An inclusive Lifecycle Approach for IoT Devices Trust and Identity Management

Konstantinos Loupos*

Inlecom Innovation, konstantinos.loupos@inlecomsystems.com

Harris Niavis

Inlecom Innovation, harris.niavis@inlecomsystems.com

Fotis Michalopoulos

Inlecom Innovation, fotis.michalopoulos@inlecomsystems.com

George Misiakoulis

Inlecom Innovation, George.misiakoulis@inlecomsystems.com

Antonio Skarmeta

Universidad De Murcia, skarmeta@um.es

Angel Palomares

ATOS It Solutions And Services Iberia Sl, angel.palomares@atos.net

Hui Song

SINTEF AS, hui.song@sintef.no

Rustem Dautov

SINTEF AS, rustem.dautov@sintef.no

Francesca Giampaolo

Engineering - Ingegneria Informatica SPA, francesca.giampaolo@eng.it

Rosella Omana Mancilla

Engineering - Ingegneria Informatica SPA, RosellaOmana.Mancilla@eng.it

Francesca Costantino

Engineering - Ingegneria Informatica SPA, francesca.costantino@eng.it

Dimitri Van Landuyt

* Place the footnote text for the author (if applicable) here.

Katholieke Universiteit Leuven, dimitri.vanlanduyt@kuleuven.be

Sam Michiels

Katholieke Universiteit Leuven, sam.michiels@kuleuven.be

Blaž Podgorelec

Technische Universitaet Graz, blaz.podgorelec@iaik.tugraz.at

Christos Xenakis

University Of Piraeus Research Center, xenakis@unipi.gr

Michail Bampatsikos

University Of Piraeus Research Center, mbampatsikos@ssl-unipi.gr

Konstantinos Krilakis

Eulambia Advanced Technologies, konstantinos.krilakis@eulambia.com

Dimitris Syvridis

Eulambia Advanced Technologies, Dimitris.Syvridis@eulambia.com

ERATOSTHENES is an EC, co-funded, research project strongly considering modern security challenges in the domain of Internet of Things in mind of their huge penetration into our day to day lives. There are a series of recent challenges that recently have been converted into obstacles or risk points that could block the secure operation of IoT networks in all day to day activities, from home to office, to leisure and security. These include examples such as the highly increased number of connected devices (at all network levels) that are on top forming inhomogeneous networks and systems of systems. Different vendor characteristics further increase the attack surface that is expected to further rise in the upcoming years. Such, highly critical, characteristics, dramatically increase the needs for confidentiality access control, user and things' privacy, devices' trustworthiness and compliance that require lifecycle considerations. The ERATOSTHENES project orchestrates a novel distributed, automated, auditable, yet privacy-respectful, Trust and Identity Management Framework and Reference Architecture with the ultimate scope to dynamically and holistically manage IoT devices in a lifecycle approach, strengthening trust, identities, and resilience in the entire IoT ecosystem while supporting the enforcement of the NIS directive, GDPR and Cybersecurity Act. This publication describes the ERATOSTHENES technical concept and reference architecture as well as design considerations, architecture characteristics, connectivity and interoperability.

CCS CONCEPTS • End-to-end system security models for IoT • Privacy preserving in IoT • Security and privacy frameworks

Additional Keywords and Phrases: IoT lifecycle security, device management, identity management, IoT trust.

1 INTRODUCTION

Internet of Things (IoT) has recently brought increased interconnectivity and distributed deployment of devices in our day to day lives at a very large scale and capacity directly affecting the everyday environment as well as various industrial pillars and activities. On top of this, the industrial image indicates a high increase in the attack surface of these devices and networks that increases exposure of people and things. At the same time, taking advantage of this situation, there is a high increase in new types of attacks and threats that increases the detection, mitigation and overall resilience over these even

more challenging. The situation is even more complex in mind of the large heterogeneity of devices, including different interfaces, processing power and architectures, vendors and capabilities [1].

1.1 Current IoT Security Challenges

Security challenges faced by IoT devices and networks are complex and multipart. With the rapid spread of IoT, the attack surface has expanded exponentially, necessitating robust security measures for each device and the overall network. However, the limited computing power and memory of many IoT devices pose obstacles to implementing effective security measures. Furthermore, the absence of built-in security features and outdated firmware make IoT devices vulnerable to unauthorized access, data breaches, and manipulation. Interoperability issues and the diversity of IoT ecosystems complicate the establishment of consistent security standards. Insufficient regulations and standards allow manufacturers to prioritize functionality over security, putting users at risk. Additionally, the susceptibility of IoT networks to botnet attacks, privacy concerns regarding personal data, and the need to secure communication channels and authentication mechanisms present significant challenges. Ensuring secure identity management, access control, and user consent mechanisms are further complexities. Supply chain vulnerabilities, weak encryption, and the lack of centralized security management hamper effective detection and response to security incidents. The resource-constrained nature of IoT devices limits intrusion detection capabilities, while the absence of standardized security testing and certification processes hinders consumer decision-making. Exploiting IoT devices as entry points, attackers threaten the overall system security. Finally, the expansion of IoT networks into critical infrastructure sectors raises the stakes, emphasizing the need for heightened security measures to mitigate potential severe consequences [2] [3].

Currently, there is a significant heterogeneity in IoT devices, specifications and vendors and this poses limited security visibility over these devices trust in an IoT network. Common trust mechanisms and other related standards over trust are limited while frequently they are not properly maintained and controlled/managed that is sourced to the actual maintenance of their embedded software (firmware) as well as them including several security holes that can act as an attacker honeypot

Identity management of IoT devices is another critical challenge that involves lacking transparent processes for identity and privacy of devices and things. Simultaneously, there is a lack of adequate security training and protocols implementation for both individuals and devices, and the effectiveness of sharing information with CERTs/CSIRTs (Computer Emergency Response Teams/Computer Security Incident Response Teams) falls short [4] [5].

Blockchain addresses IoT security confronts through enhancing the overall IoT security levels by offering decentralized and immutable data storage capabilities that can be beneficial for trust and identity management over IoT spaces, enabling secure authentication and authorization of the devices themselves or other network things. In a blockchain environment, secure communications are managed via encryption and validation inside the actual blockchain solution. At the same time blockchain can ensure integrity of firmware updates and support decentralized governance, data integrity and privacy.

Blockchain solutions are a core component of the solution offered by ERATOSTHENES. In practice, although existing blockchain solutions have the potential to significantly enhance the trustworthiness and management of an IoT network, their application faces substantial challenges. The need for extensive computational resources, resulting from advanced cryptography requirements, presents inherent drawbacks that hinder their effectiveness. Overcoming these challenges necessitates targeted improvements in various aspects of a blockchain network, with the aim of addressing the specific security concerns posed by the IoT environment [6] [7].

1.2 The ERATOSTHENES project

The ERATOSTHENES project draws inspiration from Eratosthenes of Cyrene (c. 276—194 BC), a renowned Greek scholar, geographer, and astronomer who founded scientific chronography. This project specifically focuses on addressing the lifecycle aspects of IoT networks [5]. The project falls under the category of a Research and Innovation Action (RIA) and has received funding from the European Commission (EC) within the framework of SU-DS02-2020, which focuses on Intelligent security and privacy management. Specifically, the project is dedicated to the subtopic (d) of Distributed trust management and digital identity solutions. INLECOM INNOVATION, based in Athens, Greece, takes the lead in coordinating the project, while a consortium of 14 partners from 8 countries actively participates. The project, with a budget of approximately 6M€, commenced its activities on 1st October 2021 and is scheduled to conclude in March 2025 [2].

ERATOSTHENES project develops and integrates several innovative components (as presented below) in mind of a critical list of highly challenging and very specific IoT security challenges/risks including: i) Establishing a trustworthy environment among objects and individuals in the IoT faces significant challenges due to the lack of security visibility and the heterogeneity of devices. ii) Common trust enforcement mechanisms and relevant standards are lacking, hindering the establishment of a unified and secure IoT ecosystem. iii) Infrequent firmware and security updates for IoT devices leave them vulnerable to known vulnerabilities and exploits. iv) Transparent identity and privacy frameworks are needed to empower users with full control over their identity and data at the device level. v) Insufficient security training and adoption of protocols for both individuals and devices pose risks to the overall security of the IoT. vi) The effectiveness of sharing information with CERTs/CSIRTs is limited, impeding timely response and mitigation of security incidents.

ERATOSTHENES aims to develop an innovative Trust and Identity Management Framework for IoT devices. This framework will be distributed, automated, auditable, and privacy-respectful, effectively managing the lifecycle of IoT devices. It will enhance trust, strengthen identities, and bolster resilience throughout the entire IoT ecosystem. The framework aligns with the NIS directive, GDPR, and Cybersecurity Act, ensuring compliance with relevant regulations. Additionally, scientific writing principles will be followed, including maintaining consistency in the order of currency figures. In the diagram below, the basic components of the solution can be found. The architecture of the solution is presented in the next chapter accompanied by descriptions of all system components.

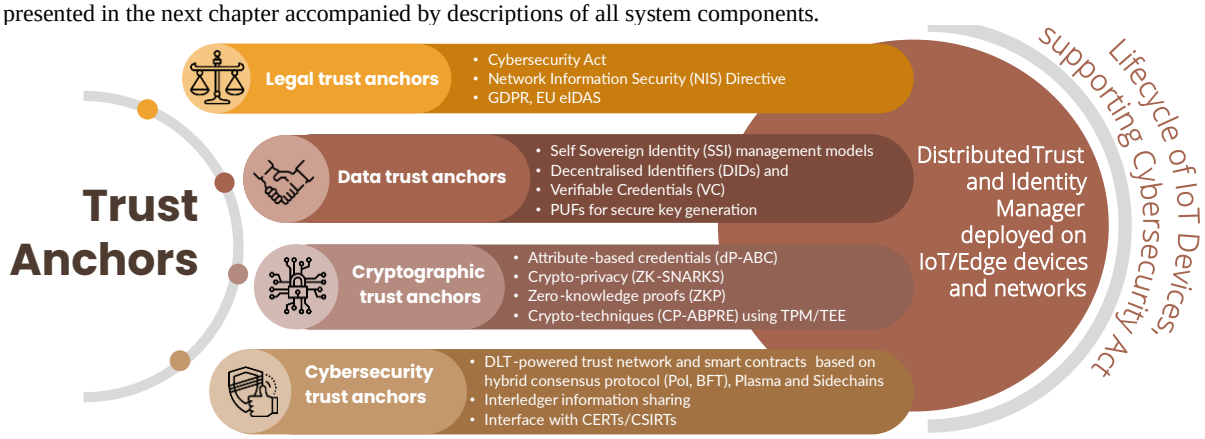

Figure 1: ERATOSTHENES concept description and main components

2 THE ERATOSTHENES REFERENCE ARCHITECTURE AND COMPONENTS

In the chapters that follow, we start by presenting the ERATOSTHENES reference architecture, followed by a description of each of the system components as included in the architecture and their interfaces.

2.1 Architecture Overall Design and Architecture

The ERATOSTHENES architecture and concept have been carefully developed to be adaptable across multiple industrial domains. It is designed to accommodate different use cases, specific requirements, and unique characteristics of each application environment. This flexibility enables its implementation in various scenarios, including transport infrastructures and vehicles, smart devices, personalized health devices, and more. The subsequent chapters of this document delve into the architecture's design and provide detailed considerations for each component, beginning with the core architecture design itself [8].

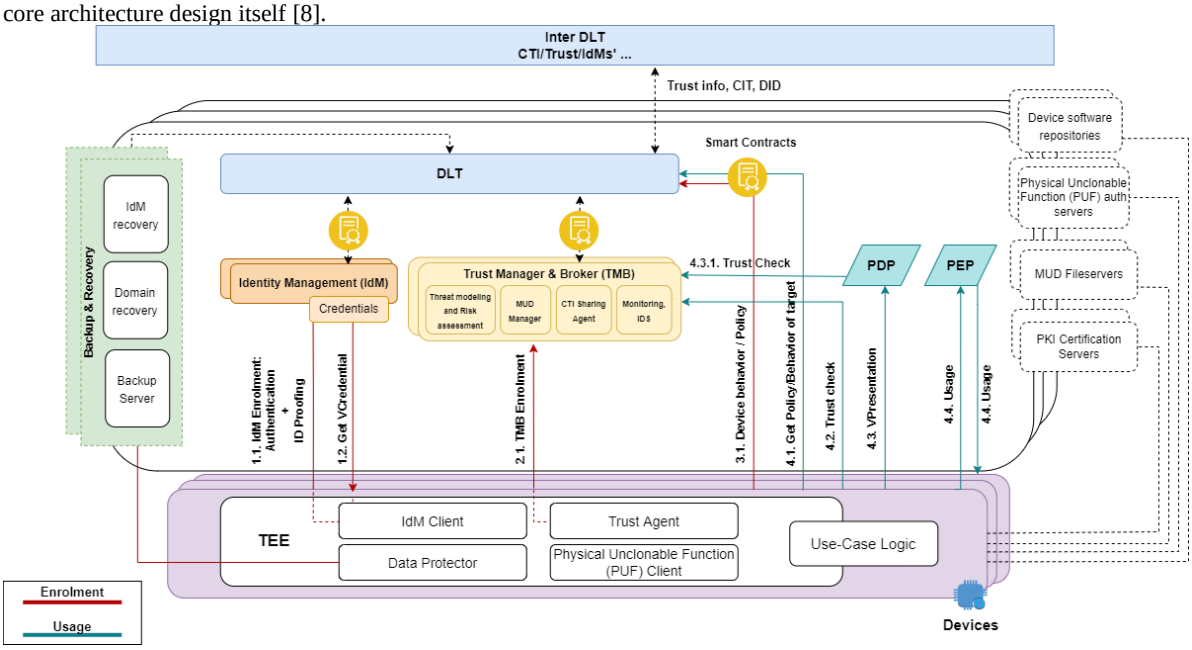

Figure 2: ERATOSTHENES reference architecture - 1st version – as defined in March 2022 [8]

In the chapters that follow we include descriptions for the main architecture components as presented above.

2.2 Trust Manager and Broker (TMB)

The Trust Manager and Broker TMB is also a central component of the architecture, responsible for reputation matters and trust associated parameters concerning the IoT devices while it is in direct cooperation with the DLT layer. Its submodules include a threat modeling and risk assessment component, acting as a real-time threat modeling layer, the MUD manager responsible for interpreting and incorporating the MUD file of the IoT devices, a monitoring and IDS layer responsible for infrastructure monitoring and anomalous behaviour detection, as well as a CTI sharing agent as an interface with CERTs/CSERTs. This component as a major component of the ERATOSTHENES architecture is acting as an enabler for communication between the Threat Modelling & Risk Assessment components, the actual IoT devices, the MUD manager, the CTI agent and the intrusion detection system (IDS). This component, on top, enables formation exchange on trust

relationships between the different IoT entities and at the same time evaluates the trust-worthiness of the IoT devices themselves while manages and controls the trust records for each network IoT device. A basic design characteristic of the TMB is the consideration of various and multiple facts of IoT devices even before the computation of a trustworthiness score while further manage the transmission of events of the IoT devices to the other domains and nodes relating to the risk score of the devices [8] [9].

2.3 Distributed Ledger Technologies (DLT)

A basic component of the above architecture consists of a DLT (Distributed Ledger Technology) layer combined with smart contracts as single-domain and inter-domain layers with providing immutability and auditability for advanced identity management, trusted data sharing and discovery. This is done by combining smart contracts so that entities interact with DLTs locally but also inter-domain. The DLT layer is responsible for the exchange of cybersecurity information, trust and identity data sharing. Another critical component of the architecture is the identity management (IdM) that provides the identity management solution incorporating advanced privacy features and enabling deployment of privacy-preserving credentials, disposable IDs while directly interfacing and interacting with the DLT component [10].

2.4 Recovery and Self-adaptation Mechanism

The current implementation of this component involves a self-adaptive recovery process that manages various tasks. These tasks include coordinating the monitoring of device lifecycle, redeploying a "stateless" trust agent, enrolling the agent identity using the PUF component, and recovering trust management context and data using the DLT component. To ensure quick recovery of trust management agents' execution logic, the component will rely on deployment languages and engines. We are currently exploring different mechanisms to implement the "blue-green" deployment pattern for various device types. This pattern involves deploying a redundant trust agent (the "green" agent) alongside the main agent (the "blue" agent) on the same device, an accessible Edge device, or a dedicated cloud resource. By doing so, we can activate the backup agent with minimal downtime when the main agent experiences a failure. Our intention is to integrate these redeployment mechanisms with the monitoring mechanisms in lifecycle management tasks. This integration will enable us to detect failures or potential risks of failures for the agents and trigger redeployment actions on the relevant devices.

2.5 Physical Unclonable Functions

PUF Authentication Servers utilize a cryptographic fingerprint based on Physical Unclonable Function (PUF) technology to establish the authenticity of the PUF against other entities via the authentication servers of its manufacturer. Within the aforementioned architecture, two types of entities exist: high-level entities and low-level entities. The low-level entities refer to IoT/Fog devices that make use of the ERATOSTHNES Domain services. On the other hand, the high-level entities consist of the IdM, Trust Manager, and the supporting infrastructure depicted on the left and right sides. Before enrolling and utilizing the ERATOSTHENES Domain, all low-level entities can only collaborate with specific supporting infrastructure.

From the standpoint of the PUF ecosystem, the architecture dictates that each low-level entity can exclusively collaborate with specific PUF ecosystem services. This collaboration occurs through specialized applications utilizing client-server functionality and adhering to their own software protocol. The relationship between an IoT device and the ERATOSTHENES infrastructure can be likened to a secure line, ensuring secure authentication solely for enrolled devices. To maintain system security, the legitimate enrollment of a device occurs during its production stage, guaranteeing its

initial state. By employing hardware-specific applications tailored to each device, the system introduces a countermeasure against the usage of counterfeit applications during device authentication, as well as the replication of the device.

2.6 Trusted Execution Environment

The ongoing development of the TEE (Trusted Execution Environment) layer encompasses various device components. These components consist of an IDM (Identity Management) client, which facilitates the collection and management of identities and cryptography. Additionally, there is a data protector that supports backup and recovery mechanisms. Another crucial component is the trust agent, responsible for interacting with the trust and reputation of the devices. Lastly, the PUF client communicates with the authentication server.

By establishing a secure and isolated execution zone within a processor, the Trusted Execution Environment (TEE) plays a critical role in upholding the confidentiality and integrity of both deployed data and code. This robust security infrastructure enables the creation of a root-of-trust, ensuring the availability of essential security features even in the presence of untrusted applications. The TEE's capabilities span across the entire software lifecycle, providing a continuous layer of protection.

Within the ERATOSTHENES project, a primary objective is to tackle the initial challenge of defining a concise yet comprehensive set of trusted computing primitives. These primitives serve as the fundamental building blocks for establishing a trusted execution environment. By carefully crafting this minimal but essential set, ERATOSTHENES aims to provide a solid foundation for secure computing operations.

Furthermore, a significant focus of the project lies in simplifying the utilization of trusted computing. To achieve this, ERATOSTHENES seeks to unify security middleware, streamlining the integration and implementation of trusted computing technologies. This unification effort aims to reduce complexity and enhance accessibility, making trusted computing more practical and user-friendly for developers and system administrators.

3 SYSTEM VALIDATION AND REFERENCE DEPLOYMENTS

The system is undergoing an end-to-end integration phase, where all components are being integrated into a cohesive and robust component with appropriate interfaces and communications between its building blocks, following the system architecture. The ERATOSTHENES project will showcase its technical components through three industry-specific pilots. These pilots serve as practical demonstrations to validate the technical and operational effectiveness of the ERATOSTHENES solution.

The initial deployment and pilot of the ERATOSTHENES project will focus on vehicle-to-vehicle (V2V) interaction within an environment. Two primary use cases will be explored, aiming to standardize cybersecurity and software update processes. The deployment will showcase a scenario demonstrating the interaction between vehicles and infrastructure devices, highlighting the challenges associated with trust in V2V and V2I communication during software updates. Through this demonstration, the ERATOSTHENES project aims to exhibit how its developed technologies can effectively detect network misbehaviors, identify potential malicious actors, and demonstrate resilience in the face of cyber-attacks. The pilot will emphasize the project's ability to address cybersecurity concerns and ensure the reliability and resilience of devices and networks [11].

The project's second pilot centers around Smart Health devices and concentrates on a remote patient monitoring system. This system aims to enable remote assistance and follow-up for patients managing chronic diseases such as diabetes, COPD, or Covid-19. By utilizing this system, patients can receive care, treatment, and foster self-care while remaining in the comfort of their own homes. Key to this pilot is the implementation of a Personal Health Gateway in each patient's

residence. This gateway serves as a crucial component responsible for gathering data from diverse medical sensors and transmitting it to the back-end Cloud services. This infrastructure enables seamless data collection and ensures that the patients' health information is securely transmitted for further analysis and monitoring [11].

The third pilot will specifically target the unique identification of devices within an industrial network, considering the dynamic and heterogeneous nature of such networks. This pilot, known as the Industry 4.0 I (disposable IDs) pilot, aims to enhance the security of connected devices, data transfer services, and analytics applications. At the heart of this pilot is the generation of secure disposable IDs for IoT devices. This process will utilize a combination of Physical Unclonable Functions (PUF) and Distributed Ledger Technology (DLT). Each generated ID will act as a distinctive fingerprint for a connected device, ensuring its unique identification within the network. By implementing this innovative approach, the pilot will contribute to bolstering the overall security framework of the industrial network, providing a robust means of device identification and enhancing data protection and trustworthiness [11].

The validation of the components and the integrated solution will follow an iterative approach in parallel to development cycles as shown in the diagram below.

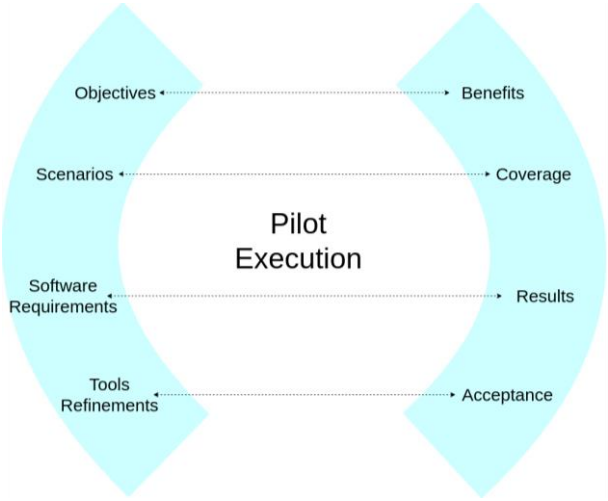

Figure 3: ERATOSTHENES Pilots and Validation Approach

4 CURRENT STATUS AND NEXT STEPS

The project is currently through an integration stage incorporating all major system components into a cohesive deployment as a proof of concept in the first pilots (automotive). This is supporting the consortium to provide a first deployment of the solution into a realistic environment able to support different interfaces, data exchanges and also bring to light any integration blocking points that need to be carefully considered at initial steps. The project is in the meantime carefully studying and analyzing deployment details for the other two pilots that will begin shortly in the next months. In parallel a second version of all components is being produced based on the technical feedback received from the pilot deployments.

5 ACKNOWLEDGEMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101020416. The authors acknowledge the research outcomes of this publication belonging to the ERATOSTHENES (101020416) project consortium.

6 REFERENCES

[1] ERATOSTHENES – D1.1 - Research Agenda, IoT threat landscape and security challenges, December 2021.

[2] K. Loupos - INTEGRATED SOLUTION FOR PRIVACY AND SECURITY OF IOT DEVICES IN CRITICAL INFRASTRUCTURES, Critical Infrastructure Protection and Resilience Europe (CIPRE 2020), 6-8 Oct. 2020, Bucharest, Romania.

[3] [47] - K. Loupos, A. Papageorgiou, T. Krousarlis, A. Mygiakis, C. Skoufis, S. Christofi, V. Hadjioannou, K. Zavitsas, S. Zemouri , M. Kacmajor, A. Battaglia, A. Chiappetta, J. Cavallo, G. Theofilis, H. Avgoustidis, V. Kalompatsos, B. Starynkevitch, F. Vedrine, G. Yvette, - INTEGRATED SOLUTION FOR INDUSTRIAL IOT DATA SECURITY - THE CHARIOT SOLUTION, ECLIPSE SAM IoT 2020, Security, Artificial Intelligence and Modelling for the next generation Internet of Things, 17-18 September, 2020.

[4] H. Navis, K. Loupos - ConSenseIoT: A CONSENSUS ALGORITHM FOR SECURE AND SCALABLE BLOCKCHAIN IN THE IOT CONTEXT, 4th Workshop on Internet of Things Security and Privacy (WISP), Global IoT Summit 2022, Dublin, June 202, doi: 10.1145/3538969.3543811.

[5] K. Loupos, C. Kalogirou, H. Niavis, A. F. Skarmeta, E. Torroglosa-Garcia, A. Palomares, H. Song, P.E. Brun, F. Giampaolo, D. V. Landuyt, S. Michiels, B. Podgorelec, C. Xenakis, M. Bampatsikos, K. Krilakis - A HOLISTIC APPROACH FOR IOT NETWORKS' IDENTITY AND TRUST MANAGEMENT - THE ERATOSTHENES PROJECT, 4th Workshop on Internet of Things Security and Privacy (WISP), Global IoT Summit 2022, Dublin, June 2022.

[6] K. Loupos, B. Caglayan, A. Papageorgiou, B. Starynkevitch, F. Vedrine, C. Skoufis, S. Christofi, B. Karakostas, A. Mygiakis, G. Theofilis, A. Chiappetta, H. Avgoustidis, George Boulougouris - COGNITION ENABLED IOT PLATFORM FOR INDUSTRIAL IOT SAFETY, SECURITY AND PRIVACY – THE CHARIOT PROJECT, IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE XPLORE, 11-13 September 2019, Limassol, Cyprus, DOI: 10.1109/CAMAD.2019.8858488.

[7] [44] – K. Loupos, A. Papageorgiou, A. Mygiakis, B. Caglayan, B. Karakostas, T. Krousarlis, F. Vedrine, C. Skoufis, S. Christofi, G. Theofilis, H. Avgoustidis, G. Boulougouris, A. Battaglia, M. Villiani - COGNITIVE PLATFORM FOR INDUSTRIAL IOT SYSTEM SECURITY, SAFETY AND PRIVACY, Embedded World 2020 Conference and Exhibition, 25 - 27 Feb. 2020, Nuremberg, Germany.

[8] ERATOSTHENES – D1.3 Preliminary ERATOSTHENES Architecture, March 2022.

[9] ERATOSTHENES – D2.1 - Trust Broker Mechanism, December 2022.

[10] ERATOSTHENES – D4.1 - D4.1 DLT-based Trust Frameworkt, April 2023.

[11] ERATOSTHENES – D5.2 - Preparatory Activities and Deployment Planning, December 2022.