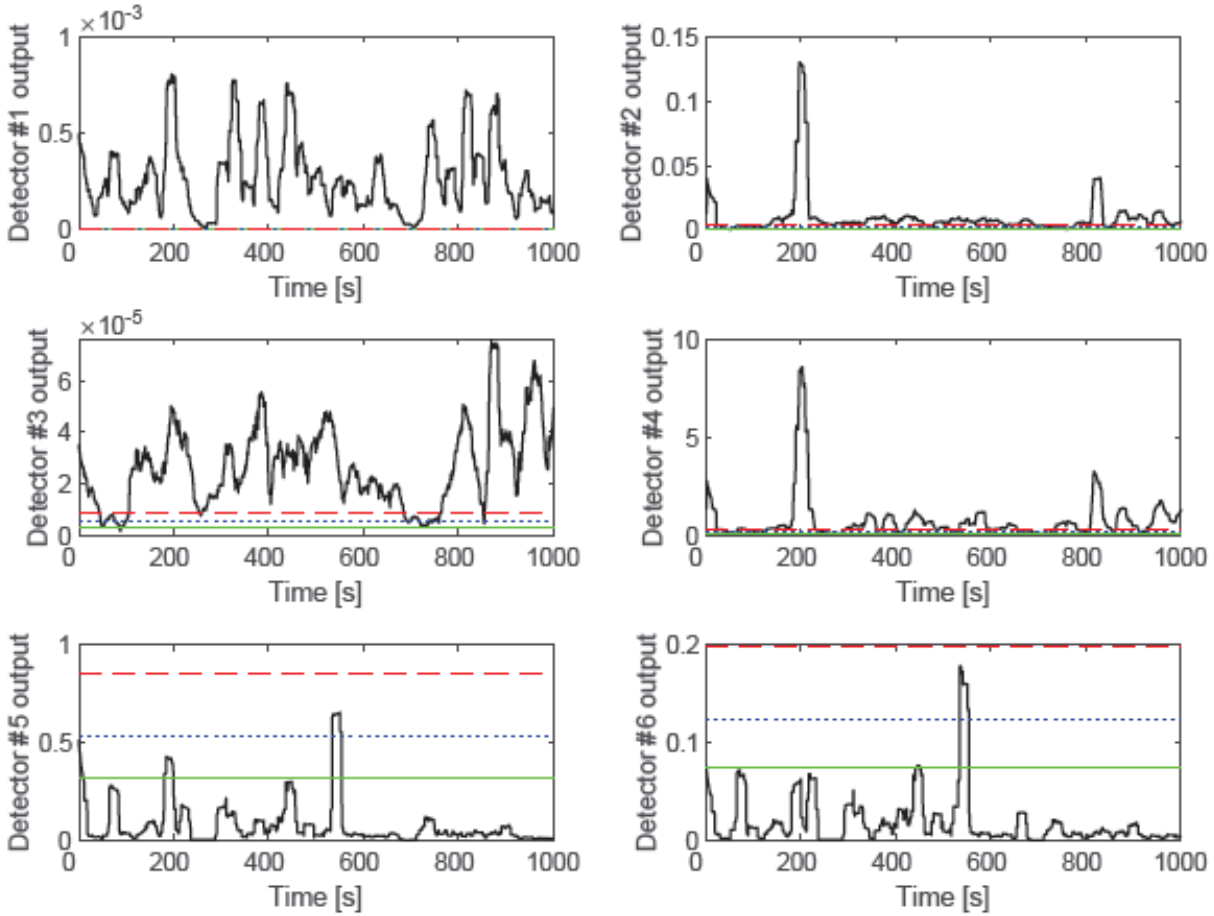


Figure 8: Detector raw output in the presence of tampering.

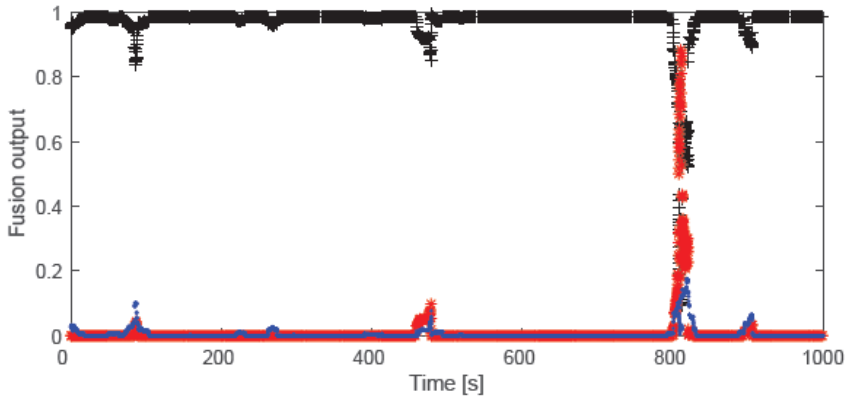


Figure 10: Detector fusion in the absence of tampering: black denotes $m(\{NORMAL\})$, red denotes $m(\{ANOMALY\})$, and blue denotes $m(\{ANOMALY, NORMAL\})$.

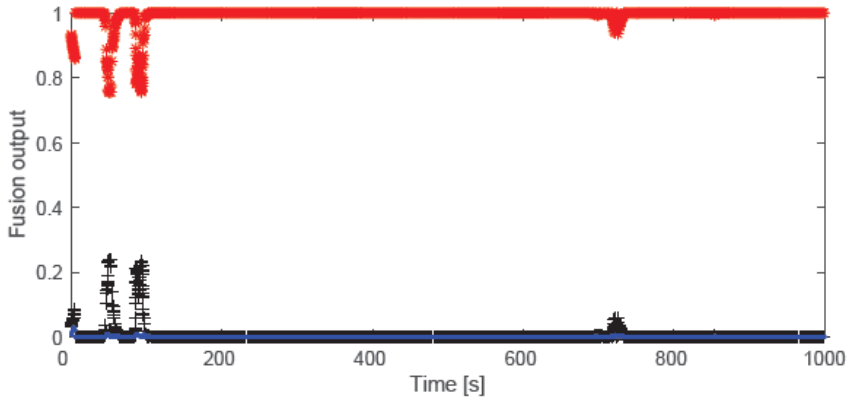


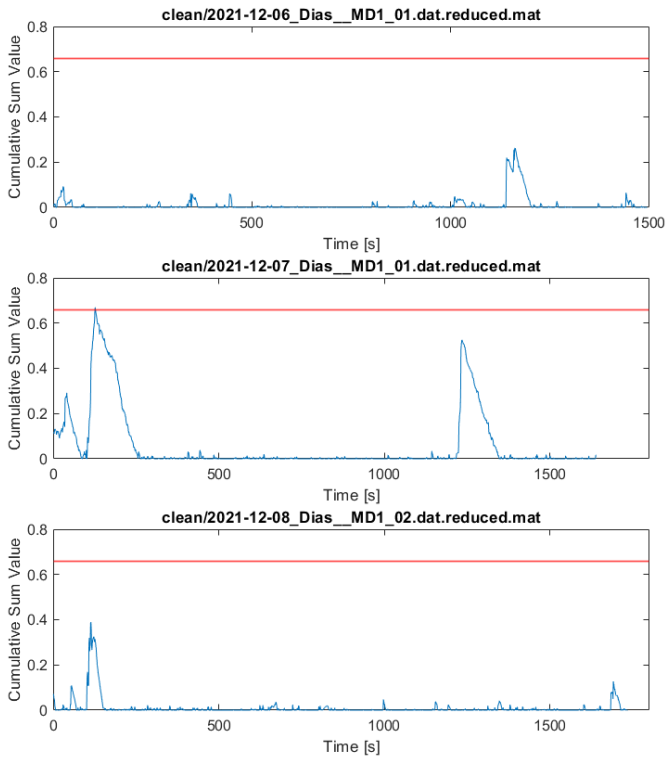
Figure 11: Detector fusion in the presence of tampering: black denotes $m(\{NORMAL\})$, red denotes $m(\{ANOMALY\})$, and blue denotes $m(\{ANOMALY, NORMAL\})$.

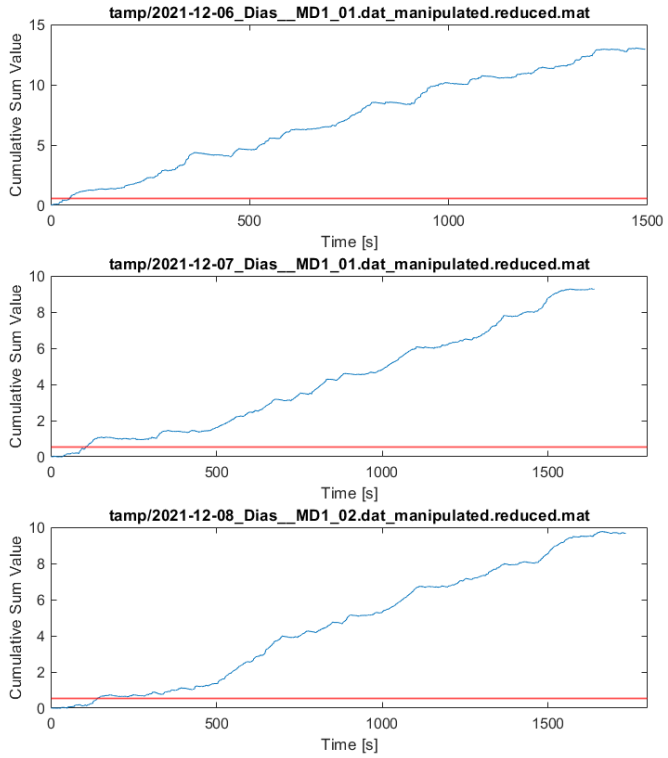
DIAS

Detection on FMAX data

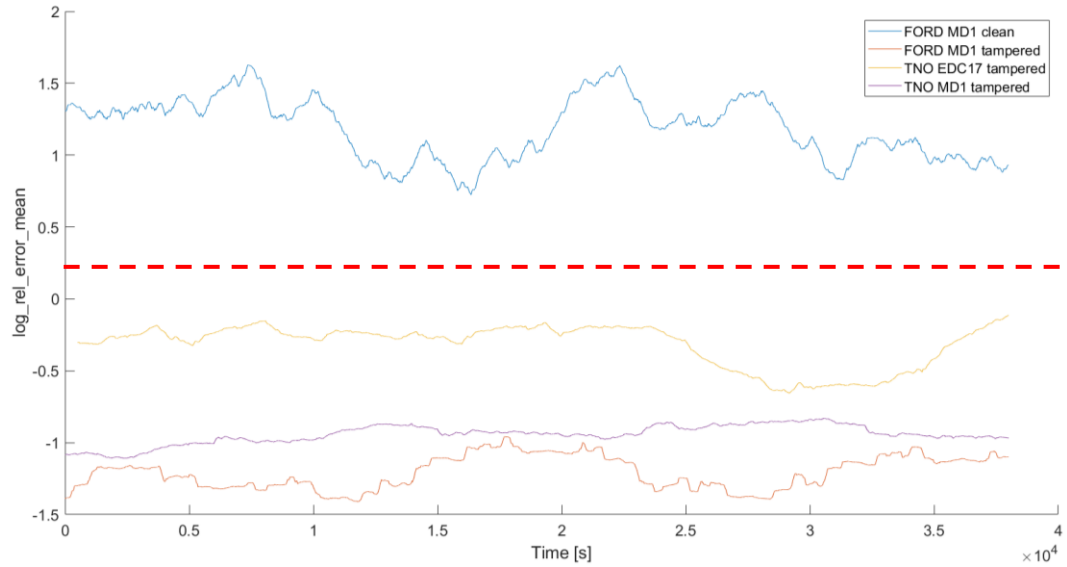
- Simulated tampering:
  - Simplest approach – NOx output value = 5% of SCR upstream NOx, all other signals are unmodified
  - Model based approach – TNO creates a model based on the signals available on the CAN bus - NOx output value
- Use the trained LSTM network

cusum based detection



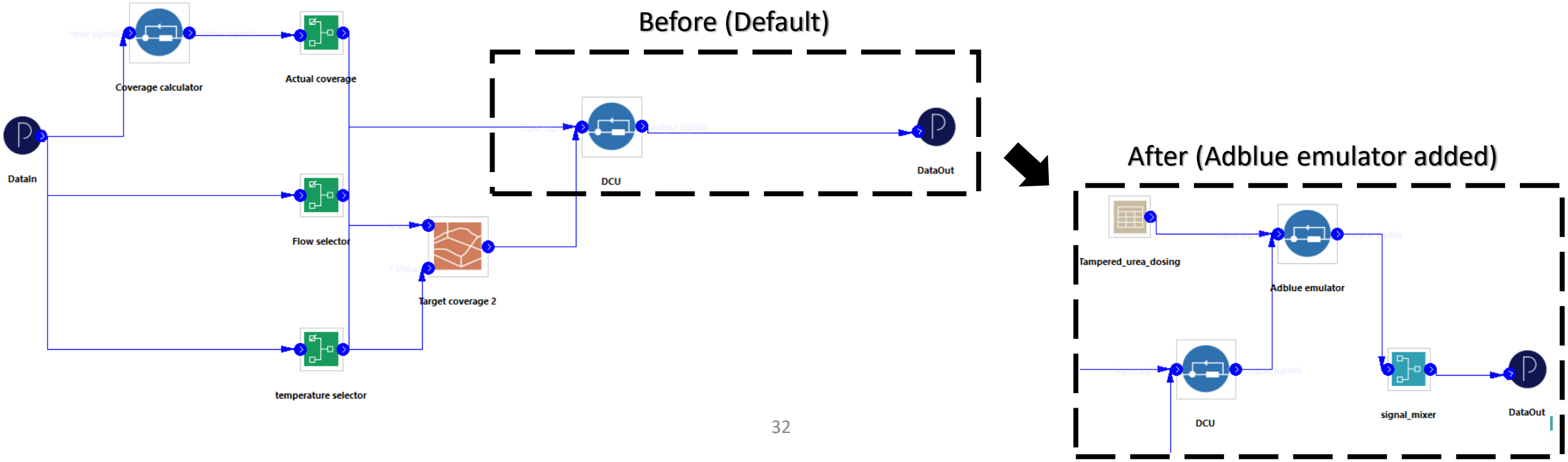


windowed mean relative error



Generic simulation environment (LAT)

- Generic model available and validated
- Model is adjustable (e.g. incorporate FORD's EAT)
- Different cycles: WHVC, fige, VECTO Regional Delivery, WHVCx2 Back-to-back and VECTO Long Haul, cycles with continuous urea injection
- Data was generated by 2 different sampling rate: 1Hz, 10Hz
- New component added to simulation environment de-NOx control system
- More than 150 experiment

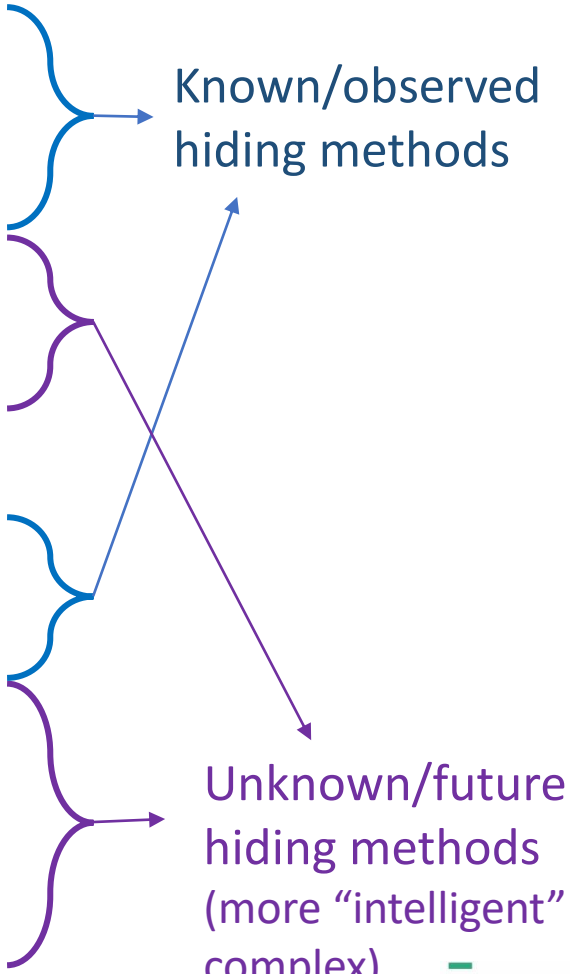


Tampering approach in simulation environment

➢ Simulation -“Hiding" methods applied:

- Urea_hid:
  - **A. Urea_hid A** = Urea_dis × 2.5
    → Since Urea_dis signal has a rectangular wave motive, Urea_hid signal has repeated identical values in a fixed order
  - **B. Urea_hid B** = Urea_dis × Random factor between 1 to 4
    → Express a more complex version of method “A”

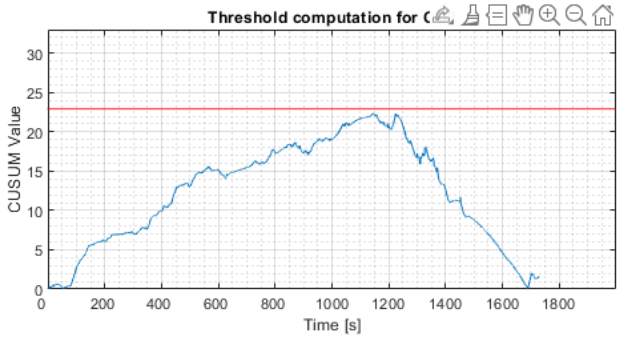
- NOx_out_SCRx_hid* (SCRx = SCRF or SCR):
  1. **NOx_out_SCRx_hid 1** = 5% of SCRx upstream NOx
  2. **NOx_out_SCRx_hid 2** = Random percentage of SCRx upstream NOx
  3. **NOx_out_SCRx_hid 3A and …3B** = Multiple linear regression function based on NOx_in_SCRx and Urea_hid A and B respectively
  4. **NOx_out_SCRx_hid 4A and …4B** = Similar to 3 but with moving average applied (to NOx_out_SCRx_hid signal) every 3 seconds

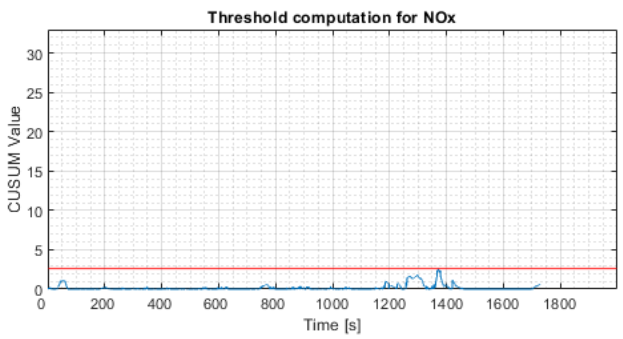


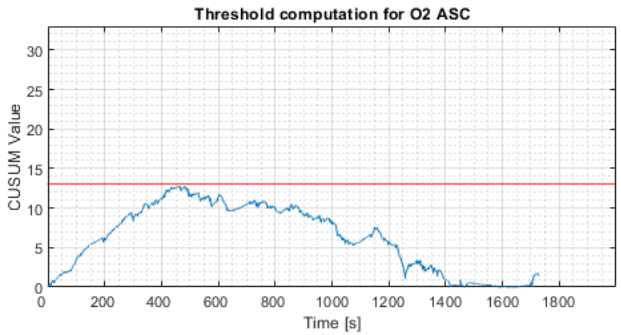
Dis: Disabling action/signal
Hid: Hiding action/signal

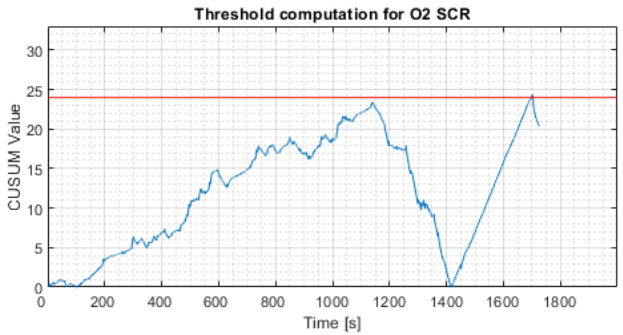
LAT Simulation Results

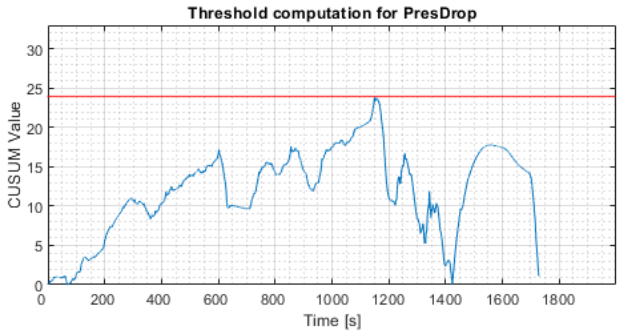
clean data – threshold

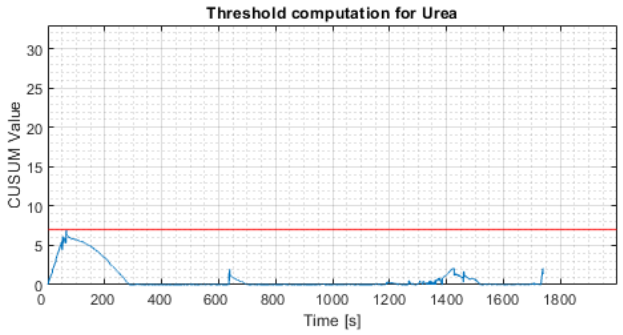








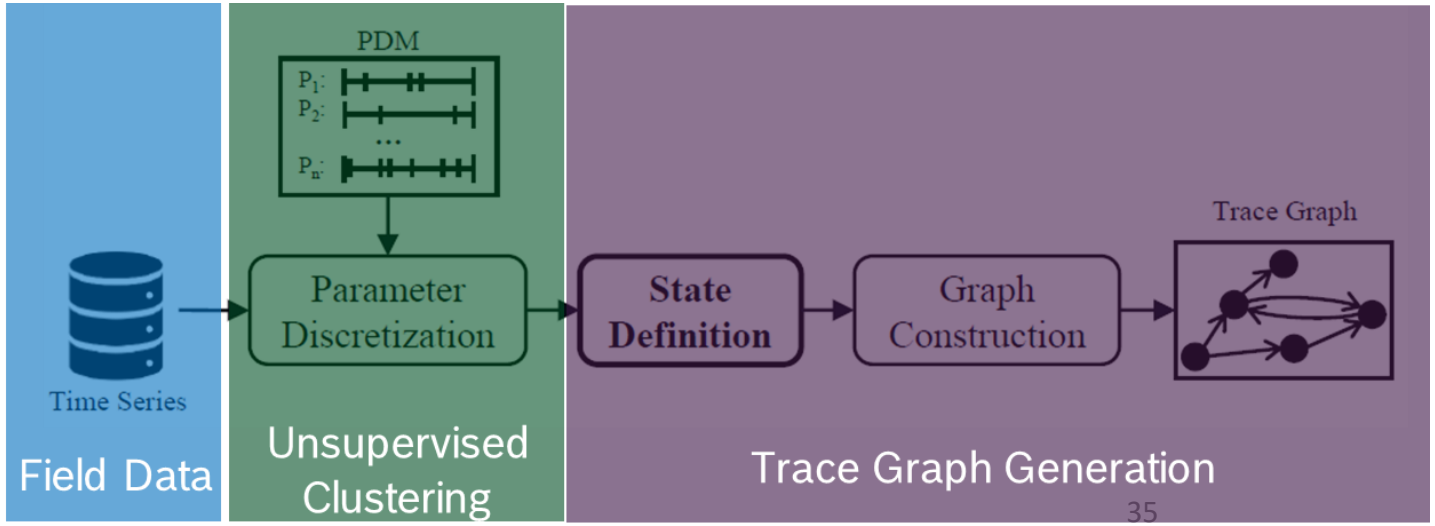




Driving scenario	Monitored Signal	Detection Delay [s]		
		MIN	MAX	AVG
WHVC	NOx out ASC (out hidden)	3	4	3.5
	NOx out ASC (in/out hidden)	15	31	22.83
	O2 in ASC (in hidden)	22	23	22.33
	O2 in SCR (in hidden)	32	36	33.83
	PrDrop SCRFPa (in hidden)	330	480	408.33
	CO2 out ASC (in hidden)	500	660	578.33
	Urea cmd (out hidden)	90	95	92.5
FIGE	NOx out ASC (out hidden)	4	5	4.5
	NOx out ASC (in/out hidden)	49	94	72
	O2 in ASC (in hidden)	10	12	11
	O2 in SCR (in hidden)	16	17	16.5
	PrDrop SCRFPa (in hidden)	290	376	336
	CO2 out ASC (in hidden)	470	580	525.83
	Urea cmd (out hidden)	630	700	665

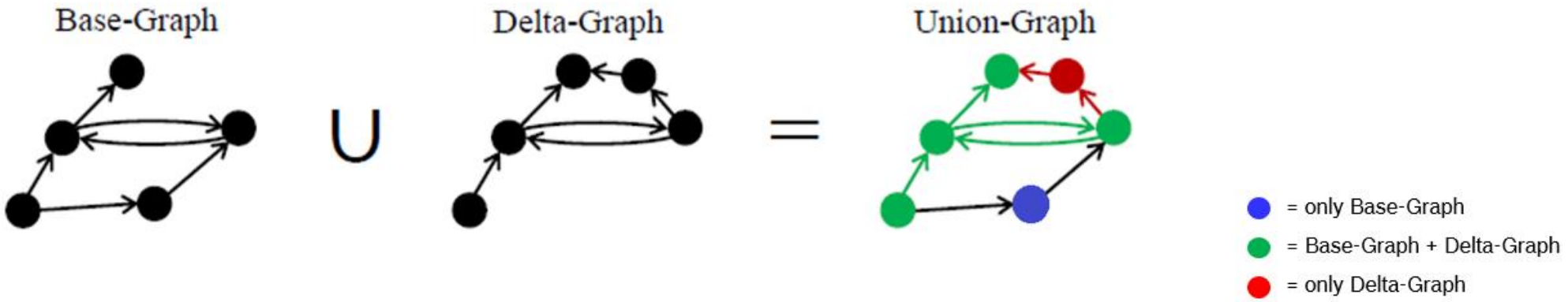
Trace graphs based detection

- Time Series to Trace Graph:
  - Clustering of selected input features / parameters using unsupervised learning mechanism and create parameter discretization model
  - State-to-Vector transformation of the selected input features / parameters
  - Creation and optimisation of the graph using the vectors
  - Analysis of the graph by means of e.g.
    - node size (cumulated visit count)
    - heat maps (permanence time)



Discover the unknown with unsupervised trace graphs

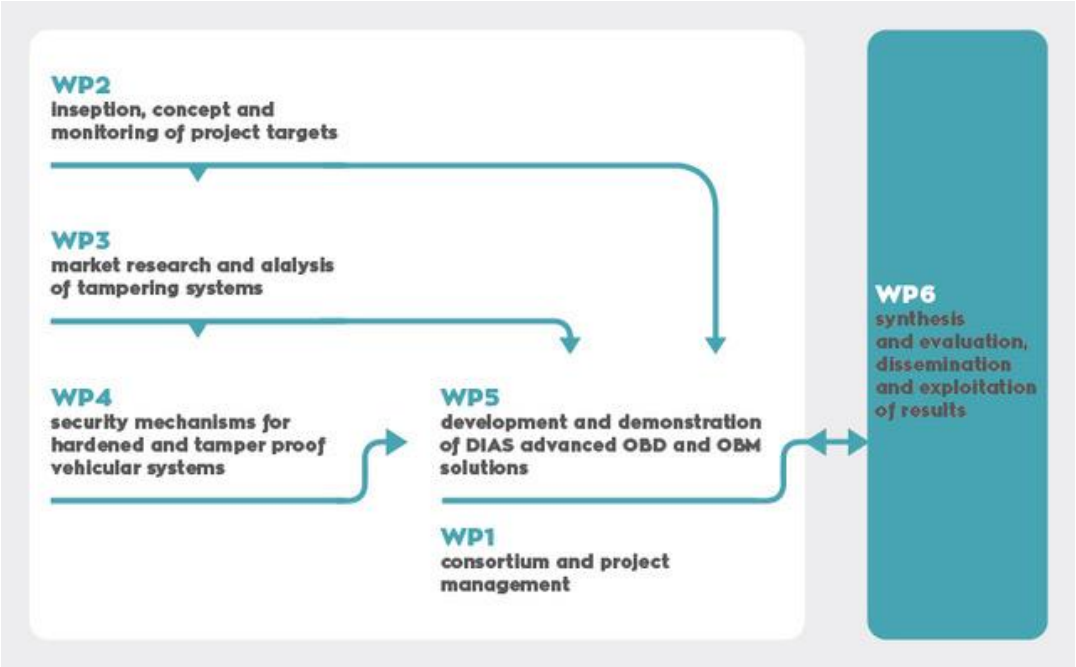
- Optimized parameter discretization model is applied on the set of data to be checked for anomalies (multi timeseries)
- A delta-graph is constructed by executing the trace graph creation procedure
- Comparative Trace Selection takes the base-graph (training data) and delta-graph (test data) as input and checks their comparability
- Nodes, edge that only appear in the delta graph, but not in the base graph indicate an anomaly, such as tampering



Contents

- Countermeasures based on market/system analysis
  - Security solutions
  - Diagnostic Solutions

  --> Overall Diagnostic System
- **Remote Tampering Reporting**
  - Trusted data exchange Self Sovereign Identities
  - Digital Emission Certificates & Visualization
- Summary
- Q&A



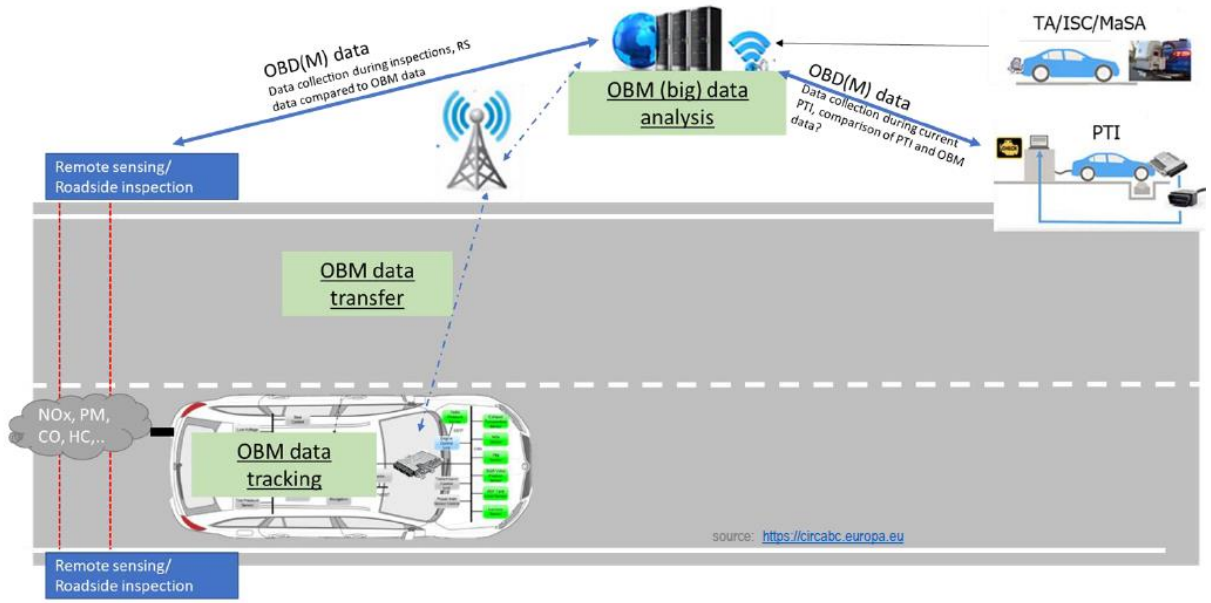
DIAS: Secure Reporting Schemes

WP2
Inseption, concept and monitoring of project targets

WP3
market research and alalysis of tampering systems

WP4
security mechanisms for hardened and tamper proof vehicular systems

WP5
development and demonstration of DIAS advanced OBD and OBM solutions



Demonstrator for Trusted Data Exchange, facilitating remote reporting services. Example: Digital Emission Certificates.

Trusted Data Exchange: Motivation

Why is trusted data exchange important?

1. For business cases where **vehicle-to-cloud** communication is required, we need to make sure the vehicle is the true origin.

   Challenges:

   - **Connectivity** may not be constantly guaranteed.
   - **Integrity** and tamper-proofing along communication chain.
   - **Computational load** on vehicle side is restricted through CCU.

2. For business cases where **cloud-to-vehicle** communication is required, the tamper-proof origin is even more critical, depending on how the vehicle needs to process the incoming data.

   Challenges:

   - Origin must be "trusted", especially if the incoming data is a SW-update or interferes with the critical vehicle systems.

DIAS

SSI (Self-sovereign identity) - the Idea

YESTERDAY
Isolated silos

→ *Different digital identities for each digital service*

TODAY
Central Identity Providers

→ *Dependency on central ID provider; no control over data usage*

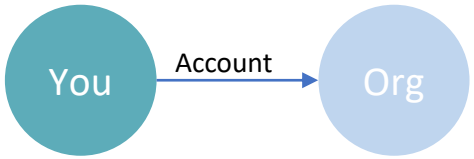
TOMORROW
User-Centric Identity
(also called **Self-Sovereign Identity**)

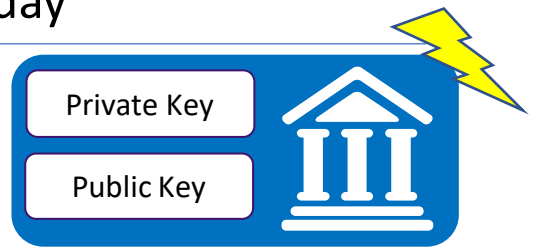
→ *Shift back control to users themselves*

Using SSI as a vehicle for secure P2P communication

Identity today

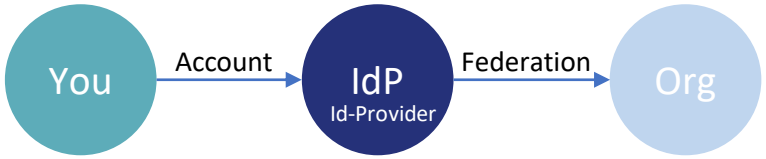
1. Centralized identity





- Each organization has is own identity system
- ID is managed by the organization itself

2. Federated identity

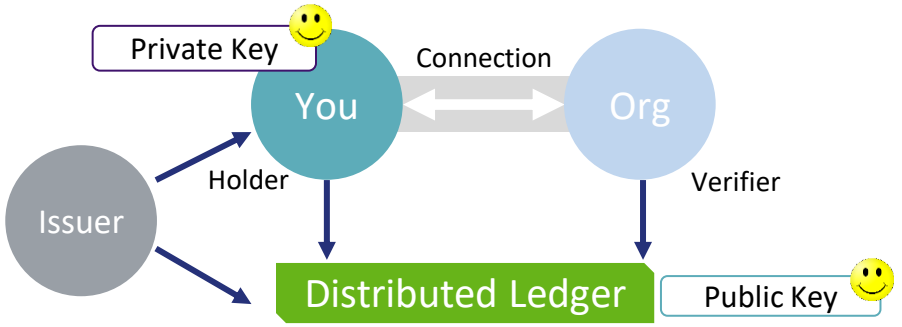


- Identity providers can create profiles
- ID managed by identity providers
- Needs agreement on federated Trustcenter
- Requires centralized distribution of keys

Nobody knows who is on the other site

Identity with SSI

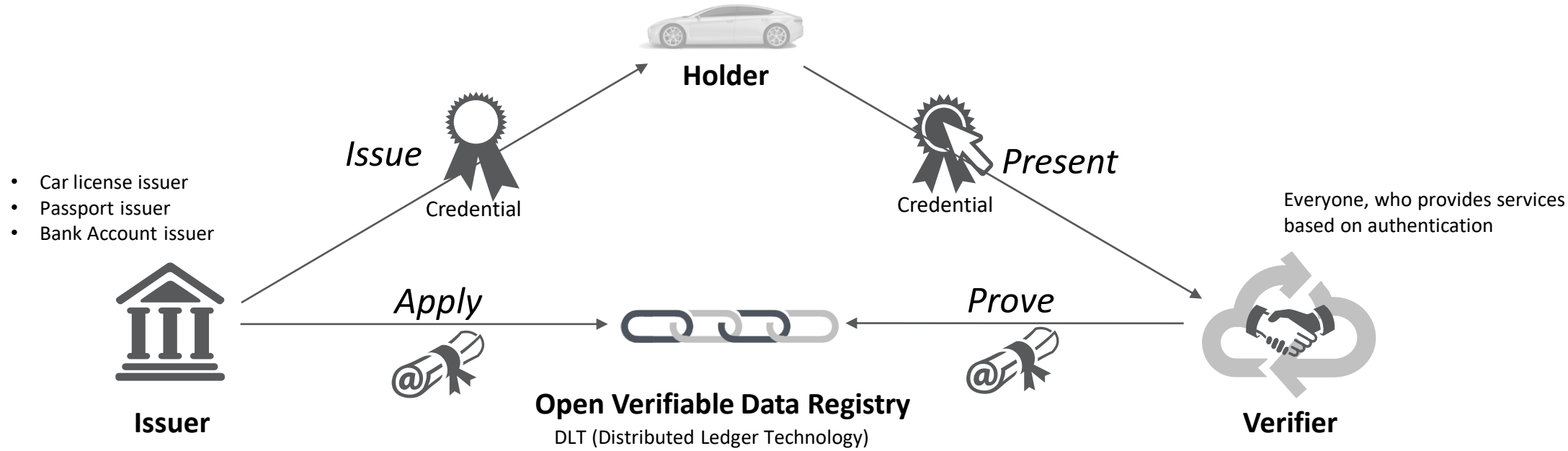
3. Self-sovereign identity (SSI)



- Cryptographic ensures immutability of provided information
- The self-sovereign identity approach offers built-in authenticity during information exchange
- Resiliency through decentralized public key distribution
- No central traceability possible

Decentralized public key infrastructure

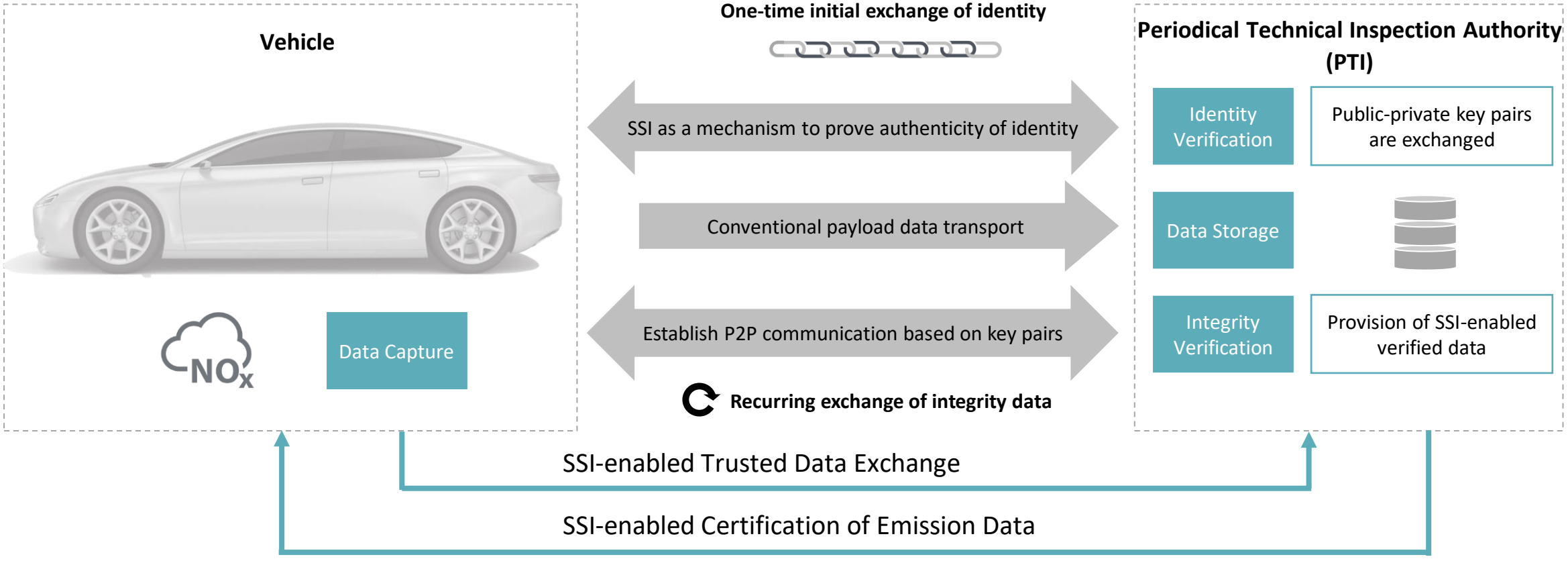
Verifiable Credentials - VCs



VCs are the objects and mechanism to establish a SSI utilizing DIDs. Without VCs, DIDs are meaningless.
On the other hand, DIDs are the “adresses” to deal with VCs, otherwise machines are not able to process them.

Trusted Data Exchange: Principles and Use Cases

1 *Use Case 1: SSI as proof of identity*

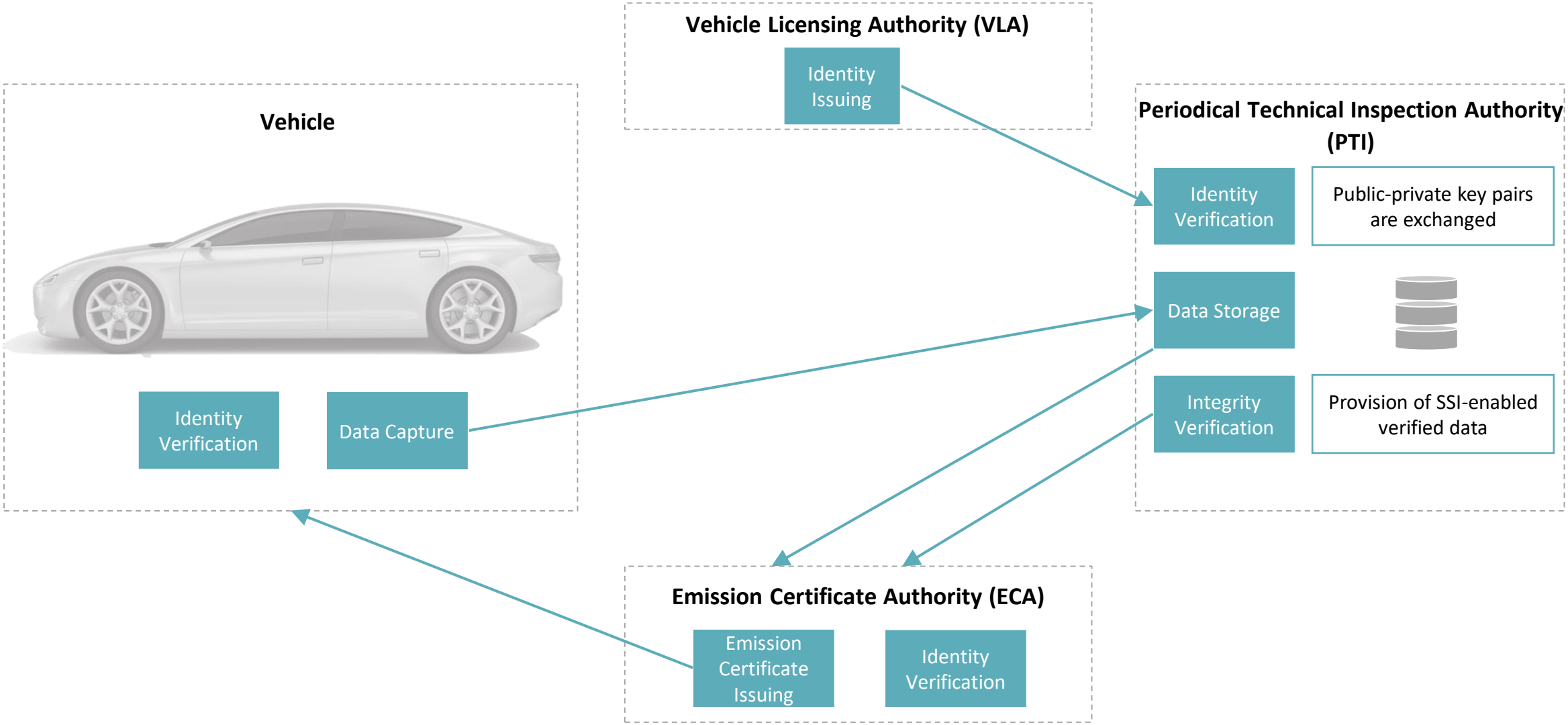


2 *Use Case 2: Using SSI to establish a secure P2P communication to deliver integrity data*

3 *Use Case 3: Certification of Emission Data*

SSI: Self-sovereign identity

Trusted Data Exchange: Principles and Use Cases



SSI: Self-sovereign identity

FMAX: Trusted Data Exchange Suitcase – HW setup

Monitoring & Validation Dashboards

Cloud platform

DIDComm HTTP

VLA, PTI and ECA business logic running in AKS Cloud environment

Router

Ethernet

Base Suite Case

Control circuit

Raspberry Pi 4

7-inch touch screen

CAN module

CAN ports

Demo circuit

CCU: HCP5 (Microprocessor: R-CAR M3N)

Vehicle business logic running on HCP5 in Docker containers

Preprocessed CAN data will be played within CCU

Real Time Streaming Data Visualization

VCAN (Log Files)	Transmission	Streaming Pipelines	UI for data visualization & Utilities

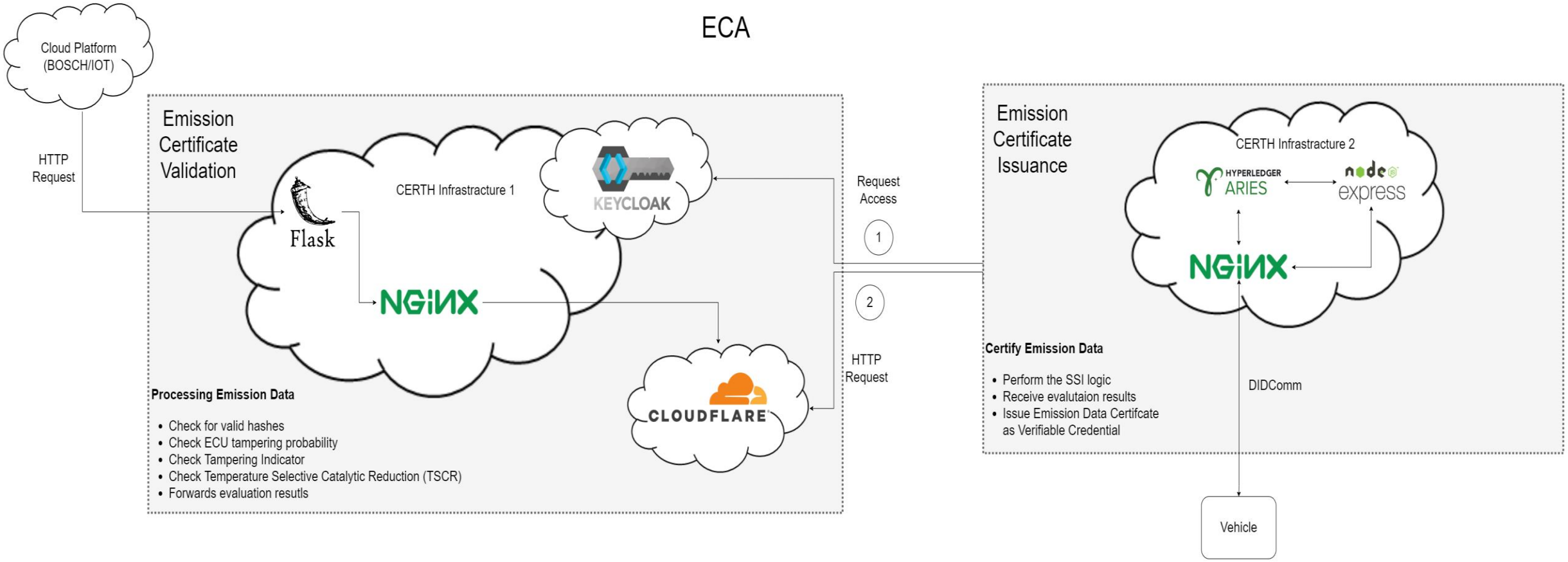
Authentication &
SSL/TLS Encryption

- Messaging protocol for IoT communication
- Used in automotive field
- Consists of 3 entities the Broker, the publisher (KUKSA) and the receiver
- Data transfer with the use of **TOPIC NAMES** e.g., fleet_id/vehicle_id/sensor_id

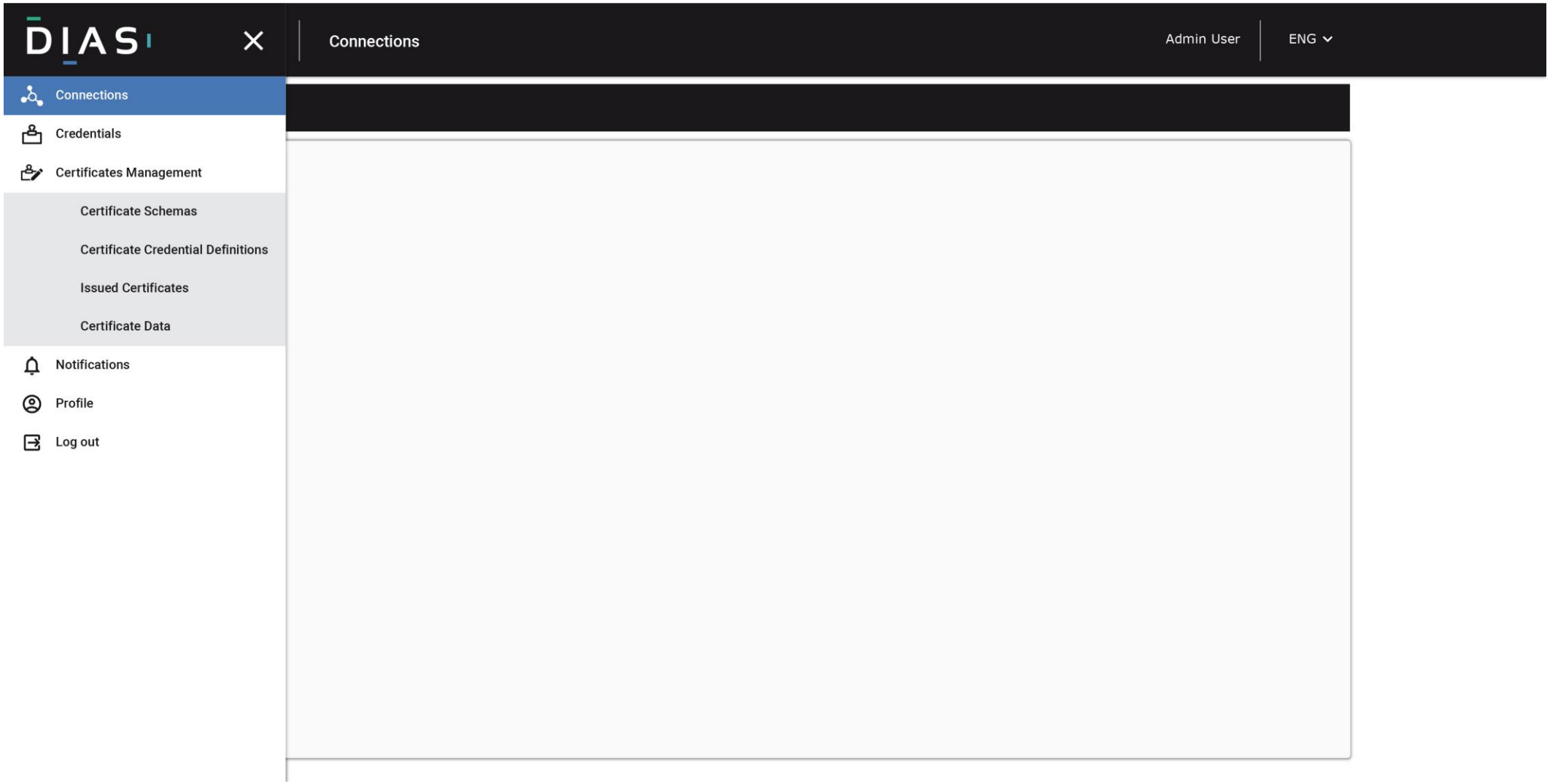
- Distributed event streaming platform
- Lightweight publish/subscribe messaging transport
- Streaming analytics
- High availability
- High throughput (latencies as low as 2ms)
- Scalability

- Streaming data observability
- Streaming data security & compliance
- Streaming data processing (SQL engine e.g., query the data from a KAFKA topic with emission values which are outside accepted threshold values)

Emission Certificate Authority

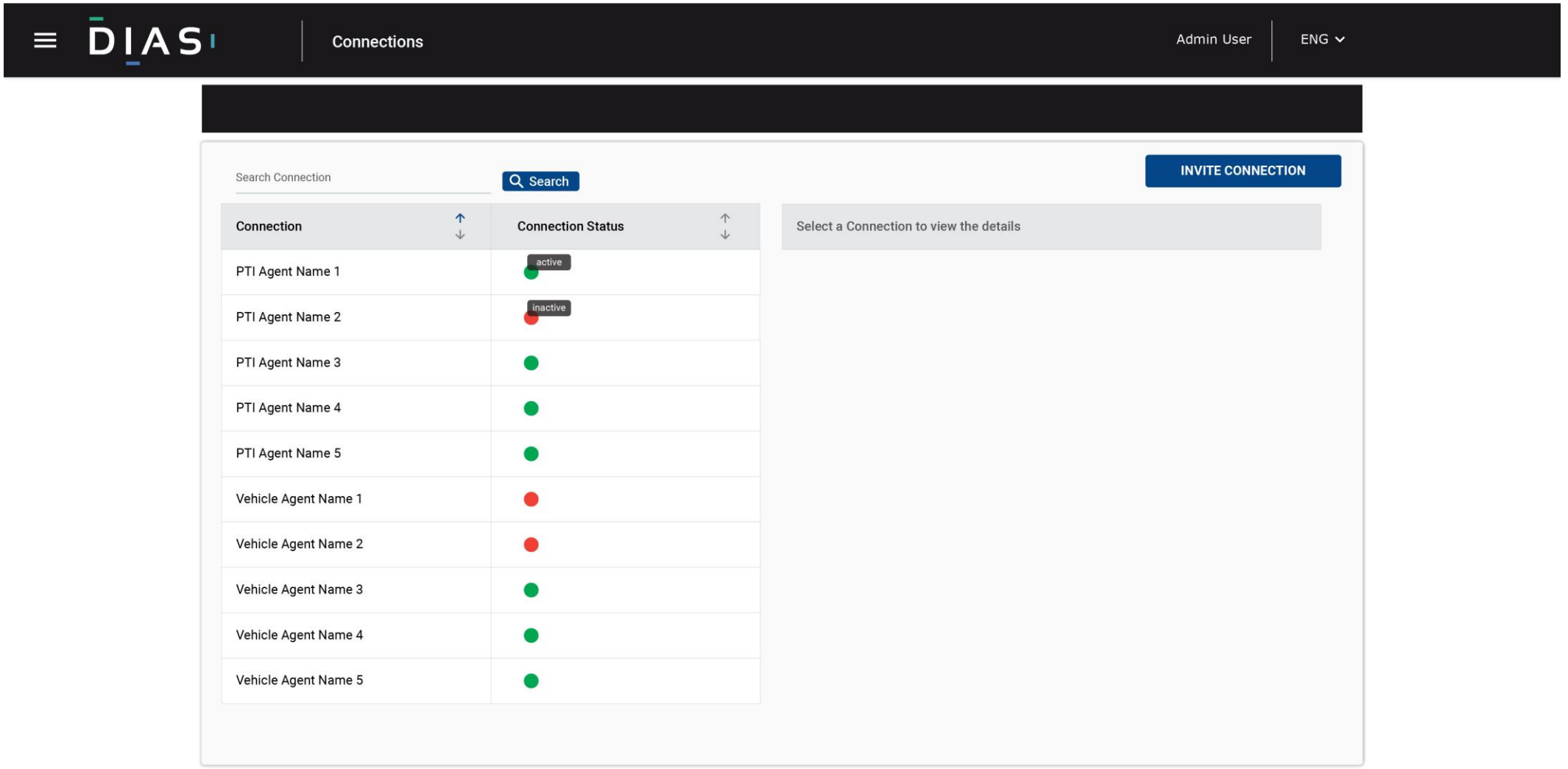


ECA Admin Interface I



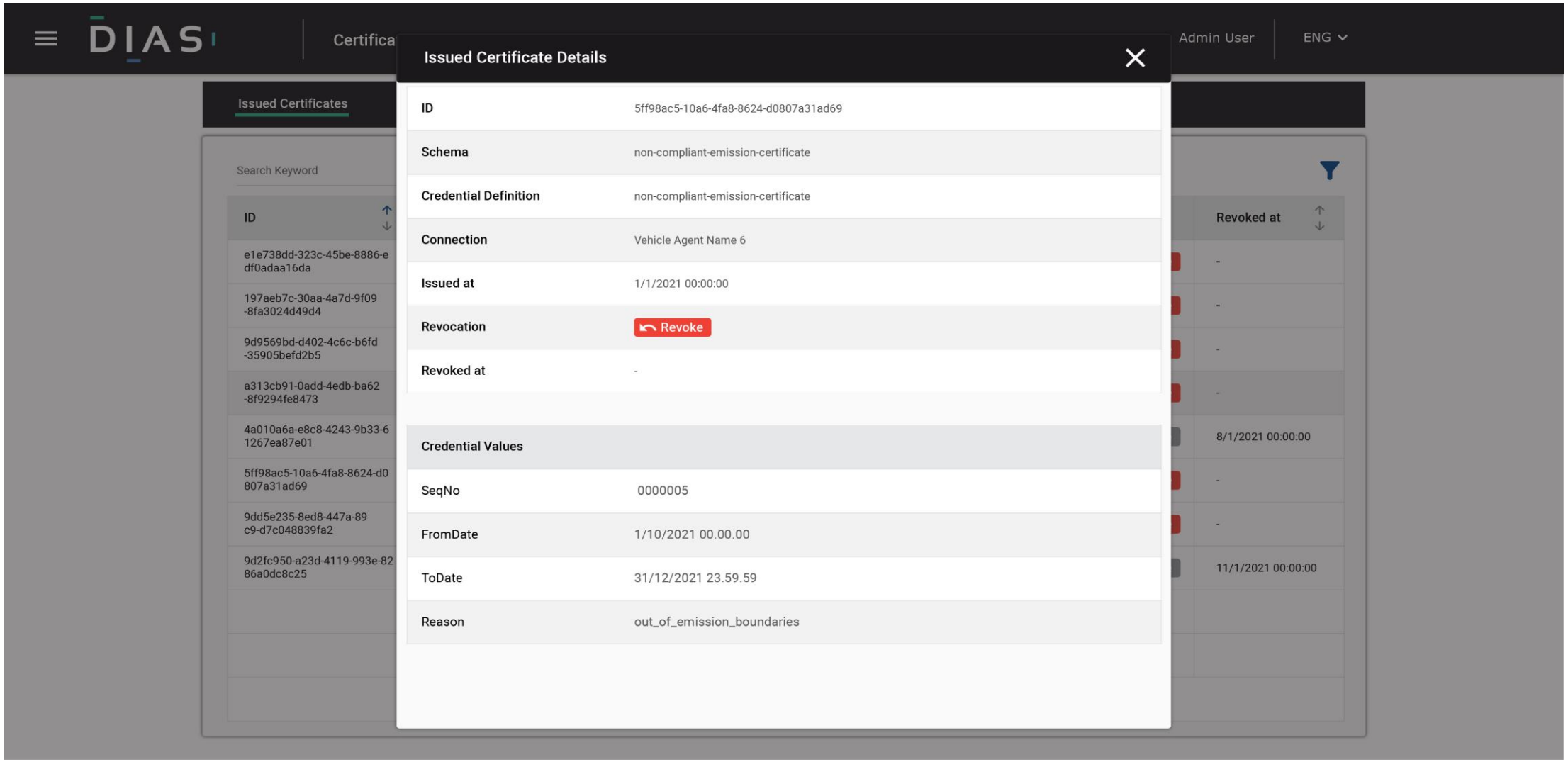
Main Menu of the ECA Admin Interface

ECA Admin Interface II



Connection tab of the ECA Admin Interface

ECA Admin Interface III



Detailed preview of issued certificates in the ECA Admin Interface

Summary

- As a response to the market research and system analysis state of the art **security, diagnostic and reporting features** were developed .
- A set of **distributed demonstrators** was implemented prototypically to prove technical feasibility considering resource contraints
- The Overall Diagnostic System and individual solutions/demonstrators were put to the test in two hacking events and in-depth penetration tests. **No significant weaknesses were found**.
- The system approach helps in defining reasonable, realistic and targeted requirements, allowing alternative solutions to achieve the same goal: **Vehicles that cannot be tampered in an economic way.**

DIAS

SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS

Thank you

Q & A

DIAS
SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS