Secure management of IoT devices lifecycle through identities, trust and distributed ledgers

D5.3 Pilot 1 – PoC Evaluation

Document Summary Information

Grant Agreement No	101020416	**Acronym**	ERATOSTHENES
Full Title	Secure management of IoT devices lifecycle through identities, trust and distributed ledgers		
Start Date	01/10/2021	**Duration**	42 months
Project URL	www.eratosthenes-project.eu		
Deliverable	Pilot 1 – PoC Evaluation		
Work Package	5		
Contractual due date	31/03/2023	**Actual submission date**	26/04/2023
Nature	Report	**Dissemination Level**	Public
Responsible author	John Savill	**Lead Beneficiary**	IDIADA
Authors	John Savill (IDIADA UK) Manel Rodríguez (IDIADA)		
Internal reviewers	George Baroutas (INLE), Blaž Podgorelec (TUG)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 101020416.

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
V0.0	5/01/23	10	Initial Deliverable Structure	Manel Rodríguez (IDIADA)
V0.1	13/01/23	20	Added table of contents and 5.3 specific titles.	Manel Rodríguez (IDIADA SPAIN)
V0.2	26/01/23	30	Filled out executive summary and introduction chapters.	John Savill (IDIADA UK) Manel Rodríguez (IDIADA)
V0.6	10/03/23	75	Sections 1-5 are filled out ready to be reviewed and ready for the results evaluation information to be added.	John Savill (IDIADA UK) Manel Rodríguez (IDIADA)
V1.0	27/03/23	100	Filled sections 5-7 after running the PoC successfully at IDIADA's UK site.	John Savill (IDIADA UK)
V1.5	29/03/23	100	Review and comments	George Baroutas (INLE)
V1.6	31/03/23	100	INLE comments applied	John Savill (IDIADA UK)
V1.7	05/04/23	100	Review and comments	Blaž Podgorelec (TUG)
V1.8	11/04/23	100	TUG comments applied	Manel Rodríguez (IDADA) John Savill (IDIADA UK)

Disclaimer

Copyright message

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
ADAS	Advanced driver-assistance system
CV2X	Cellular Vehicle to Infrastructure
IDAPT	IDIADA Advance driver-assistance systems Platform Tool
IoT	Internet of Things
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
MAPEM/SPAaTEM	Message with detailed road topology information / Signal Phase and Timing Messages. (Shortened to MAP/SPaT)
MQTT	Message Queueing Telemetry Transport
OBU	On Board Unit
PoC	Proof of Concept
PUF	Physically Unclonable Function
RSU	Roadside Unit
TEE	Trusted Execution Environment
VC	Verifiable Credential
V2V	Vehicle to Vehicle communication
V2X	Vehicle to Infrastructure communication

Table 1 - Glossary

1 Executive Summary

This report of deliverable D5.3 describes the evaluation for the PoC leading onto Pilot 1. The deliverable is part of work package 5, framework integration, real-world pilots and cybersecurity exercises, more specifically it is part of Task 5.3 Pilot 1 - Connected Vehicles: Execution and Validation. The present task focuses on the sub-project pilot that aims to develop and test the ERASTOSTHENES solution modules in conjunction with connected vehicles and transport infrastructure.

The report puts the task into context with the rest of the ERASTOSTHENES project, describes the internal validation plan and procedure, the process of evaluating the PoC in the test environment, and the subsequent outcomes and conclusions.

Overall, the deliverable has demonstrated the progress made so far integrating the various PoC versions of the ERASTOSTHENES modules and the feasibility of the modules in a controlled environment that emulates the real-world scenario has been evaluated.

The PoC is evaluated and the feedback for the technical partners is provided below. The required modules can run in the Pilot architecture, the communication between the devices is verified, and authentication of the devices is successful. Individual commands had to be passed on running each stage of the PoC, from bootstrapping to service usage, so the main feedback was to further collaborate with the technical partners to develop the invoking process and streamline the service stage. The PoC architecture is designed to be a good simulator of the Pilot 1 scenario, which aims to be demonstrated in a real-life environment. As such the PoC scenario evaluation provides useful feedback to the technical partners and demonstrates well the technical milestones achieved by the ERATOSTHENES project consortium.

2 Introduction

The following section describes the deliverable overview and progress. It defines the report structure and development over time and the response to review comments. The ERATOSTHENES technologies are described as all the components and applications involved in building the ERATOSTHENES architecture, whilst the modules are the individual containers that are designed by the partners that are run in the domain/IOT device.

2.1 Deliverable Overview and Report Structure

In chapter 3 of the report it is described the strategy for this task and gives a clear roadmap to follow for task 5.3 until its end. Chapter 4 details the Proof of Concept (PoC) evaluation environment and it contains information regarding the PoC scenario, the ERASTOSTHENES modules involved and integrated into the PoC (i.e. bootstrapping, domain enrolment, operational phase), and the specific phases that occur in the PoC scenario. ERATOSTHENES consortium partners have developed modules involved in this pilot, while IDAIDA's primary role is to support and help with PoC execution. In chapter 5, the PoC validation plan is outlined, and the acceptance criteria for the success of the PoC are described. The output of the PoC scenario and a report of the results is defined in chapter 6 while a critical view of the results regarding the future development of the Pilot and the initial acceptance criteria is described in chapter 7. The report concludes in chapter 8.

2.2 Mapping ERATOSTHENES Outputs

ERATOSTHENES GA Component Title	ERATOSTHENES GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D5.3 PoC Evaluation	Evaluation of the PoC in the IDIADA infrastructure, simulating the Pilot 1 use case 1 scenario.	Chapters 6,7,8	These chapters contain IDIADA's evaluation write-up of the PoC, complete with feedback for the technical partners.
TASKS			
T5.3 Pilot 1 Connected Vehicles	This task is devoted to the development, deployment, operation and validation of the IoT-based Connected Vehicle pilot, namely the two use cases focused in the V2I/V2V secure communication (use case 1) and the software update (use case 2) for car/vehicles under protected communication using proposed project services (such as blockchain). The task involves the deployment of the IoT system, collection of data, application/ validation and evaluation of the ERATOSHENES cybersecurity modules, as well as the business validation of the pilot use cases. The outcomes for this task are reported in D5.3, D5.7, D5.11 and D5.13	Chapters 3,4	These chapters contain the relevant information for the pilot strategy lifecycle and the information about the hardware IOT device used in the use case scenarios.

Table 2 – mapping ERATOSTHENES outputs

3 Strategy

This section outlines the strategy used throughout the task to evaluate the PoC and produce the deliverable 5.3.

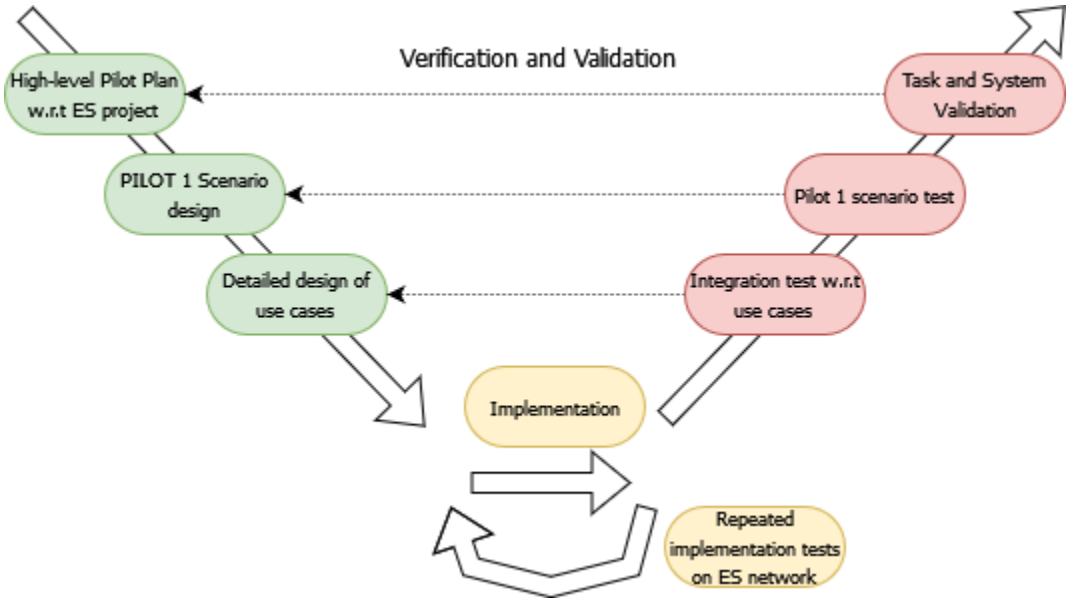


Figure 1 - Strategy plan for task 5.3

Figure 1 describes the lifecycle plan for entire task 5.3, from Pilot 1 planning, detailed designing of the use cases, implementing the modules and finally the task verification and validation. The verification and validation requirements are set early in the Pilot stage by the Pilot leaders (IDIADA). For this specific deliverable, the strategy is similar to the overall task strategy. It involves defining a set of acceptance criteria for verifying and validating the PoC scenario. The detailed process is described below.

IDIADA started by providing hardware details about the IDIADA Advance driver-assistance systems Platform Tool (IDAPT) to the technical partners. A docker image of the IDAPT was uploaded to the hosted Nexus repository for the technical partners to test and ensure that the client-side modules were compatible.

First, a Pilot 1 scenario for the use cases was designed, and then an adapted scenario for the POC was also defined. This meant the PoC scenario plan that was described to all the technical partners was as close to a scaled-down version of the Pilot 1 scenario of the use case one without the need for vehicles.

The use cases describing how the ERATOSTHENES modules will be used were defined early in the roadmap that is described below. They are designed to show off all the capabilities of the modules.

The implementation of the ERATOSTHENES modules contains the PoC evaluation. Here the Pilot 1 lead, IDIADA, repeatedly tests the modules developed by the technical partners on their hardware, constantly giving feedback to the technical partners to ensure the modules work to perform all the functions for the required use case.

The verification and validation process continues on as the Pilot 1 scenario is developed and tested at the IDIADA Spain ADAS testing track.

3.1 Roadmap

The detailed roadmap followed and implemented is presented in Table 3. The roadmap was decided upon early in task 5.3 by IDIADA in conjunction with the WP5 leader.

Description	Timeline
Task start	M12
Hardware and scenario details provided to technical partners	M14
Initial document writing	M16
Validation plan defined	M17
PoC scenario integration	M17
PoC scenario testing + result gathering	M18
PoC scenario evaluation and report writing	M18
Deliver Deliverable 5.3	M18
Pilot 1 Development	M16 Onwards

Table 3 – Task 5.3 Roadmap

4 PoC Evaluation Environment

The PoC scenario aims to replicate the one performed in D5.1, which was a preliminary scenario where the already developed modules had been put together to test its functionality in ENG facilities, but in IDIADA's environment to find possible issues in the devices used by Pilot 1.

The scenario, not being the final one, wants to be as much faithful as possible to the one that will be evaluated in the real-world scenario; hence be able to fix potential incompatibilities with the ERATOSTHENES solution.

4.1 Devices Involved

The IoT devices to be used during the PoC evaluation will be:

IDAPT is an IDIADA product that is a multi-purpose, flexible On Board Unit (OBU) development tool for connected prototyping and development activities, Linux Based System with Automotive I/O and was already used in previous projects, for example, in the H2020 SecureIoT Project (https://secureiot.eu/).

An IDAPT can support a Roadside Unit (RSU) and a vehicle (as an OBU). In the PoC scenario, one IDAPT will be used as an RSU (Traffic light) and another as an OBU (simulating the vehicle). This representation will also be present in the final Pilot use case 1 scenario, where an IDAPT will give the connectivity capability to a smart traffic light and another IDAPT will be placed in the vehicle to be able to receive the information from the traffic light.

Figure 2 - IDAPT

4.2 ERATOSTHENES Modules Involved

Following the D5.1 approach, the modules involved in this PoC evaluation are the ones in green in Figure 3, which is extracted from the D5.1 - Proof-of-Concept. Being the first proof of concept, the version of each component that is used (highlighted in green) is not definitive and shows a reduced functionality from the final one. Only partial implementation of the modules is performed.

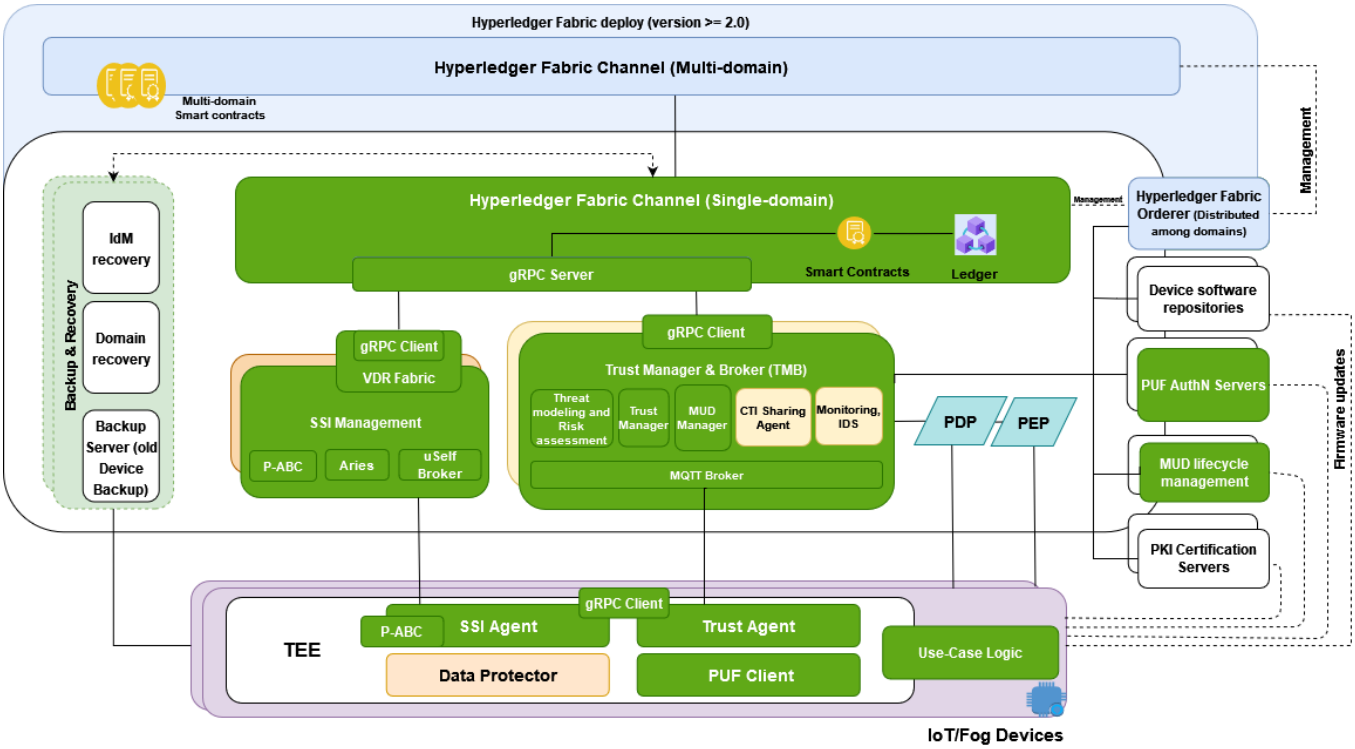


Figure 3 - ERATOSTENES PoC system architecture in relation to the full architecture

The modules that are deployed are preliminary versions as the full Trusted Execution Environment (TEE) has not been integrated at this stage of the project. There are modules that will eventually run inside the TEE that are implemented in the PoC evaluation but since the TEE has not been created for any IOT device, the modules run at the user-level of the IOT device.

On the IDAPT it is the Ledger uSelf application for IoT devices. This is a unique executable that compiles several different subcomponents, specifically for the PoC and has been written in a deployable way by members of the ERATOSTHENES project consortium (ATOS and UMU). The components installed in the IDAPT have been written for the PoC evaluation but represent the functionality of the full modules.

- PUF Client
- Aries Trust Agent
- SSI Agent:

Deployed in the network are the following modules. Some directly interact with the IDAPT, while others interact purely within the domain.

- Trust Manager & Broker
  - Threat modelling and risk assessment – purely domain
  - Trust Manager – interacts with IoT device (IDAPT)
  - MUD Manager – purely domain
- Identity Management
  - P-ABC – interacts with IoT device (IDAPT)
  - Aries – interacts with IoT device (IDAPT)
  - uSelf Broker – interacts with IoT device (IDAPT)
  - PUF Authentication Server
- IoT device Lifecycle Management
  - MUD Manager and MUD File Server – purely domain

The domain-side and the device-side modules have been described fully in D5.1, including the I/O and how these are interconnected. Section 4.4 presents in more detail how these ERATOSTHENES modules are used.

4.3 Infrastructure

The infrastructure of the scenario used in the PoC evaluation has been defined in the previous deliverable, D5.1. A simplified setup of Pilot 1 is constructed to test the required modules. This involves two IDAPT devices, representing the traffic light infrastructure and the car, communicating and verifying trustworthiness. The involved elements of the infrastructure are:

- IDAPT-0064-ES
- IDAPT-0065-ES
- Mosquito MQTT broker (an open source, industry standard MQTT broker: https://mosquitto.org/)
- Server-side docker containers
- Monitoring terminal

The IDAPTs listed will represent the IDAPTs in the vehicle and connected to the infrastructure, but in this PoC, they are standalone devices. They communicate over an MQTT broker, emulating the cellular broker to disseminate the MAP/SPaT messages in the Pilot 1 use case 1. The ERATOSTHENES modules are deployed in individual Docker containers that are hosted in IDIADA's network. The monitoring terminal is a point for key areas of the PoC evaluation to be monitored, with ports to the IDAPTs, the Docker containers, and a view of the MQTT broker.

To ensure the module integration process within the devices, IDIADA provided a Docker image of the IoT device that the client-side modules could be tested and integrated into before the IDAPT installation.

A similar approach has been followed with the ERATSOSTHENES PoC network module infrastructure, with the modules being run in individual Docker containers cloned from the central repository to the local server in the IDIADA site following the process defined in deliverable D5.1.

The communication of the IDAPTs will occur over a communications MQTT broker, hosted at the IDIADA site. This was decided as it is similar to the IDIADA test track's cellular network, where the final Pilot 1 will be deployed and evaluated. The hosted communication MQTT broker can be monitored to check for issues during the PoC evaluation.

The PoC architecture where can be appreciated how every element is deployed and how each one interacts with the others in the PoC scenario to be evaluated in this deliverable, can be seen in Figure 4.

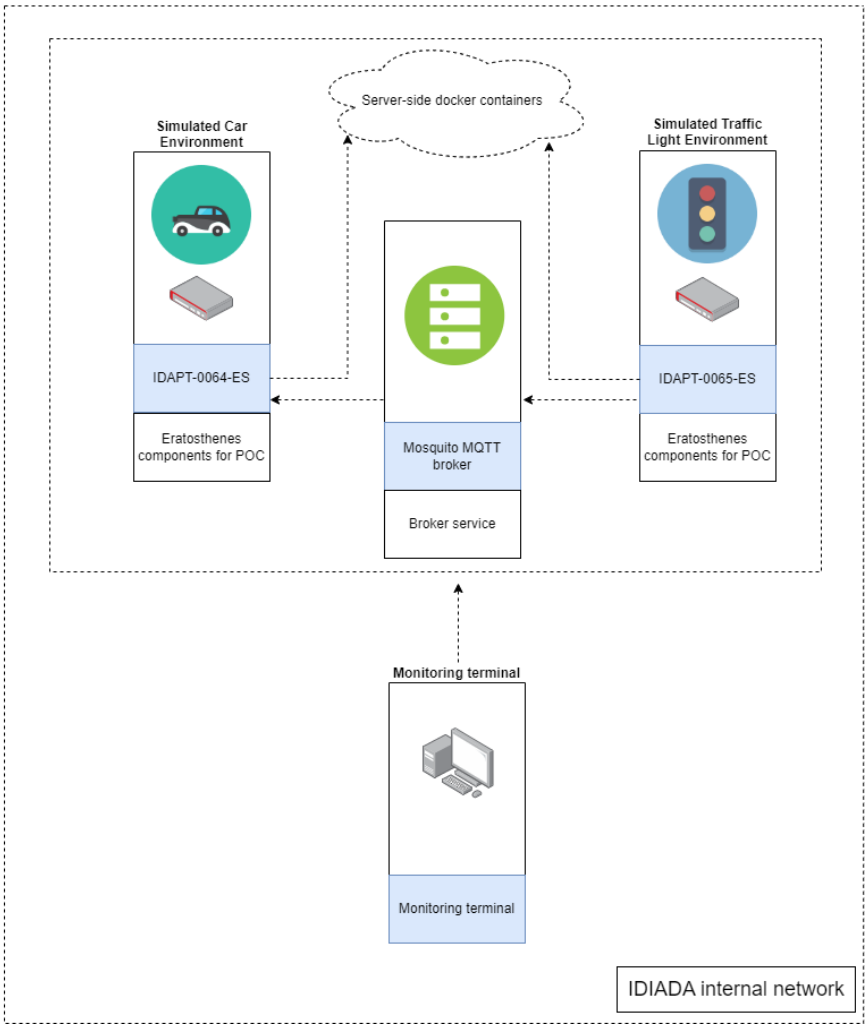


Figure 4 - PoC architecture overview

Figure 4 shows an updated PoC architecture overview from D5.1. Included in D5.1 was a VPN for connecting to the domain modules, but since the domain modules are now installed in IDIADA UK, no VPN is required. This was decided for security reasons and so that the architecture is as similar as possible to the final pilot architecture, with the devices interfacing straight to the domain via a broker.

4.4 Phases

During the validation process, the same phases tested in D5.1 will be performed and evaluated. The flow of these phases has been defined in D5.1, with the IDAPT representing the IoT device and the domain hosted locally on the internal IDIADA servers. The phases are presented below with specific information about how they are working in the PoC infrastructure and in Annex I it is described graphically all the interactions in every phase.

4.4.1 Bootstrapping

The first phase of the PoC is the bootstrapping phase. This phase was defined in D1.3, along with the domain enrolment. For the phase, ATOS has developed Docker modules that have been built on an image that is compatible with IDAPT.

The modules are started remotely on the IDAPT using the monitoring terminal. This deploys and starts the docker containers, including the SSI Agent and the Trust Agent. A similar process occurs with the domain components, they are started from the monitoring terminal and run on a headless server, which includes the PUF authentication and the MUD server.

The device is connected over the IEEE 802.11p wireless standard to the internal network that the MQTT server is running on and performs an initial handshake. The traffic light information topics are identified for publication/subscription.

As the IDAPT has already been configured and no manufacturer is involved in performing the PUF enrolment, the device is enrolled automatically to the network during the setup process. The address of the servers on the "localhost" domain are defined here by the pilot leaders, IDIADA, as the ERATOSTHENES PoC network deployment is specific to their network.

The various environment variables are defined; SSI_CLIENT_HOST, SSI_CLIENT_PORT, BROKER_HOST, BROKER_PORT, ISSUER_DID, and the ISSUER_URL.

At the end of the bootstrapping phase, the expected results are having the docker containers of the modules running on the device and the domain with the environment variables for each container configured and ready to connect.

4.4.2 Domain Enrolment

When the bootstrapping phase has been completed, the domain enrolment phase occurs. Since it is a PoC and the domain has limited functionality, a limited enrolment process occurs.

The device generates a DID for its interactions in the ERATOSTHENES framework (with a DID authentication key pair). The PUF server container provides the Verifiable Credential to the IDAPT that it can use for secure message transmission.

Once the device is enrolled in the IdM service, despite the lack of a TEE, the IDAPT device is given a high trust score for the PoC stored in the TMB.

The Verifiable credential is then provided to the device from the onboard SSI client for message transmission.

At the end of the domain enrolment phase, the expected results are having both IDAPTs successfully enrolled with the IdM service and for them to receive a verification message back. The verifiable credential will be issued to the devices for the secure and trusted communication.

4.4.3 Operational Phase

During the operational phase, there is an exchange of information, over the wireless network, from one IDAPT to another that will be verified using the ERATOSTHENES modules.

Inside the traffic light IDAPT, the pre-defined Verifiable Credential will be added to the demonstration Vehicle to Infrastructure communication (V2X) MAP message to create a JSON message to be disseminated. This message is published to a topic on the MQTT broker.

The broker topics are monitored from the monitoring terminal to ensure the message is being passed correctly.

The vehicle IDAPT is subscribed to the topic and receives the JSON message. The JSON message is decoded into the V2X message and the Verifiable Credential.

Passing the ERATOSTHENES components of the message to the required docker container invokes the trust validation process, which communicates with the domain aspects to confirm the message's legitimacy.

When the message has been confirmed to come from a trusted source, the raw MAP message can be printed on the IDAPT terminal, which is, in turn, monitored from the monitoring terminal. This confirms a successful message transmission between the two trusted devices.

At the end of the operational phase, the expected results are having the V2X components on the devices sending/receiving a trusted message. The sending/receiving of the trusted message can be verified using the monitoring terminal to view the messages between the devices.

5 Validation Plan

This section defines the validation strategy and acceptance criteria that have been decided. These have been carefully considered to ensure that evaluating the PoC against these criteria will produce meaningful results and feedback for the ERATOSTHENES consortium, and the teams running the pilot programs (IDIADA, TEL, DWG).

5.1 Validation Strategy

The PoC validation will occur with a successful test scenario. The PoC scenario has been designed to closely resemble the final Pilot 1 scenario for the selected modules, ensuring a successful outcome of the PoC and critical evaluation of its parts will lead to useful feedback for Pilot 1 which will be used for improvement in future versions. This Pilot, in turn, represents an accurate, real-world scenario that the ERATOSTHENES solution is solving.

To validate the actual successfulness of the PoC scenario, it will be tested and monitored to check for the confirmation of a received message from one trusted device to another.

5.2 Acceptance Criteria

The acceptance criteria is split in:

- A list of relevant KPI's extracted from D1.2 – Use cases, requirements, and methodological framework. Which can be seen in Table 4.
- The other part of the acceptance criteria, which is decided with the relevant partners so critical and useful feedback can be provided to the project consortium, is below Table 4 and has been written to address the questions the PoC is trying to answer.

Any other requirements from deliverable D1.2 which has not been chosen as applicable to be evaluated by the PoC rely on modules that are not at the developed stage to be tested (such as the TEE or the recovery modules).

These acceptance criteria, below the table, were decided after planning the scenario and in conjunction with the technical designers of the modules describing the capabilities of their modules at the time of the evaluation.

Req ID	Description	Rationale	Validation Means	Measurable Success Criteria (KPI)	Dependency with other requirements
P1_FR_10	Devices in a network must have some increased trust value/score	Consistency regarding the trust values between the IoT network and the blockchain	Ensure that the blockchain and all nodes of the IoT network have the same picture regarding the Trust Relationships.	Trust score values of IoT devices stored in blockchain. Algorithm implemented.	P1_NFR_13
P1_FR_11	Sender/Receiver devices must identify each other	In order to establish a trusted communication between devices, they should identify each other in a decentralized approach	Sender/Receiver IoT devices identification verified	Devices identify each other in 100% tested scenarios	-
P1_FR_12	Sender device verifies that it can trust receiver device before starting the communication	Before starting the communication between the Sender and Receiver, the Sender must verify that the Receiver is trustable. Device needs to perform the operation to be trusted in Receiver device before	The device is registered into a Trusted Registry or obtain a Verifiable Credential claiming its trust-ability	100% of network devices can be verified as trustable	P1_FR_01, P1_FR_11

		starting the communication			
P1_FR_17	Vehicle to Traffic light data transaction authentication	The Vehicle can authenticate with the traffic light control center as a trusted user.	Vehicle PUF enrollment - authentication	Real time authentication and data transfer	-

Table 4 - KPIs from D1.2

Since this is a simplified scenario for the PoC, there are limits to the extent these criteria can be evaluated. For example, since there are just two devices in the network that we assume are trustworthy, the extent to which P1_FR_10 can be evaluated is limited. The trust scores of the IoT devices are pre-defined, and there is no trust algorithm to update.

Described below are further acceptance criteria that will be evaluated to ensure there are meaningful PoC results, and the modules are ready for Pilot integration. To evaluate these questions, IDIADA will analyse the PoC, its architecture and keep a log of any issues that occur during the testing. By evaluating the PoC against the following questions, we can determine if the concept was successful and a good proof of the Pilot scenario:

1. Does the PoC represent a realistic beta-version of the Pilot? To answer this question an analysis between the system architecture of Pilot 1 use case 1 and the PoC evaluation scenario is done. A write-up summarising the differences and similarities is included in section 6.3.
2. Are the modules able to be easily installed, accounting for a variety of hardware? To answer this question a log is kept of the process IDIADA UK goes through to install the modules. The measure of how ease-of-use of the individual modules are described below in section 6.3.
3. Does the operational phase occur at a realistic speed for connected vehicles? During the PoC evaluation the operational phase for the bootstrapping, enrolment and authentication will be checked to ensure the process occurs quick enough to not affect the vehicles reactive actions.
4. Where are the points in the system where an attack could occur? To evaluate this acceptance criteria IDIADA will perform a system analysis on the PoC and identify where is the best location to attack the network and devices during the Pilot 1 use case 1 scenario.

6 Validation Outputs

6.1 Validation Reports

Multiple consortium partners contributed to generating the validation reports and testing the concept network and client-side modules in the IDIADA connected vehicles environments.

The three main subcomponents of this PoC evaluation to generate the validation reports are the V2X connectivity, the client-side modules, and the domain-side modules.

V2X subcomponent – To create the validation reports, a reliable V2X messaging service needed to be used. The IDIADA team has developed their satellite application exclusively for disseminating V2X messages over their internal MQTT service. The application is run on the IDAPTs and can be monitored and controlled from a console on the same network.

Client-side subcomponent – The client-side modules were installed with the help of ATOS. The repository was cloned from the GitLab repository. The most recent branch of the client-side modules was used. The environment variables file was edited to account for the IDAPT architecture and communication the different communication structure. Processes such as verifying the Verifiable Credential were performed by entering the full command into the device terminal.

Domain-side subcomponent – The domain-side modules were installed with the help from ENG. The development branch of the GitLab repository for the required modules was cloned to IDIADA UK's internal servers. The environment variables file for each of the modules was edited to account for the network architecture at IDIADA UK and the required ports were opened.

Monitoring the interactions of these project sub-components, and the subsequent feedback, on the internal network enabled IDIADA to evaluate the PoC.

6.2 KPI validation extent

There are four KPIs, from section 5.2, that the IDIADA team decided were relevant to check the PoC against taking into account the state of the project regarding which functionalities/modules are already present and can be validated.

- P1_FR_10 – This indicator is to check whether the devices on the network have an increased trust score. It is validated by ensuring the nodes on the network can check the Trust Relationships of the other nodes. Using the provided SSI-ledger application provided by ATOS/UMU the IDAPTs can manually assign a trust score to the devices on the network.

  This a limited trust process. The trust scores are provided for the device without verifying any TEE or anything identifiable by the device and are manually handled by commands sent to the device itself.

- P1_FR_11 – This indicator is to check the sender/receiver trust verification. To validate this indicator the IDAPTs are tasked with verifying each other using a combination of the Verifiable Credential and the domain service. The V2X messages that are passed between the IDAPT devices are wrapped into a JSON container that includes the Verifiable Credential in the "meta" part of the message.

- P1_FR_12 – This indicator is to check that that the devices verify each other as trusted before the messaging commences. To validate this specific KPI the device(s) must be registered into a trusted registry or issued with a Verifiable Credential. As described above the V2X messages are sent with the Verifiable Credential. Then each message can be verified as sent from a trusted device. It is important in Pilot 1 as there will be many MAP and SPaT messages sent during the course of the scenario, with the traffic light keeping all vehicles updated on the light's situation.

- P1_FR_17 – Finally, this indicator checks the specific traffic light and vehicle data authentication. The messaging application, developed by IDIADA, provides the V2X MAP message. To measure the success of this KPI, and validate it, the devices are required to be enrolled with the PUF. The PUF client, at this stage of the project, is in preliminary development. The ideal scenario would have the devices being enrolled and authenticated by the manufacturer rather than during the scenario test. There is no attacking threat in this PoC, and all devices are authenticated.

6.3 Acceptance criteria evaluation

This section will be focused on the acceptance criteria getting back to the questions to be answered presented in section 5.2.

1. Is the PoC represent a realistic beta-version of the Pilot?

   During the PoC evaluation the IoT devices, where the Eratosthenes modules which are not deployed in the network are installed, are IDAPTs. The IDAPT device will be the one used as an OBU for the vehicle and as a RSU for the traffic light in the final first use case scenario. This part is one of the most critical points regarding incompatibility between Eratosthenes solution and the final pilot use cases.
   The communication between the IDAPTs will be different, as now is used IEEE 802.11p and in the final scenario it will be cellular, but the network difference should not affect the result.

   Taking this into account it is reaffirmed that the PoC evaluation is a realistic beta-version of the final Pilot where the most critical points are the same ones that match between scenarios.

2. Are the modules able to be easily installed, accounting for a variety of hardware?

   The modules are developed to run in individual Docker instances. Having the modules run on this universal virtualization platform has meant that the installation and running has been relatively simple. The IDIADA domain architecture was X86 and strictly headless. To install the required modules, a terminal was connected, and the containers were cloned from the GitLab project hub. The process was similar for the IOT device (IDAPT) with the client-side modules installed on the ARM architecture of the IDAPT, after cloning from the Gitlab project repository.

3. Does the operational phase occur at a realistic speed for connected vehicles?

   The dispersion of the messages between the IDAPTS, as viewed from the central control terminal, is of an adequate phase-time for use with MAP and SPAT messages. The message rate can be modified to a more recurring step if needed, but the current communication between the V2X chipsets on either IDAPTs is more than satisfactory.

4. Where are the points in the system where an attack could occur?

   This acceptance criteria are about establishing where it is best to demonstrate the improved security of the ERATOSTHENES network architecture. When the multiple MAP and SPAT messages are being passed between the IDAPTs they transfer via a centralised MQTT broker. A cellular broker will be used in the Pilot 1 scenario, in both use cases. In either case the messages from the traffic light need to be dispersed publicly to be useful. This is where the system is most vulnerable. If the messages that are received by vehicles are not validated and authenticated, then their source cannot be confirmed. For the Pilot scenario, with the TEE,

there may be different points of attack. Malicious code could be injected into the infrastructure device, the cellular network channel between the devices and the ERATOSTHENES server could be interrupted and spoofing devices might try to send messages to the cellular broker. The nature of the attack and how the system is set up to deal with them has to be decided with the consortium and the pilot partners as the final system architecture is designed. Now that IDIADA has a strong idea of the capabilities of the network and also specifications for the connected vehicles communication channels, they will lead this decision process to ensure the attack is realistic and feasible.

7 Critical View of the Results

- The overall architecture of PoC evaluation, in the domain and the client, was smoothly implemented. The modules, in their container form, were downloaded from the repository efficiently. The individual modules met the expectations and fulfilled the requirements of the system at this stage. The SSI agent is able to enrol the device into the ERATOSTHENES trust server, using its counterpart module in the domain. The IDM-agent on the device is able so successfully trigger a trust check with the verifiable presentation and communicate with the domain. The trust management broker is able to verify that the devices are enrolled on the server when a trust check is performed by the car (receiving) IDAPT when it has received the V2X message.

Though the PoC in the IDIADA environment was successful, there are parts of the process that can be improved:

- The installation of the modules: Using the group Gitlab site to develop the modules and then disseminate them worked well. IDIADA could clone the relevant branch for the modules required and run the docker images in the device/domain. Having to change the environment variables for this specific scenario and device is fine for testing the network concept, but for a complete project, a final package that self-deploys with a simple script is necessary. The pilot programs that are starting now will require the modules to be deployed, and it would be preferable that the technical partners continue to develop a script to install and deploy the client-side modules in the devices.

- The running of the code: Having to enter all the commands manually on the devices is not how the final scenario will run. This method used in the PoC meant that each authentication and each message had to be individually triggered. The invoking of the modules on the device will be handled by a separate script. The V2X message received on the vehicle IDAPT will trigger the commands to verify the Verifiable Credential. Work will be done by the Pilot development partners to ensure their devices/scenarios are able to activate the required ERATOSTHENES modules. Setting up and running the domain-side modules worked fine, the containers ran on the domain and hardware with some configuring of the environment files.

- The uniform platform application: For the ERATOSTHENES modules to be implemented in all the Pilot scenarios they need to run on multiple different platforms. There were some issues with the implementation of some of the docker containers (Swagger-UI) on the IDAPT architecture. The project consortium must work together to ensure that all modules are applicable to all different types of hardware, especially as the TEE gets developed. The ERATOSTHENES modules must run uniformly on all different platforms when required.

- Messaging network security: The MQTT network tested in the PoC evaluation is not particularly secure. This is improved by using a cellular broadcaster but improving the channel that the messages are broadcast across is limited by what is being used in the current market. This may only be relevant to the Pilot 1 as there are multiple public messages across multiple devices. A possibility could be the encryption and decryption of the .json message, in particular the Verifiable Credential.

8 Conclusions

The main purpose of the deliverable D5.3 was to evaluate the PoC deployed in the deliverable D5.1 in ENG facilities but now in IDIADA's environment and in a close as possible scenario to the final one developed for Pilot 1. It was intended to extract as much as possible feedback in order to find improvements or weak points of the already developed modules.

- SSI-Agent: This module worked and is able to enrol the device into the ERATOSTHENES trust server, using its counterpart module in the domain. The registration was manual with the commands having to be typed out in the command line by the user.
- IDM Agent: This module worked and is able so successfully trigger a trust check with the verifiable presentation and communicate with the domain. The trust check passed, verifying any device as a trusted device when communicating with it.
- SSI Broker: This module worked, administered the credential and achieved the device enrolling when triggered from the SSI-Agent module on the IDAPT.
- TMB: This module worked and can verify that the devices are enrolled on the server when a trust check is performed by the car (receiving) IDAPT when it has received the V2X message. This module is working as expected for the connected vehicles use case.

Following deliverable D5.1 guidelines it was possible to deploy the current developed ERATOSTHENES modules in IDIADA's hardware, which will be used in the final use cases scenarios of the Pilot 1, and with that deliver the first outcome of Task 5.3. The ERATOSTHENES network security concept has been tested in a scenario that closely resembles realistic conditions and has been evaluated by IDIADA. With the feedback provided to the consortium technical partners, improvements to their modules can be implemented in time for the pilot demonstrations where even more, specific feedback can be provided (D5.7).

The feedback retrieved during the PoC evaluation for the technical partners has been detailed in the critical view of the results section above and the following points are a summary of the feedback of what needs to be considered going forwards:

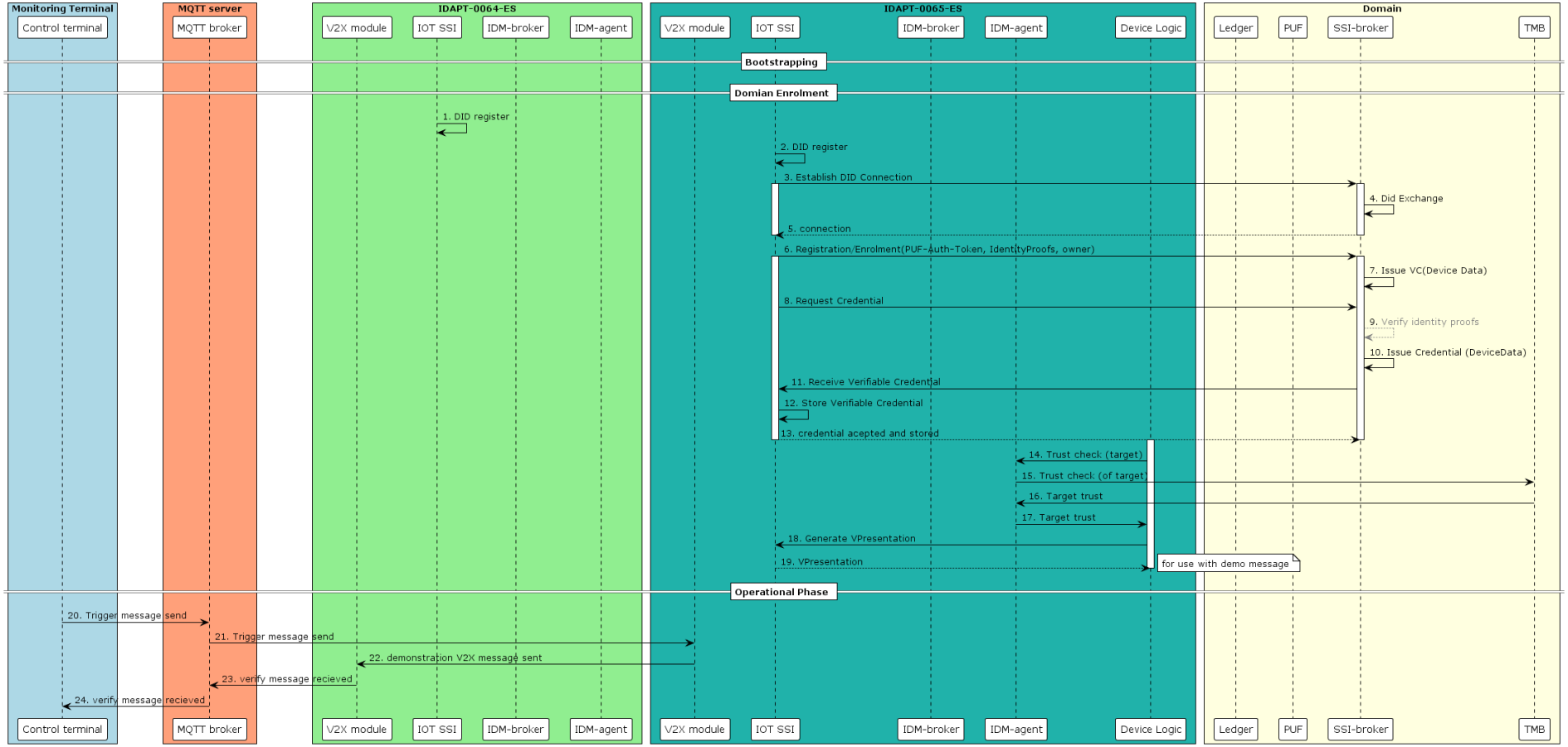
1. The installation of the modules worked correctly but it has identified that a final package that self-deploys with a simple script would be helpful and is something to be considered in future loops.
2. During next steps the pilot tasks partners will need to develop a process which facilitates the verification process of the messages instead of being manual. Being the first PoC it was awaited that it would work less smooth as it will be the final solution.
3. Work to ensure that all modules are applicable to all type of hardware will be needed. This will done whilst the other Pilot scenarios are developed.
4. A weak point where the communications could be violated had been identified regarding Pilot 1 use cases. Further analysis regarding other possible scenarios must be performed to ensure the security of the designed architecture is fully tested and to determine the best possible attack to demonstrate the ERATOSTHENES project. This needs to be carefully considered.

The overall conclusion is that despite some improvement shall be performed, the proof-of-concept shows that the ERATOSTHENES modules are working with industry-standard hardware devices and registering them with a central domain. Device identities can be verified, and messages can be received.

The concept has been verified and evaluated and development of all the Pilot scenarios will continue with collaboration between the technical partners and the Pilot leaders.

With the information gained from the PoC evaluation, the process in setting up the scenario for Pilot 1 and the flow process for each of the use cases are much clearer. IDIADA can begin booking the ADAS (Automated Driver Assistance Service) test track and implementing the smart traffic light and GLOSSA service. IDADA can also begin deciding, with the help of the consortium, how best to attack the use case 1 scenario to demonstrate the ERATOSTHENES architecture. This will require decisions on the flow of the use case 1 scenario. The development of the intrusion detection can then be advance by the relevant consortium partners.

9 Annex I: Phase flow diagram



This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 101020416.