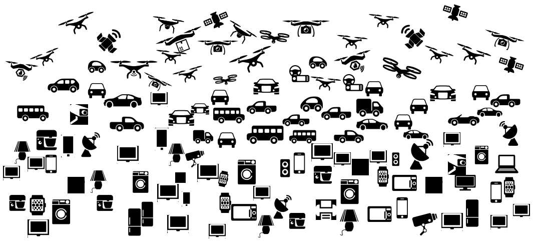
DINET: DNS-Based Trust, Security, Accountability, and Privacy for IoT



Project type: Research and Innovation Action

Horizon 2020 Cybersecurity Call SU-ICT-02-2020

Building blocks for resilience in evolving ICT systems

List of participants:

Part. no.	Short name	Participant organisation name	Country
1	INP	Institut Polytechnique de Grenoble (coordinator)	France
2	AFNIC	Association française pour le nommage Internet en coopération	France
3	NASK	Naukowa i Akademicka Sieć Komputerowa, Państwowy Instytut Badawczy	Poland
4	SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands
5	GANDI	GANDI	France
6	FUB	Freie Universität Berlin	Germany
7	INSA	Institut National de Sciences Appliquées de Lyon	France
8	UZH	Universität Zürich	Switzerland
9	WUT	Warsaw University of Technology	Poland
10	AIRBUS	AIRBUS CyberSecurity SAS	France
11	ODINS	Odin Solutions SL	Spain
12	SIEMENS	Siemens Aktiengesellschaft	Germany
13	SIGNIFY	Signify Netherlands B.V.	Netherlands
14	TTI	The Things Industries	Netherlands

The 'S' in IoT is for security.

— Tim Kadlec

1 Excellence

A recent NIST report[1] recommends to address **cybersecurity and privacy risks for IoT devices** with three high-level **mitigation goals**: i) protect device security (prevent a device from conducting attacks), ii) protect data security (guarantee confidentiality, integrity, and/or availability of data), and iii) protect privacy (prevent disclosure of personally identifiable information).

In line with these objectives, the DINET project proposes to **design and implement a framework for trust, security, accountability, and privacy based on advanced DNS (Domain Name System) functionalities**. The main idea is to **replace the trust and security schemes based on the traditional PKI** with a **novel approach that relies on the DNS infrastructure** and builds all the required functionalities upon DNS. DNS brings the advantage of a **single trust anchor** with **lightweight authentication schemes** suitable for **constrained IoT devices** and easily **automated for large-scale IoT deployments**. The traditional use of PKI does not fit constrained IoT devices: the required computing power, storage for the chain of trust, bandwidth for sending and receiving certificates, encrypted data using large block ciphers and signatures, as well as obtaining revocation lists, is technically and economically infeasible for this class of devices.

1.1 Objectives

The project aims at achieving the following **key objectives**:

1. Design and implement a **DNS-based architecture for trusted, secure, accountable, transparent, and privacy preserving IoT**.
2. Design and implement **support for DNS-based secure and trusted communication**.
3. Design and implement **support for secure on-boarding of IoT devices**.
4. Design and develop **schemes for leakless privacy**.
5. **analyze, evaluate, validate the architecture and experiment in Use Cases**.
6. **Contribute to standards and promote the project results for wide adoption**.

The project will focus on the following aspects:

- DINET will **adapt DNS based security solutions to constrained IoT devices** based on ongoing standardization work at IETF,
- DINET will build on DNS-based trust to develop **secure IoT device bootstrapping** with limited out of band configuration, accountability, trust, privacy, and discovery of resources associated with IoT devices; all solutions will be based on open standards.
- the project will **use Artificial Intelligence (AI) following the Explainable AI approach** to achieve user-centric solutions,
- DINET will develop **tools and support for proposed security schemes** so that they can be directly used by EU vendors,
- DINET will take advantage of the existing DNS infrastructure, which enables **adoption across many heterogeneous IoT platforms**, making the solutions **affordable and deployable** within the Time to Market period.

Providing **security solutions for IoT based on the DNS infrastructure** is gaining momentum around the world. A multistakeholder Canadian initiative is working on a Secure IoT Registry[2] based on DNS that allows **IoT devices to seamlessly and securely work** between any manufacturer, owner, service provider, and network operator.

[1] Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. NISTIR 8228.

[2] CIRA (Canadian DNS Registry) Secure IoT Registry, August 2019.

ICANN, an important stakeholder in the Internet argues that "*DNS provides functions and data that can help make the IoT more secure, stable, and transparent, which is critical given the IoT's interaction with the physical world*"[3]

The report of the Strategic forum for important projects of Common European Interest[4] suggests to "*Ensure the establishment of a DNS fit for the next Internet generation, including harmonisation of security requirements for the existing DNS infrastructure and R&D and standardisation efforts towards the design of a European DNS fit for the next Internet generation*".

The DINET vision follows a similar direction and results from the IoT security needs identified by major European IoT players (Siemens, Airbus Cybersecurity, and Signify) backed up by the advanced functionalities supported by Internet Registries (AFNIC, NASK, and SIDN) managing the Internet namespace and operations for France, Poland, and Netherlands, an Internet name Registrar in contact with end-users, one of the largest IoT community network operators, and major universities in Europe doing long term research on IoT security and privacy.

We discuss the details of the objectives and measures of success below.

Objective 1. Design and implement a DNS-based architecture for trusted, secure, accountable, transparent, and privacy preserving IoT.

We will start with the definition of the **requirements for security and privacy** in the context of **commodity and industrial IoT devices** as well as the threats that the devices may face. The project will identify risks that IoT devices may cause when enrolled in current networks and the requirements for their mitigation. We will consider the **lifecycle** of IoT devices and identify the impact on the DNS architecture in terms of **device ownership and provisioning** through DNS.

The architecture based on open **IETF DNS standards** and minimal extensions will rely on schemes for low-level identifiers based on **physical device fingerprinting** and **Physical Unclonable Functions (PUFs)**. We will also define **self-certifying names**, derived from a public key, which provide a means for verification based on cryptographic signatures. To this extent, entities can prove they have a given name without relying on any global trusted authority. This kind of names will enable **accountability**—providing verifiable names to all entities in the system so the infrastructure will be able to establish what an entity did and how. Finally, the project will consider **semantic names** that represent various features such as device type, localization, data format, and others defined by specific applications. The integration of all these features makes the proposed architecture novel, cost-effective, and quickly deployable in operational IoT environments.

Success Measure for Objective 1: The thrust of this objective is the design of the architecture that takes into account IoT device and network constraint requirements for security, scalability, trust, accountability, and privacy. Real IoT network Use-Cases in Objective 5 will validate the proposed architecture.

Objective 2. Design and implement support for DNS-based secure and trusted communication.

In this objective, we will design and develop a **generic trust support** for IoT based on the DNS infrastructure focusing on DNS security extension such as DNSSEC[5] (DNS Security Extensions) and DANE[6] (DNS-Based Authentication of Named Entities) TLSA resource records. The DNS security extensions cannot be re-used in IoT as is since IoT devices and networks do not have enough computing power or bandwidth, so there is a need to adapt them for IoT requirements.

The project will design and develop all the required tools and support for the use in real IoT scenarios. For this goal, we need to design and develop schemes for **managing IoT identifiers and names** as well as **keys and their TLSA signatures** (i.e., registration, revocation). Finally, we will also design and develop a blockchain for **trustless bootstrapping** of highly-constrained IoT devices or as a backup for resilient operation.

[3] "The DNS and the Internet of Things: Opportunities, Risks, and Challenges", ICANN SSAC report SAC105, June 2019

[4] Recommendations of the Strategic Forum for Important Projects of Common European Commission, EC, November 2019.

[5] RFC 4033, DNS Security Introduction and Requirements.

[6] RFC 6698, DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA.

Success Measure for Objective 2: The thrust of this objective is to provide the trust anchor based on DNS for IoT devices, compress X.509 certificates (e.g., less than 150 bytes). We should be able to automate and generate the required cryptographic keys for a minimum batch of 100 devices at a time, and to be able to set up secure communications within a certain time lap (such as 5 seconds). The objective will be evaluated in Use Cases.

Objective 3. Design and implement support for secure on-boarding of IoT devices.

The project proposes to design a generic **authentication and authorization framework** based on scalable DNS naming and resolution schemes adapted for IoT devices. The framework will take into account heterogeneous identifiers of IoT devices and resolve names in a uniform way for various types of networks. The resolution scheme will build on the DNS infrastructure and extend its functions to fit the requirements of resource-constrained IoT networks. In particular, it will take into account **device constraints** in terms of limited memory, energy, and bandwidth, and scale up to billion devices.

We will define the process of dynamic secure accountable device **on-boarding/enrollment**. Based on an initial Pre-Shared Key (PSK), a device can contact an EST (Enrollment over Secure Transport) server to obtain an owner certificate to replace PSK. Tools for **compressing X.509 certificates** will enable storing them on constrained IoT devices. Then, the device can autonomously enroll using the BRSKI (Bootstrapping Remote Secure Key Infrastructure) process. We will propose automatic generation of MUD (Manufacturer Usage Description)[7] descriptors based on the observation of the device traffic so we can lock down and rigorously verify the behavior of IoT devices in any operating environment. To provide **inward device protection**, the project will design protection schemes against **intrusions and Distributed Denial-of-Service (DDoS) attacks** based on Explainable AI (Artificial Intelligence).

Success Measure for Objective 3: The thrust of this objective is to ensure support for secure device on-boarding as well as inward and outward protection of devices and networks. Any IoT device should be able to enroll in a IoT network to establish secure communication based on the proposed mechanisms. The Objective will be evaluated in Use Cases.

Objective 4. Design and develop schemes for leakless privacy.

IoT devices may reveal sensitive information on individuals. The project proposes to develop new methods for **improving privacy** in networks with IoT devices. First, our schemes for authentication enable devices to encrypt all communications, which eliminates the risk of eavesdropping. DoT (DNS over TLS[8]) and DoH (DNS over HTTPS[9]) improve privacy because communication between the client and the resolver is encrypted and the resolver authenticates itself to the client. However, it is not sufficient—DoT and DoH do not protect the identity of the client nor hides the queried domain from the recursive resolver. It does not encrypt communication from the resolver to the authoritative name server. We propose to design and develop schemes for **hiding sources of queries** by means of **forwarding resolvers**. The DNS resolver should only know the client IP address but not the DNS query and the authoritative name server should know the queried domain but not the client IP address. The scheme should ensure private communication within the entire resolution path. We will also explore hiding IoT device identifiers through **ephemeral identities**. We also see MUD descriptions as a means for **privacy reinforcement** that will assist the process of reporting devices collecting personal data. The idea is to automate the declaration of such devices to satisfy the EU General Data Protection Regulation (GDPR).

Success Measure for Objective 4: The thrust of this objective is to ensure support for privacy of IoT devices. As our approach builds on DNS, we need to provide schemes for protecting sensitive information in DNS communications. The success measure will be the validation of the developed schemes in the three Use Cases.

Objective 5. Analyze, evaluate, validate the architecture and experiment in Use Cases.

The project will deliver a set of tools, libraries, and APIs that enable: i) IoT devices to operate in a secure

[7] RFC 8520, Manufacturer Usage Description Specification.

[8] RFC 7858, Specification for DNS over Transport Layer Security (TLS).

[9] RFC 8484, DNS Queries over HTTPS (DoH).

way and ii) domain name Registrars and TLD Registries to provision the required information in the DNS system. During the initial phase of the project, we will develop and evaluate **early prototypes** of the required functionalities: tools for managing IoT Identifiers and names, keys and certificates, protocols for secure device bootstrapping, MUD generation, and tools for inward and outward device protection. In the final phase of the project, we will **analyze the security and privacy** properties of the overall architecture and the developed tools, and experiment with possible attacks on IoT devices and threats that IoT devices may cause in their networking environments. We will also evaluate performance, scalability, and resilience of the proposed schemes. The project will validate the results in several **Use Cases**:

1. Secure IoT **device enrollment** in IoT networks: how to support autonomous enrollment in the network by an IoT device based on the developed DNS security architecture. We will consider two different types of networks: LoRa with TTN (The Things Network) and IEEE 802.15.4.
2. Secure **deployment of RIOT**[10] **IoT devices**.
3. Secure **management of Industrial IoT devices**.

Success Measure for Objective 5: The thrust of this objective is to validate the proposed architecture, the schemes, and tools developed in the project in real-world Use Cases. The success measures are two-fold:

- The proposed solutions should seamlessly integrate legacy or new IoT infrastructures without major modifications. They should be operationally feasible and do not degrade existing performance nor scalability.
- The proposed solutions should be successfully deployed in three Use Cases in real-world environments.

Objective 6. Contribute to standards and promote the project results for wide adoption.

The project aims at specifying the extensions to existing standards and defining the guidelines for their use and deployments. Contributions to open standards and providing the required tools and support for immediate deployment will promote the project results and enable their wide adoption by all stakeholders. The participating TLD registries will provide support for creating the required DNS resource records so that IoT device owners will be able to leverage the trust embedded in the DNS infrastructure. We will also promote the project outcome at the general public with tools for protecting IoT devices on home networks.

Success Measure for Objective 6: The thrust of this objective is to ensure wide adoption of the project results through contribution to standards and providing open source libraries and tools. The success measure will be the submission input documents (Internet drafts, RFCs, etc.) to standardization fora as well as delivery of open source software.

1.2 Relation to the Work Programme

DINET addresses the strategic Objective SU-ICT-02-2020: *"Building blocks for resilience in evolving ICT systems"*. In line with the objective, we propose to provide the architecture and technological foundations based on open standards for harmonizing the security infrastructure across heterogeneous IoT domains. We build on the proposed security infrastructure mechanism and provide support and tools to enhance trust, privacy, accountability, and transparency, which targets subtopic: *"c) Designing and developing privacy-friendly and secure software and hardware"*.

[10] RIOT: The Friendly Operating System for the Internet of Things, https://riot-os.org.

Table 1.1 below presents the specific challenges of the call and explains how DINET will address them.

H2020 Work Programme Topics	**How DINET addresses the specific challenge**
Challenges of SU-ICT-02-2020	
Algorithms, software and hardware systems must be designed having security, privacy, data protection, fault tolerance and accountability in mind from their **design phase** in a measurable manner, taking into account future-proof, advanced cryptographic means.	This aspect is one of the main objectives of DINET, since our focus is on **designing** an architecture that can be used as a platform to add building blocks for security, privacy, data protection, fault tolerance, and accountability. It is important that the designed architecture should be used by EU stakeholders in a Time-to-Market period across IoT domains/applications and be scalable for billions of IoT devices. This is the reason we zeroed in on **the DNS architecture** that withstood the massive Internet evolution and still is used as the cornerstone of the Internet. The security infrastructure based on DNS and extended mechanisms (AI algorithms, support tools, adapting existing standards, and proposing new standards) proposed in DINET architecture addresses the issues of IoT security, privacy, data protection, fault tolerance, and accountability in novel ways. The proposed security mechanisms adopt post-quantum cryptography algorithms for future-proof solutions.
To develop mechanisms that **measure** the performance of ICT systems with regards to cybersecurity and privacy.	DINET addresses this challenge with Explainable AI. Based on detected anomalies and descriptions provided by AI, the developed models will be able to automatically generate, in a dynamic manner, well-known security **measures**, which can be implemented even on constrained IoT devices.
(b) to enhance **control and trust** of the consumer of digital products and services with innovative tools aiming to ensure the **accountability** of the security and **privacy** levels in the algorithms, in the software, and ultimately in the ICT systems, products and services across the supply chain.	In addition to the DNS security protocols explained in detail in the Objectives section, **control and trust** are addressed by integrating the MUD, BRSKI IETF standards in the DNS infrastructure, which will enable secure bootstrapping of IoT devices to establish secure communications without out of band configurations. DINET will address accountability and transparency with mechanisms such as secure identifiers and self-certifying names that add the possibility of logging interactions with the DNS infrastructure to record evidence of system operation. The project will address specific issues of **privacy** with support for confidential communications, ephemeral identifiers to hide identities, and mechanisms for preserving privacy in DNS communications based on forwarding resolvers.
Specific challenges of Subtopic c)	
Innovative approaches to establish methods and tools for: (i) security and privacy requirements engineering (including **dynamic** threat modelling, **dynamic** attack trees, attack ontologies, **dynamic** taxonomies and **dynamic**, evidence based risk analysis).	DINET addresses the **dynamic** issue by automatic generation of MUD description of an IoT device based on the observation of the device regular traffic. In addition, the MUD model will be extended to provide higher expressiveness allowing to specify more refined security configurations. DINET will design and implement an SDN-based security framework that will host AI based detection algorithms to detect threats, attacks, and security issues that can be discovered **dynamically**, and efficiently mitigate them. The support and tools developed will be part of WP3.
Innovative approaches to establish methods and tools for: (ii) embedded algorithmic **accountability** (in order to monitor the security, **privacy** and **transparency** of the algorithms/software/systems/services).	The mechanism to address **accountability, security, and privacy** are explained in this tabular column above. The support and tools developed will be part of WP3 and WP4.

Innovative approaches to establish methods and tools for: (vi) **novel, secure and privacy-friendly IoT architectures enabling consistent trustworthy and accountable authentication, authorization and accounting services** across IoT devices/ecosystems with enhancement of Public Key Infrastructures (PKIs) aiming to **support PKI services** (e.g. registration, revocation) for IoT devices.	The basic solution for **secure and privacy-friendly IoT architectures enabling consistent trustworthy and accountable authentication, authorization and accounting services** proposed by DINET is to **replace conventional PKI with the DNS infrastructure**. All work packages except WP1 and WP7 concern the design and development of schemes, tools, and support. This approach builds on the experience of three Internet registries. Each of them have nearly 30 years of experience in the DNS industry managing millions of domain names, billions of DNS query resolutions per day, managing registration of millions of end-users, revocation of DNSSEC keys. In addition, the name registrar (GANDI) has direct contact with domain owners, which is a complimentary know-how. The tools and methods already used in their operational infrastructure and their vast experience on managing the real-time operational DNS system enables our consortium to rapidly deploy a trust infrastructure based on DNS and provide support and tools for IoT.

Table 1.1: Relation of DINET to the work programme specific challenges.

1.3 Concept and Methodology

1.3.1 Concept – Background and Drivers

Security. IoT presents a number of security risks to both consumers and businesses. IoT devices generally lack sufficient **built-in security** to protect themselves from causing or becoming a source of harm. Security risks include compromising the end-device hardware, cloning or substitution of devices, tampering with the software in the end-device, compromising the communication in IoT networks like eavesdropping, and **Man-in-the-Middle (MitM)** attacks. Poorly secured IoT devices and services can become entry points for cyberattacks, compromising sensitive data, weaponization, and threatening the safety of individual users. IoT botnets can launch large-scale **DDoS** attacks, which are one of the largest risks to many service providers on the Internet. For instance, the Mirai[11] botnet exploited weak or non-existent passwords to gain control of hundreds of thousands IoT devices to launch DDoS attacks on important Internet services. Three waves of Mirai attacks disrupted high-profile websites including Amazon, GitHub, Slack, Visa, and HBO. The Mirai example shows that other commodity devices may follow a similar path.

Constrained IoT devices. Most of low-end IoT devices are highly constrained: they have **limited memory, limited processing capacity, and limited power**. Managing Public Key security mechanisms as deployed in the Internet on such devices and transferring them over **bandwidth-constrained IoT networks** is too heavy and therefore represents a major challenge.

Secure bootstrapping. Bootstrapping trust when an IoT device connects to the network and starts to operate is a security concern. The device is usually installed with an identifier and a **Pre-Shared Key (PSK)** to contact some servers on the Internet associated with the IoT device for on-boarding. PSK needs to be shared between different stakeholders in the supply chain—from the Original Equipment Manufacturer (OEM) to the device owner, the network server provider, the application server provider, etc. PSK is shared many times in an insecure manner such as printing the keys on the back of devices, sending via mail or printing on the invoice. There have been reports of **massive breaches**[12] of PSK provisioning systems and they are vulnerable to passive pervasive monitoring. There are secure ways in which PSK could be shared, but they rely on proprietary cloud services or secure key elements, which could increase the cost of IoT services.

Privacy. Data and meta-data generated by IoT devices can reveal **personal information on individuals**. A combination of data from different IoT sources might create new knowledge on individuals that might not be revealed by separately examining the underlying data sets. The recently adopted EU General Data Protection Regulation

[11] Antonakakis et al. Understanding the Mirai Botnet, *In Proc. of the USENIX Security Symposium*, August 2017.

[12] Requirements for a Lightweight AKE for OSCORE, Internet draft

(GDPR) mandates data protection by design and default, which also applies to IoT. The upcoming e-Privacy regulation, focusing on electronic communications, will reassert those obligations. Unfortunately, Privacy by Design (PbD) is not even considered in most of IoT products and service offers.

Accountability and transparency. Accountability refers to the policies and procedures that a data processing organization puts in place to demonstrate to itself (internal accountability) or to others outside the organization (external accountability) that its data processing operations comply with the requirements of data protection legislation [1]. The most important aspect of accountability is **transparency** that relies on making the system “observable and reportable”—it consists of making actions reportable to others so that they can see what is done with data and by whom.

Autonomous management. Most of devices **do not have an interface for human interaction**. The large scale of IoT means that we cannot longer rely on **traditional management**—devices need to operate in an autonomous way without human intervention, including their configuration and security management. Thus, the critical requirement for developing IoT security solutions is the efficient operation on constrained devices and **automated operation** for large-scale deployments.

Trust. As indicated above, one of the main goals of IoT is to give autonomy to the end-devices and to enable automated decisions. Decisions taken automatically by devices or applications, based on a huge set of sensed data might not be transparent to the data subjects and therefore may create the sense of loss of control. Moreover, these decisions will be difficult to understand for individuals as information collected via sensors is often only subconsciously recognized by individuals.

Heterogeneity and Interoperability. The essential aspect of IoT concerns heterogeneous types of devices and communication networks with different requirements thus creating closed **independent silos** and leading to **interoperability issues**. Past efforts for creating a single architecture to provide security, privacy, and trust in the heterogeneous IoT eco-system did not succeed.

Cost. Current security mechanisms in IoT are based on **proprietary closed solutions**, which translates to an **increased cost** for end users and businesses. Weak IoT security has its roots in economic factors because of the tension between costs and security objectives. Including effective security and privacy in IoT costs money and slows down the product development process. In addition, security requires specialized skills and experience that manufacturers may not have at hand, requiring either new stable or external consulting, both of which increase costs. The proposed IoT security solutions should not incur much additional costs that would hinder innovation and evolution in the IoT market.

Deployability. Most of the existing IoT security and data protection solutions are **not generic**. Proposed approaches will have to strike a balance between improving security, trust, and privacy, and allowing scope for **innovation and evolution** within the market. Generic open security standards like those defined for the Internet should be **adapted for IoT** to satisfy the resource-constrained requirements, thus reducing costs. Finally, the provided solutions should be immediately deployable into **legacy or new** IoT technologies.

1.3.2 Concept – Architectural and Technical Vision

Despite significant recent advances in IoT standardization, there are still questions left in terms of a generic end-to-end vision for IoT security. When we look at the state-of-the-art, such as previous EU research and innovation projects, none of them have proposed a holistic approach of providing an end-to-end solution that is operationally feasible and immediately deployable. DINET identifies and addresses those issues.

Why DNS infrastructure? DNS has been an **operationally viable and highly distributed infrastructure**, the cornerstone of the Internet since its origins. The DNS infrastructure is:

scalable: several facts showing DNS scalability: it scaled from some hundreds of domains to around 350 million domains nowadays[13]. DNS is a distributed network database running across millions of nodes on the Internet and trillions of DNS requests are processed by these nodes in a day.

resilient: The work program main focus is on "Building blocks for resilience in evolving ICT systems". DNS is remarkably resilient for its current size and scale with very few outages. Thanks to use of anycast for DNS servers and other redundancy layers, the DNS infrastructure can handle even very heavy DDoS attacks and continue to work without visible effects to the clients.

user centric: DNS information is publicly available and managed in a distributed manner, thus providing control to the end-users.

trust anchor: With the DNSSEC and DANE security extensions, DNS provides provides trust in a similar way as a conventional PKI.

capacity to evolve: DNS has been used by different IoT networks for resolving their identifiers to the corresponding resource in the Internet and for service discovery of IoT devices, which is being evaluated in the IETF DNS-SD and Homenet WG. Many DNS record types can be used to store more complex data in DNS, thus enabling new protocols to seamlessly interact with existing DNS servers.

Most of the security mechanisms currently used in IoT are based on proprietary closed solutions: since IoT devices and networks are heterogeneous by nature, they have heterogeneous constraints and security requirements. Current security schemes are specifically tailored to a particular IoT technology and cannot be applied to the whole IoT industry. Our approach is to design a generic architecture to build the required technical solutions for security, trust, privacy, accountability, and transparency based on the DNS Infrastructure in addition to using established and emerging open standards. The proposed architecture will protect the device itself, the data on the device and the service offered by the device. We explain below in detail how we address the issues discussed in the previous subsection as part of the DINET project.

DNS for Trust. Authentication of IoT devices requires trust anchors similar to what most Internet browsers provide with the root certificates of over 1000 Certification Authorities (CA) trusted by default. The root certificates allow the validation of server certificates when establishing HTTPS/TLS sessions so that a client can trust the server. Reuse of the conventional PKI for IoT devices presents some drawbacks: i) the cost of certificates and ii) management burden for individual owners of IoT devices (storing root CA certificates, certificate revocation).

Our project proposes to take advantage of the **DNS infrastructure as the trust anchor** for IoT devices. Figure 1 presents the example of the chains of trust for a wristwatch X.509 certificate—left: a conventional PKI with recursive validation of signatures until the root CA trusted by a client. Right: the device owner creates a self-signed certificate installed on the device and placed in the TLSA record associated with `alice.priv`, the name for her domain. Domain records can be trusted because they are signed with zone signing keys up to the root zone trusted by default. The scheme enables validation of a certificate emitted by an IoT device by comparing it with a TLSA record. Note that an IoT device only needs to have the root DNS key to bootstrap trust and validate the integrity of DNS records.

Constrained IoT devices. We cannot directly reuse the existing security mechanisms of the Internet because IoT devices do not have enough computing power or network bandwidth, so we need to adapt them or propose the required extensions. we will consider the problem of **certificate management on constrained devices** and networks (e.g., LoRaWAN with the maximum frame size of 51 bytes or 222 bytes for lower spreading factors). In the Internet, the size of an X.509 certificate and its corresponding certificate chain is a few kilobytes. For authentication and authorization in an IoT constrained environment, an IoT device needs to store and transmit a compressed X.509 certificate with a much smaller size. Towards this goal, we propose to explore **compressing X.509 certificates** with IETF standards such as Concise Binary Object Representation (CBOR) using CBOR Object Signing and Encryption (COSE) and Ephemeral Diffie-Hellman Over COSE (EDHOC). When an IoT device with a compressed X.509 certificate initiates a TLS handshake, the certificate is trusted based on the DANE TLSA record stored in DNS and because DNSSEC guarantees data integrity, the trust chain for the certificate can be validated and results in establishing an encrypted authenticated communication channel.

[13] The Verisign Domain Name Industry Brief, Verisign, 2019.

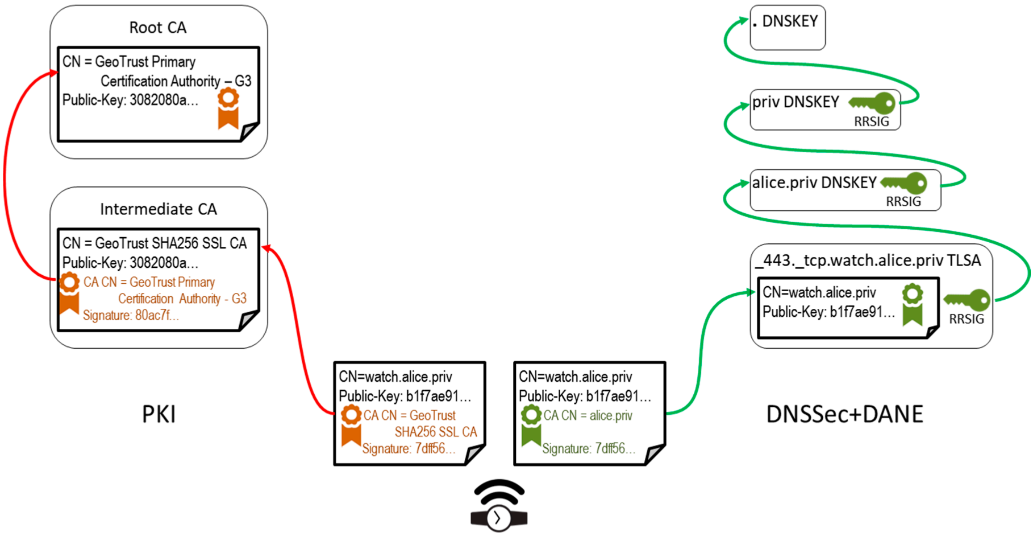


Figure 1: DNSSEC and DANE (right) as a replacement for a traditional PKI (left).

Secure bootstrapping. During the enrollment process, a device is accepted in the network and obtains a session key to perform a secure communication. There are two possible ways for that to happen. One is using a PSK and another is using a Public Key. Both of them can take advantage of DNS and we will explore both cases in the project.

A simple process consists of using an EST (Enrollment over Secure Transport) server that a device can discover with a DNS SD query and a DNSSEC signed response. The device authenticates with PSK so that the EST server can create a certificate, insert the corresponding TLSA record in DNS, and provide the device with the certificate over HTTPS.

Another approach follows the BRSKI (Bootstrapping Remote Secure Key Infrastructure) process that involves a Registrar server on the access network and a Manufacturer Authorized Signing Authority (MASA) service. The audit token from the end-device contains the domain public key material as provided to the MASA service. Then, the end-device uses DNS to establish secure bootstrapping for the IoT end-device.

In some cases, a device needs to bootstrap trust without any root of trust such as the root DNS key. DINET proposes to explore a **globally shared ledger—a blockchain** as a means for bootstraping trust. When an IoT device wants to join the network, it needs to go through the process of initial boostrapping: it connects to a partially trusted and reputable set of seed nodes or the nodes which names come from DNS entries that serve as initial entrypoints to the network. After successfully concluding the bootstrapping phase, the blockchain nodes can verify the propagated information (such as blocks and transactions) and verify the data without relying on any other trusted third parties. Therefore, unlike in a PKI, a peer does not need to get its address authenticated by any other entity or a CA. Peer nodes generate transactions that refer to blockchain addresses and each peer collects transactions into a linear chain of blocks, a distributed and tamper-resistant log of all transactions, leading to transaction non-repudiation and the ability to retrace the history of any transaction. We can use such a structure to publish critical information such as the association of the public DNSKEY with a given domain name (the root DNS key is one of such keys).

Outward and inward device protection. When a device is enrolled in a network, we need to envision means for the outward protection of the network from possible attacks from the device (e.g., DDoS). One way to accomplish this goal is through a **Manufacturer Usage Description (MUD)**—an IETF standard for describing the expected network behavior of the device in terms of what domain names and protocols it will use. Security systems in edge networks can whitelist the regular behavior based on MUD and block all other traffic such as outbound DDoS. The project will propose **automatic generation of MUD descriptors** based on the observation of the device regular traffic to create a MUD descriptor automatically.

An enrolled IoT device may become the target of external attacks such as the Mirai botnet. Once installed on a device, malware can impact the privacy and security of users by exposing private data, tracking people, controlling smart systems, or causing other devices to behave in unwanted ways. We propose to design **protection schemes against intrusion** based on detection of anomaly in the observed device behavior. The proposed security solutions will be empowered using Explainable AI (Artificial Intelligence) techniques. Explainable AI tries to explain how machine learning models are created and how decisions or predictions are made. By looking at inner parts of the algorithms, Explainable AI aims at giving the rationale behind the sequence of steps leading to the final decision, e.g., in the context of anomaly detection Explainable AI allows to visualize and verbalize what rules were used to classify a given data point as an outlier (anomaly). The benefit from state-of-the-art machine learning models becomes especially important in the context of multi-layered neural networks that are often built of millions of neural network connections combined with non-linear activation functions. It is therefore extraordinarily difficult to demystify their behavior and rationalize the decisions made.

Although several attempts have been made to address this problem in the context of visual data, such as images or videos [2], [3], [4], the issue remains unsolved for multidimensional alphanumeric data, such as the MUD standard information. By developing new methods for visualizing the decisions of the anomaly detection mechanism, we see the potential of exploring new Explainable AI concepts, as well as improving already existing ones. In fact, based on detected anomalies and descriptions provided by AI, the developed system will be able to automatically generate, in a dynamic manner, well-known security measures (e.g., whitelisting, blacklisting, signatures, etc.), which can be implemented even on constrained IoT devices.

For both cases, i.e., for outward and inward IoT devices protection, a distributed Intrusion Detection/Prevention System (ID/PS) based on Software Defined Networking (SDN) technology will be developed, which has been recently proved to be suitable for such purposes [5, 6]. It will consist of probes at the edge of the networks and security monitoring center located within the core of the DINET solution. The probes will collect information about the incoming/outgoing network traffic and send them to the security monitoring center where the security policies will be enforced, i.e., MUD descriptors will be evaluated, security incidents will be detected, and countermeasures will be invoked (e.g., temporary blockage of suspicious devices and sending security alerts to their users/administrators).

Autonomous management. MUD descriptions described earlier can assist organizations in the process of reporting devices collecting personal data, which automates the declaration of such devices to satisfy the EU GDPR regulation. Access control through authorizations attached to operational identities leads to better data supervision and provides a means to collect evidence, manage risk, and help in auditing.

Privacy. In the project, we address the privacy issues related to IoT devices with several different mechanisms. The elements of the architecture described so far guarantee the most important property of communications from the point of view of privacy: they are established between **authenticated entities and protected from eavesdropping** by strong encryption so that no personal data may leak from IoT devices.

Even if we provide the mechanisms to avoid information leaks, we will also propose to take advantage of AI systems to classify the sensitivity of data from a privacy point of view to identify pieces of data that would leak personal information. We will develop a machine learning algorithm that can identify individuals by eavesdropping their communication and then use Explainable AI models to locate parts of the communication linked to the leakage. The algorithm will allow us to further improve privacy protection mechanisms by focusing our efforts on improving the quality of information hiding in the specific areas of the packets that are used by AI to make a decision. Our work will be inspired by the Generative Adversarial Privacy approach [7], further extended to medical data processing [8]. More precisely, we will use the Siamese architecture combined with a generative model based on the GAN architecture [9] to identify the parts of the communication that contain data classified as private, i.e., allowing the eavesdropping party to identify the identity of the information source. Furthermore, we will develop a mechanism inspired by Explainable AI to visualize the private information parts.

There is a **tension between privacy and providing strong identities** for authentication. In some cases, device owners or users may want to remain anonymous and the disclosure of unique identifiers, keys, or configuration parameters may lead to identification of persons. These concerns are even more important in the case of physical fingerprints because a device cannot change the characteristics that served to derive its identifier. Such identifiers open the possibility to track devices across time and space without the consent of the user or to derive some personal data from the behavior of a device. We propose to explore an approach based on **multiple ephemeral identifiers** and names (pseudonyms) to preserve privacy while handling identities.

Recent DNS extensions allow IoT devices to authenticate resolvers and encrypt DNS traffic: DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) encrypt DNS messages between a DNS client and its resolver, thus hiding DNS queries and responses from an eventual intruder. However, the protocols do not hide the DNS queries from the

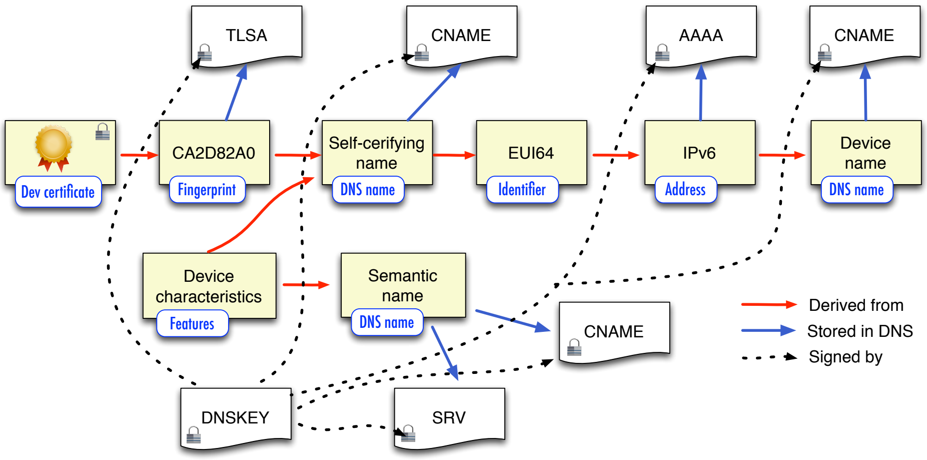


Figure 2: Proposed schemes for identifiers and names.

resolvers that may link the query to the source IP address to track or create user profiles. ObliviousDNS[14] [10] is a system to solve this issue. In Oblivious DNS, the client encrypts the queried domain with a session key and sends it to a resolver, which then forwards it to the authoritative name server for the specific `.odns` domain. The ODNS server decrypts the query and forwards it to the appropriate authoritative name server acting as a recursive resolver. The response to the query is then encrypted and sent back to the resolver which forwards it to the client, and because the result is encrypted using the session key, only the client can read the result. Such an operation decouples the knowledge of the client source IP address and the DNS query. The problem of ODNS is scalability because the scheme relies on the authoritative name server for the `.odns` domain. Some previous work [11, 12] proposed to use existing anonymising networks, like Tor, to improve the privacy of DNS, but it raises performance and privacy concerns.

We propose to design and develop a scheme involving **forwarding resolvers** in which a device encrypts its DNS queries, sends them over DoT or DoH to a forwarding resolver, which in turn relays the queries to the authoritative server of the target domain. This last server can decrypt the queried domain and proceeds with its resolution. In this way, the resolver does not know the queried domain, whereas the authoritative name server does not know the IP address of the device.

Accountability and transparency. The proposed architecture based on DNS integrates IoT **accountability** by enabling greater control and observability, enforcing confidentiality and privacy, and providing evidence on what occurred and those involved. It supports **transparency** since all DNS records are public and provided to any node requesting resolution. In addition to that, DINET addresses accountability and transparency by using **self-certified names and identifiers**.

An IoT device needs to have a static identifier generated by the device manufacturer and provisioned onto devices during manufacturing (serial number, MAC address, EUI64, PSK, etc.). It should be protected at the device level: it cannot be easily extracted and cloned by an attacker. A promising method for establishing low-level identifiers is **fingerprinting**. The idea is to passively or actively extract unique physical patterns from the device hardware. There are two families of the fingerprinting approach: signal-based fingerprinting and PUF (Physical Unclonable Function)-based identification. PUF is a primitive that derives some unique information from complex physical characteristics of an integrated circuit, for instance, it generates some unique device-specific data from the delay characteristics of wires and transistors. PUFs depend on the random variations that occur during the manufacturing process, making the PUF behavior extremely difficult to predict.

A device also requires an **operational identity or name** that may be renewed over the device lifetime. It is provisioned during the on-boarding/enrollment process. We propose to assign to IoT devices **self-certifying names**: the name is derived from a public key to enable secure establishing of the identity of a device without relying on an external infrastructure. A Bitcoin address is an example of a self-certifying name—it is constructed as a hash of a public key. This kind of names is **required for accountability** that builds on verifiable identities and the only

[14] Oblivious DNS, DNS-OARC 28, March 2018.

practical method of verification uses cryptographic signatures. Figure 2 gives an example how it can be done.

Additional functionalities for IoT based on the deployed architecture. DNS allows assigning multiple names to a device and we propose to take advantage of this functionality to create several names representing various **features of IoT devices** such as type of sensors, data encoding, data units, frequency of measurements, type of statistical processing, quality of transmission, and others defined by specific applications. We assume that features are predicates, i.e., statements that may be true or false. A name will be a Bloom Filter on a set of features so if we are given a name, we can easily check (with small false positive probability) if the device has a specific feature, thus enabling service discovery by searching given features in a list of available devices [13]. This enables easy IoT discovery of devices and data sources. We also plan to design a scheme for expressing the **geographic location of IoT devices in names** and enable queries on geographic regions. Such geo-queries can take advantage of a recursive quadtree partitioning of the 2D world map and the definition of *geo-prefixes*, compact representations of GPS area coordinates [14]. We can also use geo-identifiers from tools such as the S2 library[15]. Figure 2 gives an example of identifiers and self-certifying names.

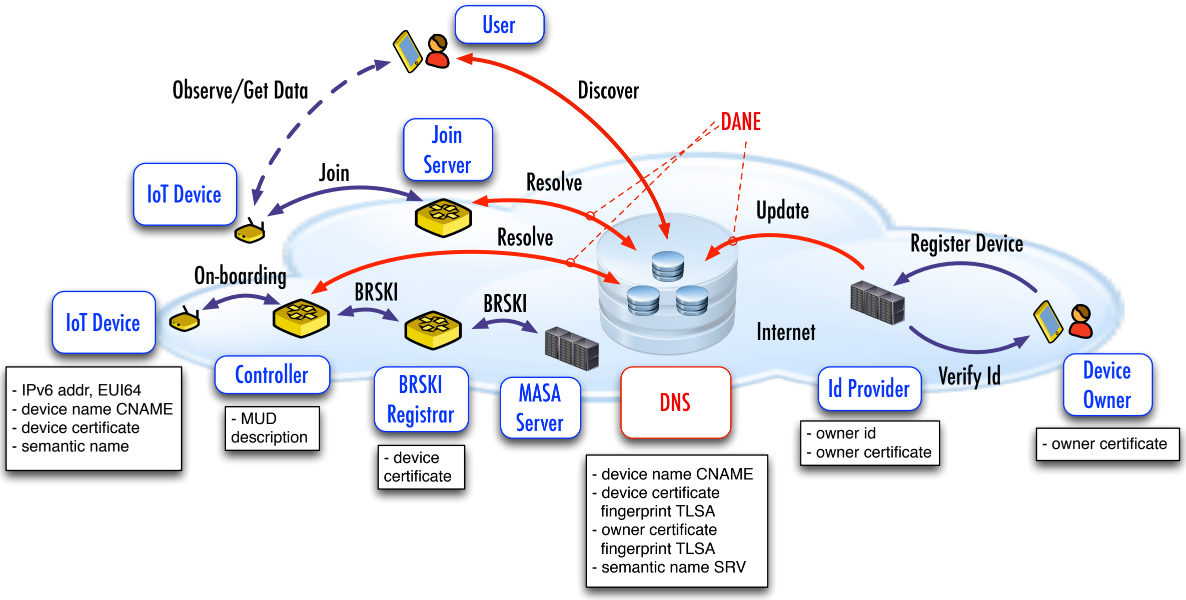


Figure 3: Principal elements of the DNS-based architecture for IoT security.

DINET architecture. The DINET architecture will take into account the complete life cycle of an IoT device from bootstrapping to registration and revocation. As the process is based on the existing DNS architecture, it is operationally feasible. It reduces cost since generated certificates are self-certifying. A generic security framework also reduces cost. We also see this architecture as a basic platform to provide other functionalities such as trust, accountability, privacy, transparency, and service discovery. Figure 3 presents the main elements of the proposed DNS-based architecture for IoT security.

Tangible project results. Besides the design of the security architecture based on DNS and the specification of different schemes or mechanisms, the project will deliver a set of tools, libraries, and APIs that enable: i) IoT devices to operate in a secure way and ii) DNS Registrars and Registries to provision the required information in the DNS system. We identify the following scope for the software developed in the project:

- **DEV**: IoT end-devices, some of which may be highly constrained (e.g., LoRa devices, industrial IoT devices);
- **NET**: the network infrastructure to which IoT end-devices connect (e.g., home network, office network, industrial network, operator network);

[15] https://s2geometry.io

- **REG**: the DNS infrastructure maintained by DNS Registries and Registrars as well as local name servers available in the network infrastructure.

The project will deliver the following results:

1. Definition of an API for automated DNS management at Registries (**REG**).
2. Tools for DNS Provisioning (management of TLSA records, DNSSEC signatures) (**REG**).
3. DNS library for IoT devices (Contiki NG and RIOT) (**DEV**).
4. Tools for secure device on-boarding (**DEV** and **NET**).
5. Accountability support (**DEV** and **NET**).
6. Tools for generating MUD descriptions (**DEV** and **NET**).
7. Tools for inward and outward device protection (**DEV** and **NET**).
8. Privacy protection tools (**DEV**, **NET**).
9. Privacy support for DoH/DoT (**DEV**, **NET**, **REG**).

The DNS library will make functions like DNSSEC validation, DANE, and DoH/DoT available on IoT devices. It will manage KSK (Key Signing Key) rollovers, support multiple recursive resolvers, and make DNS function configurable by end-users with some user-level tools.

1.3.3 Technology Readiness Level

Table 1.2 presents Technology Readiness Levels corresponding to the maturity of the technologies developed in the project. The maturity levels will be taken forward by each individual trial and partner as part of demonstration activities and pilots in terms of technology integration in various product or service platforms.

Technology	**Technology Readiness Levels**
1. API for automated DNS management at Registries	TRL3 - TRL5
2. Tools for DNS Provisioning	TRL3 - TRL5
3. DNS Library for IoT devices	TRL3 - TRL5
4. Tools for secure on-boarding	TRL3 - TRL5
5. Accountability support	TRL3 - TRL5
6. Tools for generating MUD descriptions	TRL2 - TRL5
7. Tools for inward and outward device protection	TRL2 - TRL5
8. Privacy protection tools	TRL2 - TRL5
9. Privacy support for DOH/DoT	TRL2 - TRL5

Table 1.2: Technology maturity

Table 1.3 presents the Technology Readiness Levels for the technologies developed in the project with respect to the proposed Use Cases.

Use Case 1	**Secure IoT device enrollment in IoT networks**
Description and Challenges	The Use Case will validate autonomous secure enrollment in the network by an IoT device based on the developed DNS security architecture. We will consider three different types of networks: LoRa with TTN, NB-IoT with Swisscom, and IEEE 802.15.4. The Use Case involves highly constrained IoT devices such as Arduino Mega and Wipy under Contiki NG and RIOT.

Validated Technology	This use case allows the validation of the following project results: 1. Overall architecture 2. Tools for DNS Provisioning 3. DNS Library for IoT devices 4. Tools for secure on-boarding 5. Tools for generating MUD descriptions 6. Privacy protection tools 7. Privacy support over DOH/DoT
TRL:	TRL4 - TRL5
Use Case 2	**Secure deployment of RIOT IoT devices**
Description and Challenges	This Use Case concerns the deployment of RIOT IoT devices at large scale on cars to rent.
Validated Technology	This use case allows the validation of the following project results: 1. Overall architecture 2. DNS Library for IoT devices 3. Tools for DNS Provisioning 4. Tools for secure on-boarding 5. Tools for generating MUD descriptions 6. Tools for inward and outward device protection.
TRL:	TRL4 - TRL5
Use Case 3	**Secure management of Industrial IoT devices**
Description and Challenges	The Industry 4.0 Use Case will validate the architecture and the developed tools in industrial environments. It will allow the validation of the security and privacy tools in harsh industrial conditions.
Validated Technology	This use case allows the validation of the following project results: 1. Overall architecture 2. DNS Library for IoT devices 3. Tools for DNS Provisioning 4. Tools for secure on-boarding 5. Tools for generating MUD descriptions 6. Tools for inward and outward device protection. 7. Privacy support over DOH/DoT
TRL:	TRL4 - TRL5

Table 1.3: Project Use Cases and Technology Maturity

1.3.4 Related Research and Innovation Activities

The table below presents the overview of the DINET complementarity with respect to ongoing or newly started EU projects and other international initiatives linked to DINET.

Project	**Description**	**DINET Complementarity**
ARMOUR[16] (EU project)	It aims to address security and trust issues in IoT by providing duly tested, benchmarked, and certified security and trust technological solutions for large-scale IoT using upgraded FIRE large-scale IoT/Cloud testbeds properly-equipped for security and trust experimentations.	DINET plans to address similar issues but our approach is based on the DNS infrastructure. In DINET, we propose to provide solutions for self-certification of IoT devices through signal-based fingerprinting and PUF-based identification.
BRAIN-IoT[17] (EU project)	It aims to work on a dynamic federation of IoT heterogeneous platforms and mechanisms to improve data ownership and privacy supported by semantic technologies for interoperable operations and data exchanges.	DINET can integrate heterogeneous IoT platforms thanks to open standards of DNS. We will support the role of device ownership with corresponding certificates and names stored in DNS, which allows its verification and accountability. DINET addresses several issues in privacy related to hiding identities and the possibility of disclosing sensitive information in DNS queries.
Concordia[18] (EU project)	CONCORDIA focuses on device, network, software, data, and user-centric security, privacy, reliability, and trust. The work is evaluated through a couple of use-cases in the telecom, finance, transport, e-health, and defence domain.	DINET will compliment concordia in IoT related use-cases concentrating on the DNS-based register of IoT devices allowing for extended security, privacy, and trust. Especially, DINET will focus its attention on various countermeasures against the most recent threats in the IoT domain (e.g., Mirai) concentrating on inward and outward protection of users and their IoT devices (e.g., through MUD descriptors).
IOTCRAWLER[19] (EU project)	It aims at developing a search engine for IoT devices and at a paradigm change on both how IoT applications can access IoT resources and on how IoT resources can make themselves discoverable.	DINET will provide similar functionality based on the existing DNS infrastructure, the DNS service discovery standards, and on semantic names that encode information on device features.
LIGHTest[20] (EU project)	The objective of LIGHTest is to create a global cross-domain trust infrastructure for electronic transactions. In the infrastructure, a Trust Scheme Publication Authority publishes the location of Trust Lists and Trust Translation Lists in DNS. Clients use DNS as a means for discovering Trust Scheme Providers and obtaining certificates that sign Trust Lists. LIGHTest takes advantage of DNSSEC and DANE for managing the required trust information in DNS.	LIGHTest is not specific to IoT, but rather considers DNS as a means for bootstrapping trust for electronic transactions in a similar way DINET plans to use DNS for bootstrapping trust in IoT devices. DINET will consider the problems related to the use of DNS by constrained IoT devices and cover all security, accountability, and privacy issues raised by IoT. DINET may benefit from the experience of LIGHTest on the use of DNSEC and DANE for bootstrapping trust.

[16] https://www.armour-project.eu

[17] http://www.brain-iot.eu/

[18] https://www.concordia-h2020.eu/

[19] https://iotcrawler.eu/

[20] https://www.lightest-community.org/

SERIOT[21] (EU project)	It aims to provide an open framework for real-time monitoring of the traffic exchanged through heterogeneous IoT platforms within the IoT network to recognize suspicious patterns, to evaluate them, and finally to decide on the detection of a security leak, privacy threat, and abnormal event detection, while offering parallel mitigation actions.	DINET will provide complementary solutions based on MUD descriptions. We will design and develop schemes for DDoS mitigation on networks with IoT devices and for defense against external attacks and intrusions. We will take advantage of Explainable AI to find new solutions for this kind of problems.
SECUREIoT[22] (EU project)	It aims to predict and anticipate the behavior of IoT systems and provide security support to IoT systems from the identification of trustworthy behavior of IoT devices to the establishment of secure IoT services. It also facilitates compliance with security and privacy regulations, and provides APIs and tools for trustworthy IoT solutions.	DINET will enhance trust in IoT devices thanks to bootstrapping trust based on the resilient, scalable, and proven DNS infrastructure. For IoT device bootstrapping, we will take advantage of the IETF BRSKI standard process that involves a Registrar server on the access network and a MASA manufacturer service, thus providing an operationally feasible trustworthy IoT solution.
SOFIE[23] (EU project)	It aims to design a secure, open, decentralized, and scalable IoT federation architecture that will provide integrity, confidentiality, and auditability of IoT data.	DINET will develop a complementary architecture in which the DNS infrastructure provides support for the federation of different IoT platforms or technologies. We will develop an open source library for IoT devices with all needed DNS functions thus enabling IoT federations.
CHARIOT[24] (EU project)	It proposes a unified approach towards privacy, security, and safety of industrial IoT systems based on a blockchain ledger that enables the coupling of a pre-programmed private key deployed on IoT devices with a corresponding private key. The ledger also records all physical, operational, and functional changes of IoT devices allowing for the detection of anomalies.	DINET builds trust upon the DNS infrastructure and plans to add provisions for adapting DNS resolution and secure communication to be compliant with the requirements of constrained IoT devices. DINET will also design and develop a blockchain for trustless bootstrapping of highly-constrained IoT devices so it may benefit from the experience of CHARIOT on using distributed ledgers in the context of IoT.
ENCRYPTED DNS[25] (International)	It uses DNS encryption technologies to enhance security and privacy of users in a manner that ensures the continued high performance, resiliency, stability, and security of the Internet critical namespace and name resolution services.	DINET will test the DNS encryption technologies and adapt to the requirements of constrained IoT devices. We will run tests on real-world IoT networks to ensure that adapted DNS encryption technologies does not impact their performance, resiliency, stability, and security.

[21] https://seriot-project.eu/

[22] https://secureiot.eu/

[23] https://www.sofie-iot.eu/

[24] https://www.chariotproject.eu/

[25] https://www.encrypted-dns.org/

DNS PRIVACY[26] (International)	It explores evolving DNS standards to support privacy in the Internet and empower users to take advantage of DNS privacy tools and resources.	DINET will design new schemes for DNS privacy based on forwarding resolvers and develop a privacy-enabling mechanisms based on machine learning to identify and visualize privacy leaking parts of communication. Their use may be larger than the IoT scope of the project and we will promote them to general DNS stakeholders.
PURPLE Foundation[27] (International)	It is an open-source, community-driven initiative with a focus on enabling the security and interoperability of embedded devices for the Internet of Things.	DINET pursues a similar goal of the IoT security. As we build on DNS and its open standards, our solutions will also enhance interoperability. One partner is the founder of RIOT[28], an open source IoT operating system, one of the five most popular OSes for IoT[29]. We plan to develop the project tools and libraries for RIOT, which will contribute to their large adoption.
Secure IoT[30] Registry (Canadian)	The Canadian Internet Registry (CIRA) started to work on a public DNS record of certificate fingerprints that can be used to authenticate individual IoT devices and their cloud service provider credentials based on the unique IoT device eSIMID. It will leverage the Internet based root of trust embedded in DNS and DNSSEC.	DINET has similar objectives as this project with a different scope—we do not include mobile network operators due to the limited size of the project. Nevertheless, we will provide similar functionalities based on DNS and even go farther by involving heterogeneous IoT identifiers (not only eSIMID). We will also consider the issues of accountability and privacy.
UPRISE-IoT[31] (EU project)	It aims at making users gain control over data generated and collected by the IoT devices surrounding her. The project is user-centric by considering user behaviors and the user context to improve security and privacy. The solutions developed in the project will inform users about the data that are being collected in a user-friendly manner, and offer options to oppose to them.	DINET also address the issue of personal data in IoT. However, UPRISE-IoT is focused on information and consent of data IoT collection, whereas DINET deals with potential leaks within the system infrastructure. In addition, DINET deals with the core of the IoT infrastructure while UPRISE-IoT deals with the user interactions at the edge.
SPARTA[32] (EU project)	It is a Cybersecurity Competence Network aiming at developing and implementing research and innovation collaborative actions in the area of CyberSecurity. It deals with a number of topics associated with Cybersecurity including IoT. SPARTA deals with Security and Privacy by design, and resilience for IoT.	DINET only covers a subset of the topics addressed in SPARTA, but we will consider the challenges explored in SPARTA with a specific technological focus on DNS and IoT.

Table 1.4: Related research and innovation activities

[26] https://dnsprivacy.org/wiki/

[27] https://prplfoundation.org/

[28] https://riot-os.org/

[29] https://opensourceforu.com/2019/10/the-five-most-popular-operating-systems-for-the-internet-of-things/

[30] CIRA (Canadian DNS Registry) Secure IoT Registry, August 2019.

[31] http://www.chistera.eu/projects/uprise-iot

[32] https://www.sparta.eu/

1.3.5 Methodology

The methodology of the project is driven by industrial problems and research of solutions, security analysis, experimental evaluation, and application of the developed tools and libraries to meaningful Use Cases. In particular, our methodology consists of the following activities:

1. consider the main security, privacy, and accountability issues facing IoT,
2. identify the security requirements and business drivers for DNS-based solutions and derive KPIs relative to their operation,
3. design an overall security architecture by taking into account the requirements for security and privacy as well as the constraints of IoT devices and their lifecycle,
4. identify all required elements and actors, and the interactions and interfaces between them,
5. explore new ideas and research innovative schemes and mechanisms to address all the issues,
6. evaluate them by developing operational early prototypes to validate their design,
7. refine the architecture based on the feedback from early prototyping,
8. integrate tools and mechanisms in three Use Cases: i) secure on-boarding of LoRa devices, ii) secure deployment of RIOT IoT devices, and iii) secure management of Industrial IoT,
9. analyze the security of the proposed solutions based on the existing methodological standards,
10. evaluate the proposed solutions according to the KPIs specific to each Use Case,
11. promote the solutions and mechanisms to standardization bodies, disseminate their design and properties to relevant stakeholders, and exploit them in commercial products and services.

1.3.6 Gender Analysis

Gender is not relevant to the DINET project content. Nevertheless, the institutions involved in the DINET project adhere to the principles stated in the European Charter and Code for Researchers and apply the Non-discrimination Principle and Gender Balance. Additionally, the project will promote gender equality to the largest possible extent. The project will give preference to female if equal qualifications prevail among potential candidates or beneficiaries of activities (e.g., selection for doctorate or post-doc positions). We believe that gender equality issue becomes even more important given the technological focus of the project. For this reason, in case of choice among staff with equal qualification preferences will be given to female to redress traditional inequities and achieve the best possible balance among the user group.

1.4 Ambition

Several research and innovation projects addressed the issues related to IoT security, trust, privacy, accountability, and discovery of devices and resources. Some of them explored clean slate solutions, created reference architecture models, defined new IoT identifiers, or focused on developing solutions for specific IoT technologies or applications. As IoT is an extension of the Internet, we believe that solutions suitable for IoT should be able to re-use the technologies that have proven their effectiveness in the Internet. However, IoT devices and networks have many limitations and they are inherently different from PCs or servers connected to the Internet. Even if it is difficult to take advantage of the existing Internet technologies in IoT, we are convinced that they can solve many IoT problems.

The ambition of the DINET project is to:

1. adapt the current Internet technologies for IoT wherever possible, which will contribute to the advent of the seamless secure interoperable IoT,
2. explore and evaluate new standards and mechanisms that we can use in both legacy and new IoT technologies/platforms/applications,

3. provide more information and control over sensitive data to the end-user or end-devices to enhance privacy based decisions,

4. enable accountability and transparency by using the DNS eco-system and machine learning models,

5. ensure that the proposed adaptations or new standard mechanisms satisfy performance, scalability, and security requirements, which will be demonstrated through validation in several Use Cases involving real-world IoT networks with end-devices under common IoT operating systems.

The objective of DINET is to enhance trust, privacy, security, transparency, and accountability of IoT devices based on the open DNS infrastructure and IETF standards that are operationally feasible, without additional costs, immediately deployable, and easily scalable. We review below the related work in these domains and point out the progress beyond the state of the art.

1.4.1 DNS as a replacement of a PKI for authentication and end-to-end IoT secure communications

DNSSEC and DANE provide means for replacing a traditional PKI hierarchy with a set of signed DNS records. One of them may contain a TLSA record with a certificate fingerprint, providing thus a chain of trust. Lamb explored the use of DNSSEC and DANE for IoT authentication and authorization [15]. Kamola (member of the NSAK partner) proposed an architecture that takes advantage of DNSSEC and DANE to manage device owner identification data and store required authentication information in TLSA records [16]. Sánchez et al. [17] proposed a DNS based dynamic authentication of services for IoT using a DNSSEC forwarder and DANE TLSA record for verification. VeriSign filed several patents on using DNS for authentication, service discovery, and annotation of IoT devices (U.S. Patent 9,762,556, 9,935,950, 2016/0205106A1), nevertheless the proposed schemes are not compatible with RFC 7218 (Use Cases and Requirements for DNS-Based Authentication of Named Entities). In the domain of electronic transactions, LIGHTest, an H2020 project, proposes a lightweight trust infrastructure based on DNS for providing parties of electronic transactions with automatic validation of trust based on their individual trust policies. Yan et al. [18] evaluated security, mobility, infrastructure independence, localization, and efficiency for a DNS based IoT name service. The analysis shows enhanced security with DNS, but the cost is too high for resource constrained IoT devices and application scenarios.

Other IoT alliances and standardization organizations also consider adopting IETF protocols for IoT security. The Fairhair Alliance[33] recommended: "*building upon a solid foundation of secure identities and security protocols being standardized for the Internet*". The architecture already uses the BRSKI protocol, MUD descriptors, and the EST protocol. SIGNIFY, one of the contributors to the Fairhair architecture considers extending the architecture with the use of DNS.

There are commercial security solutions for IoT based on traditional PKIs. The GlobalSign IoT identity platform uses PKI as the core identity mechanism, so all devices authenticate as they come online, prove their identity, and securely communicate with other devices, services, and users. The DigiCert PKI based IoT solution uses ECDHE (Elliptic curve Diffie–Hellman, ephemeral) and X.509 OIDs. The Janua identity management and open source IoT platform leverages PKI to control the authorization of data sharing and service access.

Using DNS in IoT raises some new issues. As all DNS traffic is currently sent in clear (unencrypted) form, privacy becomes an important issue touching all Internet users [19]. DNS-over-HTTPS (DoH) may improve privacy because all communications are encrypted and their entities authenticated. At the same time, it creates the problem of possible profiling of users by an open resolver: it knows the IP source address of the device and the DNS query, so it may track or create user profiles. Oblivious DNS [10] decouples the knowledge of the client source IP address and the DNS query, but its scalability is limited by the use of the single authoritative name server for the specific `.odns` domain. The Cloudflare onion service also proposed solution to the problem. However, it requires TOR configuration of the client, which is not suitable for IoT devices.

The recent ICANN report [20] (SIDN participated in the report) discusses the interplay between DNS and IoT, arguing that DNS provides functions and data that can make IoT more secure, stable, and transparent. It identified five challenges for DNS and IoT industries, and our project aims at the first most important one: developing a DNS library to make the DNS security functions available on IoT devices.

[33] Fairhair Alliance (now Open Connectivity Foundation): Security Architecture for the Internet of Things (IoT) in Commercial Buildings.

The already mentioned Secure IoT[34] project by CIRA aims at the similar objectives as DINET—it proposes to create a public DNS record of certificate fingerprints for authentication of IoT devices and their cloud service providers. It similarly leverages the DNS root of trust and the DNSSEC and DANE protocols for authentication.

DINET approach and progress. The main innovation of the project is the idea of using the decentralized DNS infrastructure and open Internet standards to enhance security in IoT. None of previous or existing work, which includes research projects, standards, and commercial solutions, had combined the possibility of using DNS as PKI with a compressed X.509 version fitting constrained IoT environments. DINET aims at reducing the cost of DNS based solutions and adapting the DNS operation for constrained IoT devices. DINET addresses the challenge of making the DNS security functions available to IoT devices on common operating systems and positions itself as a European counterpart of the Secure IoT project.

1.4.2 Naming and Resolution Schemes for IoT device identifiers

DNS is the naming service in the Internet and one of its most used services is to find the IP address corresponding to a domain name. Even though the Internet evolved to a scale not even dreamed of initially, DNS remains the basic infrastructure for resolving names in the Internet.

There are different naming schemes for IoT devices and most of them are not standardized—they concern specific IoT applications or technologies. Many standardized IoT naming schemes use DNS as the basic building block:

- Electronic Product Code (EPC) (e.g., RFID, Barcodes), standardized by GS1, uses the Object Naming Service (ONS), an overlay over DNS.
- Object Identifier (OID) (used as a persistent identifier for an object), standardized by ITU and ISO/IEC, uses the Object Resolution System (ORS) that interacts with DNS.
- Digital Object Identifier (DOI), standardized by ISO, relies on the DNS name resolution.
- EUI-64, standardized by IEEE, is used by the LoRa Alliance: based on the IoT end-device identifier, DNS provides the authentication server for secure on-boarding.

The EU IoT expert group[35] identified the requirements for a suitable IoT identification, addressing, and naming scheme: it should be transparent and network independent, scalable to a large number of devices, efficient for constrained devices, preserving privacy, allowing for flexible authentication and interoperability. We can notice that a naming scheme based on DNS and adapted to constrained IoT devices corresponds to the requirements. AFNIC proposed the concept of using DNS for IoT identification, naming, and resolution [21, 22]. This idea comes from their work on the Object Name Standard (ONS[36]) and related IoT research[37]. Similarly, the RFID industry already considered the use of DNS for name resolution [23].

Several systems or architectures proposed to use self-certifying names [24, 25, 26]. A self-certifying name is a name for which the ownership can be verified without relying on a trusted third party. For instance, a name can be derived from a public key to enable secure establishing of the identity/ownership without relying on an external infrastructure. This kind of names fits perfectly well DNSSEC that guarantees name integrity. Anderson et al. [26] proposed the Accountable Internet Protocol (AIP) based on self-certifying addresses for hosts. The addresses support accountability, i.e., being able to associate an action with the responsible entity.

DINET approach and progress. The project will propose a uniform scheme for self-certifying IoT device naming with the name resolution based on existing IETF standards. The proposed scheme will fit constrained IoT devices while conforming to standard DNS operation. The self-certifying names will support accountability that builds on identities verifiable with cryptographic signatures.

[34] CIRA (Canadian DNS Registry) Secure IoT Registry, August 2019.

[35] Expert Group on the Internet of Things (IoT-EG), Sub-Group on Identification

[36] GS1 Object Name Service (ONS)

[37] DNS Name Autoconfiguration for Internet of Things Devices

1.4.3 Semantic names and service discovery

With respect to semantic names, one consortium member proposed DINAS [13], a new naming scheme and a service discovery protocol for short-range sensor networks running RPL. Zaslavsky et al. discussed the reasons for which discovery can make a significant impact on the future of IoT and become a necessary component for the IoT success story [27]. DINET follows their reasoning with original ideas on semantic names. The semantic Web of Things initiative [28] undertook much research on discovery and understanding IoT data semantics, however, the approach did not pave the way for uniform IoT naming schemes. Kamilaris et al. considered DNS as a suitable framework for discovering embedded devices and environmental services in real-time [29]. They proposed to build a global meta-data repository for embedded devices based on DNS extensions for supporting location-based discovery of Web-enabled physical entities.

Brunisholz et al. described a way to encode geographical properties in a name using 2D quad-trees [14]. The same way IP subnet prefixes describe topological proximity, this method encodes in a common prefix geographical proximity: if two devices share a common prefix, they are geographically close to each other. Geo-prefixes enable service discovery based on localisation.

DINET approach and progress. DINET will extend the idea of semantic names and propose adaptations to resolve device names based on compact identifiers expressing a rich set of device features based on Bloom filters. We also plan to integrate the notion of geo-location or geographical attributes in semantic names to support geographical queries.

1.4.4 Protecting IoT networks

IoT has increased the number and impact of potential security attacks. In recent years, different botnets (e.g., Mirai) [30] have shown that the deployment of IoT devices can compromise critical infrastructures with huge economic losses. The problem is especially critical in certain scenarios (e.g., involving eHealth devices), which may affect user safety. To address such security concerns, there is a need to define approaches to reduce the attack surface of the IoT devices. Beyond the use of traditional cryptographic and access control techniques, the security aspects of IoT devices should be properly managed through a governance approach to ensure that devices behave as expected. However, the specification and enforcement of such aspects can be challenging in environments in which a huge number of IoT devices have the ability to communicate with each other and, sometimes, without the explicit consent of their owners.

To address this issue, the Manufacturer Usage Description (MUD) [31] is an Internet Engineering Task Force (IETF) standard aimed to define the intended behavior of the device through Access Control Lists (ACLs) to restrict the communication to/from a certain device. MUD defines an architecture for obtaining MUD files with the policies specified in the Yet Another Next Generation (YANG) and JavaScript Object Notation (JSON) standards. While MUD was recently standardized (March 2019), it has received a strong interest from the research community and standardisation entities worldwide. The USA National Institute of Standards and Technology (NIST) has also recommended MUD files to complement security credentials to reduce the attack surface [32]. In this sense, some authors [33] [34] has patented two different usages of MUD files: a MUD file is used to deliver policy requirements for a device joining the network and it is collected during the bootstrapping process to obtain the security policies before the device has access to the network. Hamza et al. [35] proposed a method for generating automatically the MUD file from traces of the network.The network access control policies specified in a MUD file can be straightforwardly enforced through the Software-Defined Networking (SDN) paradigm [36]. However, beyond aspects of the network level, the MUD semantics does not provide the possibility of defining security properties to provide a more fine-grained approach that determines how IoT devices should communicate.

SDN can also be used to mitigate DDoS attacks [37, 38]. FloodDefender [39] implemented three modules: i) the table-miss engineered to prevent the communication bandwidth from being exhausted by offloading traffic to the neighbor switches, ii) packet filter to identify attacks by using B+ tree traffic, and iii) flow rule management to search and purge unneeded entries in the flow table. A prototype was implemented in both software and hardware.

DINET approach and progress. DINET will propose automatic generation of MUD descriptors based on the observation of the device regular traffic. In addition, the MUD model will be extended to provide higher expressiveness allowing to specify more refined security configurations.
DINET will use MUD files not only to monitor the behavior of the network components, but also to white-list the regular behavior in the edge networks and to provide a way to perform accountability and reporting of any device collecting personal data in a standardized way.
DINET will design and implement an SDN-based, dedicated security framework that will host AI-based anomaly detection algorithms able to identify various threats (like DDoS attacks). Additionally, it will allow automatic and dynamic reaction to the discovered security issues to efficiently mitigate them.

1.4.5 Protecting privacy with pseudonym identifiers

Network traffic generated by IoT devices can be a rich source of information that can undermine users' privacy [40]. In particular, identifiers such as MAC addresses and other network addresses can be leveraged to track users [41]. Random and periodically changing addresses have been introduced to address the tracking issues, e.g. in the Bluetooth specifications. For 802.11, random MAC address has been included in mobile OSs. A member of the consortium is involved in the development of those mechanisms in the IEEE 802 working group.

However, periodically changing identifiers can disrupt the operation of other protocols and services. To solve this issue, resolvable identifiers have been introduced—they enable identification by trusted parties while preventing tracking by other parties. Current resolvable approaches rely on a pairing mechanism in which secret keys are exchanged between parties. In its current state, this approach do not scale and is incompatible with the current DNS architecture.

DINET approach and progress. DINET will extend the concept of resolvable pseudonyms and propose adaptation to integrate this feature in the context of the DNS architecture for IoT potentially leveraging self-certifying names.

1.4.6 AI techniques for attack detection and privacy leakage identification

Artificial Intelligence methods based on machine learning are extensively used in the context of cybersecurity [42], e.g., in the context of malware [43, 44], botnets [45], or general cybersecurity threat detection [46]. Relevant to this proposal, the authors of [47] propose to use Long-Short Term Memory neural networks [48] to identify DDoS attacks in the context of intrusion detection. Applications of machine learning methods in security naturally extend to the privacy protection, essential and important part of many cyberattacks focused on identifying individuals based on their digital trace. For example, Huang et al. [7] proposed to build a data-driven model of privacy extending the Generative Adversarial Network architecture [9]. One partner member proposed to apply this notion of privacy to medical images [8].

However, one of the most important shortcomings of the proposed AI-driven methods is the lack of interpretability. In other words, most of the decisions indicated by complex machine learning models, such as LSTM or GANs, do not allow to investigate the inner mechanisms of the decision process. This aspect becomes especially important in the context of security and privacy. As one of the first publications in this area, recent work [49] attempts to address this problem using adversarial examples to visualize the decision logic in the context of ML-powered intrusion detection systems. Nevertheless, there are still other techniques that can be exploited, e.g., Siamese architectures and GANs.

DINET approach and progress. DINET will design and implement machine learning methods for DDoS detection and privacy leakage identification based on Generative Adversarial Networks and Siamese architectures. Contrary to the existing methods, we will expand those models to explain the internal decision process of algorithms trained to detect anomalies (such as DDoS attacks). Furthermore, we will propose a novel data-driven privacy protection approach in the context of cybersecurity.

> *You know what? That IoT light bulb is connected to the same home network on which you do your banking transactions...*
>
> — Anonymous

2 Impact

DINET will have an important impact with a breakthrough in IoT security and privacy by developing lightweight solutions suitable for constrained IoT devices backed by the robust DNS infrastructure. In comparison to existing security standards and techniques, the proposed approach will achieve a consistent level of security across the entire IoT domain based on a single trust anchor and the extension of the Internet security protocols.

2.1 Expected Impacts

The DINET objectives directly correspond to one of enabling actions defined for the Cybersecurity strategic value chain: *"Create the next generation EU framework for PKI infrastructure and European DNS management for critical infrastructure"*[1]. Table 2.1 gives extensive details on the ability of the project to achieve the expected impact as listed in the work programme.

Expected Impact of Objective SU-ICT-2018-2020	**DINET contribution towards the expected impact**
Improved market opportunities for the EU vendors of security components.	DINET involves several complementary EU stakeholders. Such a diverse consortium facilitates the development of advanced cybersecurity products and services that will enable EU companies to be at the forefront of IoT security and privacy components.
Increased trust both by developers using/integrating the ICT components and by the end users of IT systems and services.	In the current Internet, an end-user has trust in a WWW connection based on the server certificate validation in the conventional PKI. Using the same scheme in IoT is only possible for sufficiently powerful devices that can store root CA certificates. There are also different IoT security components for different IoT domains, which hinders the use of conventional PKI. DINET will enable communications having the same security properties, but based on DNS as a single trust anchor, thus enhancing trust for users, and enabling developers of ICT components to provide security solutions much easier.
Protect the privacy of citizens and trustworthiness of ICT.	Results from a survey[2] of consumers in Australia, Canada, France, Japan, UK, and the US by Consumers International and the Internet Society on IoT in 2019 indicate that 75% of people have concerns about their data being used by other organisations without their permission. The DINET architecture protects communications from eavesdropping and proposes to take advantage of AI systems to classify the sensitivity of data from a privacy point of view and identify pieces of data that would leak personal information. As DNS queries may also leak some personal information, DINET will provide adequate solutions to protect privacy.
Acceleration of the development and implementation of certification process.	The DINET architecture will reduce the costs for all related stakeholders by relying on the open DNS infrastructure as a trust anchor. The IoT device owner could either use a CA for certification process or rely on self-signed certificates and use DNS to act as a trust anchor to authenticate the self-signed certificates. Since the certificates are based on standards, tools, and support processes delivered as the results of the DINET project, they will accelerate the development and implementation of the certification process in IoT.

[1] Recommendations of the Strategic Forum for Important Projects of Common European Commission.

[2] The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things.

Advanced cybersecurity products and services will be developed improving trust in the Digital Single Market.	The tools and libraries from DINET will foster the development of advanced cybersecurity products and services conformant to standards and regulations, which will contribute to improving trust in the Digital Single Market.
The use of more harmonized certification schemes will increase the business cases for cybersecurity services as they will become more reliable.	Providing an open security solution based on a unique trust anchor will harmonize IoT security developments, thus speeding the adoption of IoT security deployments, which will lead to the increase in business cases for cybersecurity services. Moreover, the proposed DINET architecture is much less complex than solutions based on conventional PKI, which will enhance intrinsic reliability of IoT devices and networks.
Validation platforms will provide assessments with less effort compared with nowadays and assure a better compliance with relevant regulations and standards.	DINET focuses on delivering functional demonstrators to showcase their viability in real-world networks. The Use Cases will show that assessments are much easier and the developed solution based on the technologies proven in the Internet guarantees better compliance with relevant regulations and standards.

Table 2.1: Relevance of DINET to the expected impact defined in the work programme.

2.1.1 Key Performance Indicators

We present below the Key Performance Indicators (KPI) for each project Obejctive.

Obj.	KPI reference	Description	Method	KPI indicator
1	Requirement collection	Requirement collection for security, privacy, trust, accountability from different IoT domains industries	Survey, Questionnaire, Interview	A minimum of three different IoT networks from commodity and industry domains
1	End-to-End IoT resolution	Should able to get an IoT device to use the DNS infrastructure to resolve to a service in the Internet	Experimentation, Software development	A minimum of two heterogeneous IoT networks should be able to do end-to-end resolution
1	End-to-End Resolution time	Should able to get an IoT device to use the DNS infrastructure to resolve to a service in the Internet within the IoT device resolution constraint	Test platform	Should be able to resolve within 5 seconds duration as per the limit in LoRaWAN specifications
2	X.509 digital certificate compression	Should be able to compress X.509 certificates to IoT constrained devices	Use standardized compression techniques or propose a new one	Should be able to compress an X.509 certificate which is of around few kilobytes to less than 55-222 bytes for LoRa usage.
2	Bootstrap trust	Should be able to bootstrap trust on IoT devices using large number of X.509 certificates in a blockchain	Tests	A blockchain storing a total capacity of X.509 certificates exceeding typical 10K RAM and 100K storage should be considered.
3	Post-quantum certified security protocols [%]	Measures the fraction of post-quantum security protocols established in the project.	Quantum computing is expected to break long-key RSA/ECC encryption	The project will re-use quantum certified protocols; quantum-based analysis of all protocols (100%) used in the project completed.

3	Security support mechanisms	Able to create self-signed certificates, generate TLSA records, and compressed X.509 for IoT scenarios	Software development, test	Able to automate and generate the required cryptographic keys for a minimum batch of 100 devices at a time.
3	Secure onboarding	Test proof of ownership using MUD, BRSKI, and MASA based on the DNS infrastructure	Software development, test	Able to have at least three different IoT devices using three different networks securely enrolled.
3	Formally verified authentication schemes [%]	This KPI will measure the number of formally proved authentication protocols.	Provide verification of developed procedures with known authentication risks	100% evaluated resilient against common attacking techniques.
3	Mean-Time to Detect [s]	Is the time required to detect a malicious event running in the IoT environment.	Evaluated through AI techniques in Tests	Real-time detection.
3	Mean-Time to React [s]	How long does it take to respond to a threat once the event is detected.	Testing autonomous policy management	Real-time reaction.
4	Privacy Schemes [%]	Analysis of DNS query privacy protection.	Formal methods used	100% mechanisms evaluated; assessment of known threats provided.
4	Delayed Operation due to Privacy Schemes	The privacy schemes considered add additional processing overhead	Test cases	Remain in the 5 seconds limit for name resolution.
5	Evaluation of Use Cases	Evaluate the complete IoT device life-cycle using the proposed architecture.	Test cases	Devices in the three Use Cases should be able to bootstrap and establish a secure connection.
5	Business drivers	Convincing IoT industry body or business to test the proposed infrastructure.	Organize plug-fest at different events	Test interoperability during the plug-fest with at least three different IoT industry or businesses.
6	Scientific publications	Publish papers at relevant workshops, conferences, and journals	Writing good scientific papers	At least 20 papers should be published with ACM, IEEE, Elsevier, or Springer.
6	Standardization bodies	Undertaking standardization actions	Participation at standardization bodies	Developments of standards at minimum 3 relevant organizations (cf. Exploitation plan) at least at the follow-up level.

Table 2.2: KPIs of the project.

2.1.2 Impact on business and economy

Nowadays, the global IoT market is estimated to be \$1.7trillion[3] and a 10% increase in IoT connections between 2018-2032 would generate[4] an increase in GDP of \$370bn in Germany and \$2.26trillion in the US, which shows the direct impact of IoT on economic development. It is forecasted that there will be an average of ten IoT devices per person, thus impacting all domains of our life. Rapid adoption of IoT will create new products, services, revenue

[3] iPropertyManagement: IoT Statistics, https://ipropertymanagement.com/iot-statistics.

[4] IoT economic impact study, https://www.frontier-economics.com.

models that will attract investments and create jobs.

However, along these benefits come concerns of security, privacy, accountability, and transparency. Most of the research or projects involved in providing solutions for mitigating these concerns focused on IoT as a domain separate from the Internet. In DINET, we look at IoT as an extension of the Internet with some constraints. Hence, our approach is to address the concerns using the technologies and architectures that have been proven in the Internet and new technologies that could be used across the plethora of IoT technologies. In this way, DINET will make a major impact on business, economy, and society because solutions based on standards allow easy learning curves for developers and reduce the cost for business.

DINET dedicates WP3 and WP4 to tools and support focused on business and manufacturers. They will be able to use them in their domains, thus focusing their technical expertise on specific domain-oriented solutions and outsourcing important generic features such as security, privacy, transparency, and accountability to the solutions proposed by DINET, which will enable new market opportunities.

For the society, giving control to the users on their data being transmitted and adding accountability and transparency helps to increase trust in using the IoT applications.

Some research organizations started initiatives similar to DINET of using DNS for IoT internationally with a limited scope. One such example is the Canadian Secure IoT registry, part of a “Canadian Multistakeholder Process: Enhancing IoT Security”[5]. The DINET consortium based on its prior complimentary expertise and experience can rapidly develop adequate solutions, thus providing an advantage for EU companies and products with respect to other countries or regions.

2.1.3 Impact on Security, Privacy, and IoT Adoption

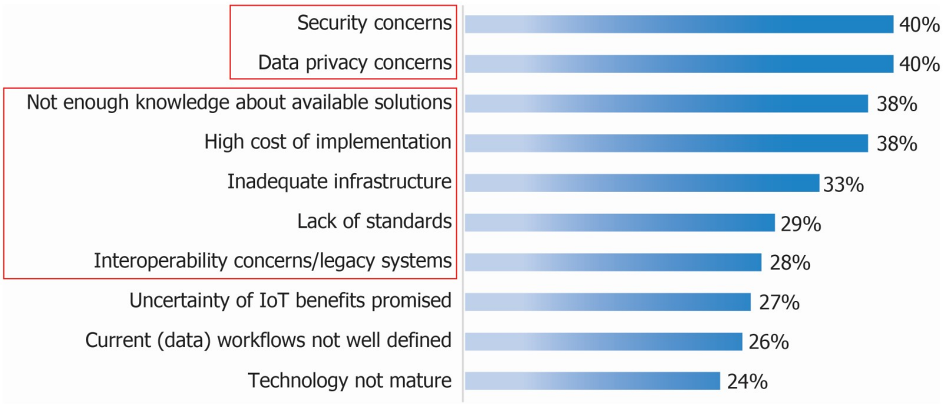


Figure 4: IoT adoption inhibitors. Source: Penton Media.

A survey by Penton Media[6] showed the major IoT adoption inhibitors with the top two concerns of **Security** and **Privacy**. According to the 2019 IoT Developer Survey by the Eclipse IoT Working Group, **Security** is the leading concern for the IoT domain (cf. Figure 5) with **Privacy** attaining 18%, almost the same score as other important concerns (Connectivity, Data Collection, and Performance). The consequences of inadequate support for security and privacy include the impact from lost data, reduced sales, increased expenses, regulatory fines, and customer dissatisfaction. DINET with its lightweight DNS-based solution for IoT security and privacy will have important impact on the concerns and inhibitors of wide IoT adoption.

The European Commission launched in 2016 a strategy on the Fourth Industrial Revolution (Industry 4.0)[7] that leverages on IoT to raise global income levels and improve the quality of life for populations around the world. Given the significant attention and prioritization of the digitization of the EU industrial sector, the security of IoT in the context of Industry 4.0 is an aspect of great importance. Security, if not properly and efficiently managed might raise an extremely high risk and can hinder the evolution of the Industry 4.0. On a long term, security risks may eventually represent a threat to the existence of Industry 4.0 itself. The industrial partners of the project believe that

[5] Canadian Multistakeholder Process: Enhancing IoT Security. Final Outcomes and Recommendations Report, 2019.

[6] Top 10 Reasons People Aren’t Embracing the IoT, https://www.iotworldtoday.com.

[7] EC, Fourth Industrial Revolution, https://ec.europa.eu/digital-single-market.

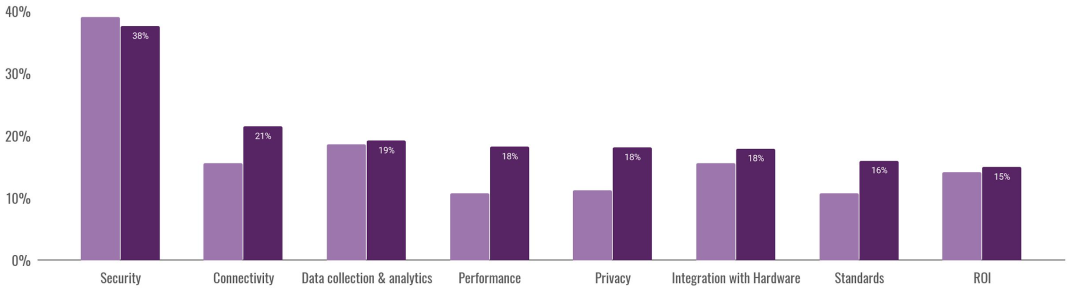


Figure 5: IoT concerns. Source: Eclipse IWG.

efficient and effective security practices and solutions in Industrial IoT are paramount to the success of Industry 4.0, in particular, by supporting a high degree of automation for long product life-cycles.

The project results will have an important impact on the mitigation of IoT-powered DDoS attacks. Large DDoS attacks generated by IoT bots are increasingly common and bring considerable risks to critical infrastructures and services. Our proposed mechanisms placed in edge networks will automatically block traffic from devices that are part of a botnet, which would proactively stop DDoS attacks close to the source, thereby reducing the amount of DDoS traffic that operators would have to handle.

Proposing the right security mechanisms while guaranteeing long lifetimes of IoT devices will have a positive impact on adoptability of the project results. This native security approach will increase the acceptance level and further adoption of the project solutions.

Inadequate support for privacy may lead to important consequences having strong impact on our lives: identification of a person, its localization and tracking, profiling, linking and combination of information leading to the disclosure of some sensitive information. We attach particular importance to the issue of privacy in our project and we will propose several different mechanisms to enforce privacy related to IoT devices.

2.1.4 Environmental and social impacts

In this context, the major impact of the project results relates to fact that IoT devices sense and act upon physical environments so that security breaches may have physical world safety implications—they may harm humans, reveal their location, or disrupt the operation of service providers and critical infrastructures. If the project solutions can prevent such consequences, the environmental and social quality of life will be improved.

The project will also have impact on improving the consumer awareness with respect to IoT. According to the survey[8] of consumers, half of people across markets distrust their connected devices to protect their privacy and handle their information in a respectful manner. This distrust discourages consumers from purchasing connected devices. Our solution that provides high levels of security and privacy will contribute to building trust with current and future customers, while at the same time creating a more secure IoT environment. While there are many factors at play when it comes to consumer trust in connected devices, we can achieve significant impact by proposing adequate IoT privacy and security standards so that consumers can more confidently buy and enjoy safer IoT devices.

2.1.5 Impact on Standards

DINET plan to impact the development of IETF and ICANN as well as IEEE and LoRa Alliance standards. We discuss the details in the part on Standardization.

2.1.6 Reinforcing European Technological Leadership

The future marketplace for the DINET solution will reside in the pan-European sector of the IoT Security. Early development and adoption of the proposed solution in Europe will give Europe a significant head start globally to capture a significant market share and even setting a standard for these markets. New solutions are replicable for exports to other parts of the world.

[8] The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things, https://www.internetsociety.org.

In the DINET consortium, all partners have complementary roles in increasing the share of the Secure IoT markets:

- Industrial partners have roles in increasing the share of the Industrial and consumer IoT markets.
- Top-Level Domain Registries and a Domain Name Registrar can increase the potential for new IoT applications by supporting the resilient operation of the DNS infrastructure.
- Research partners can attract new students and employees enticed by the challenges and (job) opportunities of a new market.

A number of examples highlighted and being used, tested, implemented or developed within the scope of the project:

- **Increasing the market of software IoT systems**: The project will build on **RIOT**, the leading European OS for IoT with the objective of creating a secure eco-system around the software platform for a multitude of hardware devices. RIOT is open source and based on standard protocols with a significant community of developers, both from Industry and Academia. The project results will directly impact the **adoption of RIOT** as a software system to use by integrators and suppliers of sub-systems.

- **Increasing the competitiveness by developing innovations in DNS IoT**: The results of DINET will raise significant business perspectives related to the development of new secure IoT services based on DNS. Moreover, there is a place for startup companies to make the interactions with the DNS infrastructure smooth and easy. We plan to explore business possibility of a company that placed between end-users, Domain Name Registrars, and Top-Level Domain Registries will provide a service of provisioning the required cryptographic material and signatures in DNS, and registering/signing/verifying the identities of IoT owners or providers.

- **Emergence and growth of new companies, in particular SMEs**: IoT is a **domain of choice for innovation** by new companies and especially SMEs. It requires a little entry investment and with a good application idea, an SME can easily end up with an interesting product. The project results delivering a lightweight security and privacy solution will contribute to the sophisticated software and hardware platforms that will enable such innovations and further open up new business opportunities for actors willing to develop applications and/or provide value-added services.

2.1.7 Barriers/Obstacles and framework conditions

Barriers likely to be encountered are:

- Reluctance to adopt a new trust anchor by those who run and operates current IoT networks that rely on the conventional PKI.
- Liability issues if some responsibilities are not well defined.
- Regulatory issues: many activities and processes are strictly regulated by international and national regulations. The introduction of an innovative technology like the one proposed in the project must be carefully thought to fulfil legacy requirements, or to face inappropriateness or un-applicability of old regulations, potentially unable to manage the new features and uses that the results of the project will make available.
- Acceptance of a technology not yet widely proven or even known.

2.2 Measures to Maximise Impact

2.2.1 Dissemination and exploitation of results

2.2.1.1 Dissemination of results

The objectives of the dissemination activities are the following:

- raise awareness within various target communities about the project research activities and results,

- demonstrate the project concept and potential applications to key stakeholders at the European level,
- promote the DINET research results by providing contributions to different standardization bodies and user fora.
- disseminate the project results at relevant conferences and journals,
- pave the way for exploitation of project results.

At the early stage, DINET dissemination activities will be focused on the creation of a basic set of necessary presentation material-dissemination package that will be used as a basis for any dissemination actions. A website, newsletter, posters, and brochures will be designed during the first months of the project and will be used by all partners of the consortium. The project will setup a YouTube DINET channel where short video describing the preliminary vision and results achieved in the first stage of the project will be presented outside the consortium. DINET will also be active on social media, e.g., by setting up a Twitter and LinkedIn accounts to promote its activities and results.

Early dissemination. During the first year of the project, DINET will focus on the promotion of its vision and architecture towards the major players, key stakeholders, and IoT industrial fora. Concerning research opportunities, DINET will highlight the fact that its proposed technologies will open new research topics. Furthermore, the project will communicate on its business potential to key stakeholders.

Planned dissemination activities include:

- Publication of a white paper about the DINET concepts and its business opportunities, based on the gap analysis done by the consortium members.
- Article in a technology magazine focusing on the core components of the DINET architecture, the security and privacy requirements, application scenarios, and their impact on the system, design, and technical requirements to support the proposed technologies. The article aims at raising awareness in the research community on the challenges and research potential of the project.
- Presentations of the technology developed in the project at recognized workshops or conferences.

The aim of these preliminary dissemination activities is to gain the attention of major stakeholders, allow collaboration with on-going research initiatives in relevant fields, and raise anticipation for the specific results that will appear during the next period.

Main dissemination activities during the project.

- **Demonstration activities at events**. The DINET architecture and main components will be demonstrated in dedicated activities. With the progress of the project, various components within the architecture will be integrated and demonstrated, which will allow technical and business feedback, and will add to the project impact by raising awareness of its status, progress, and results. In particular, these demonstrations will be performed in selected scientific events, such as conferences, workshops, and international industrial fairs. Moreover, DINET will produce different video demonstrators shared through the DINET channel to reach the specific background and interests of different audiences, with a particular focus on enterprises outside the consortium.
- **Organization of targeted workshops**. DINET will organize at least two workshops targeting both the research and industrial community working in the relevant domains. The workshops will bring opportunity to present and discuss the DINET most recent results with field experts, getting feedback from a highly interested community. In addition to project dissemination, the workshops will increase the DINET impact by better shaping its position and approach, and potentially by inciting collaboration and sharing of the research results.

- **International and national research conferences**. DINET will publish the main results at various international and national conferences. Appropriate conferences will be selected by the project coordinator, the WP leaders, and the task leaders. High profile conferences in the main areas of interest where the project will contribute will be primarily targeted. The large span of research domains has the potential to impact simultaneously multiple research areas. Example venues suitable for the project: IEEE International Conference on Communications (ICC), IEEE Global Communications Conference (GLOBECOM), IEEE Conference on Computer Communications (INFOCOM), ACM Special Interest Group on Data Communications Conference (SIGCOMM), International Conference on Embedded Wireless Systems and Networks (EWSN), USENIX Annual Technical Conference, USENIX Symposium on Operating Systems Design and Implementation (OSDI), USENIX Symposium on Networked Systems Design and Implementation (NSDI), IEEE Symposium on Security and Privacy, ACM Conference on Computer and Communications Security (CCS), IEEE Symposium on Security and Privacy (S&P), Network and Distributed System Security Symposium (NDSS), USENIX Security Symposium.

- **International and national industry conferences**. The results will also be disseminated at leading industry conferences dedicated to DNS, IoT, and cybersecurity such as the DNS Operations, Analysis, and Research Center (DNS-OARC), ICANN Public Meetings, IoT Forum, IoT Solutions World Congress, IETF Meetings, LoRa Alliance Meetings, RIPE Network Coordination Centre Meetings, the European Union Agency for Cybersecurity (ENISA), International National Cyber Security Centre (NCSC) One Conference, Cybersecurity Leadership Summit (SCLS).

- **Publications in journals and magazines**. DINET will also publish the results in technical journals and magazines, as well as newspapers and blogs for security enthusiasts and professionals. Targeted journals will be major IEEE, ACM, and other recognized transactions: IEEE Communications Magazine, IEEE Wireless Communications Magazine, IEEE Network Magazine, IEEE Security and Privacy Magazine, IEEE Computer, IEEE Access, IEEE Transactions on Network and Service Management, IEEE Transactions on Mobile Computing, IEEE Transactions on Parallel and Distributed Systems, Elsevier Computer Networks, IEEE Transactions on Wireless Communications, IEEE Transactions on Information Forensics and Security, ACM Transactions on Privacy and Security.

End of project and outlook. Upon the maturation and the delivery of the technical solutions, the focus of the dissemination activities will shift, in the last 6 months, to the evaluation of such solutions and their demonstrations in Use Cases. DINET achievements will be exhibited at industry fora and, after the end of the project, the official web portal will continue to disseminate the results and the exploitation activities. The software (tools and libraries) developed in the project will be maintained and proposed as a basis for further developments.

2.2.1.2 Exploitation plan

The DINET will follow an integrated approach to exploitation. The first step will be the evaluation of the business environment, analyzing the interactions of all stakeholders, and identifying market opportunities. This procedure will be carried out from the beginning of the project, early analysis and business plans will be revised according to project outcomes and up-to-date information from the external environment. This means that potential new stakeholders will be identified, carrying out an analysis of potential risks, and refining the monetization schemes initially defined. These analysis, which final results will be a set of specific exploitation strategies, will lead to propose a competitive security and privacy solution for IoT, with a clear definition of the key actors and their role in the IoT ecosystem, the added value for each one of them, the cost structures and revenue streams involved. Moreover, this integrated approach to exploitation will also contribute to the definition of the requirements fundamental in the design of the overall architecture.

Business environment. The exploitation strategy of DINET will be also focused on the perspective of several stakeholder in the specific areas of interest. The stakeholders are well represented in the consortium, from from the Top-Level Domain Registries to IoT companies with also an Internet Domain Name Registrar, an IoT operator, an innovative SME, and universities. To complete the spectrum of concerned institutions, we need to involve mobile operators that run IoT networks (the limited budget for the project made it impossible to include more partners, mobile operators). In this way, the results of the project can be exploited in all relevant domains.

Novel business opportunities can be created around the overall system, taking into account provisioning of DNS information, deploying inward and outward protection schemes, supporting confidential and privacy-friendly solutions for querying DNS, detecting privacy leaks. DINET will also extend the business landscape of IoT security with new players related to the DNS eco-system.

DINET targets a Technology Readiness Level (TRL) of 5 aiming to deliver operational demonstrations in relevant environments by the end of the project lifetime. The design of the overall security architecture will be driven by specific use cases and business scenarios, identified by key stakeholders. Research and development activities will continuously receive feedback from a double technical and business perspective. Following this approach, some prototypes will be available from the early stage of the project and it will incrementally evolve, integrating additional functionalities driven by a mix of technical research and market demands. We will analyze the security and privacy of the proposed schemes and mechanisms, and experimentally evaluate them based on some KPIs capturing the perspective of different stakeholders.
Below, we provide specific exploitation plans of each partner.

AFNIC, the French Internet registry has been involved in using DNS for IoT since 2008. The French Government wanted Afnic to work with GS1 France to set up a Federated DNS root for an IoT use-case for the supply chain Industry, thus intending to strengthen the EU position. Currently AFNIC operates a Proof of Concept DNS service for the LoRa alliance, which is another example of how AFNIC has been involved in using DNS infrastructure for real IoT networks. The AFNIC vision is to have a secure seamless IoT and has in its strategic plans to operate an IoT registry using the DNS infrastructure for IoT name resolution, security, and discovery. DINET project will be an excellent platform to achieve that strategy. AFNIC intends to use the results of DINET to standardize an approach of compressing X.509 algorithms for constrained IoT devices at IETF. The DINET project will also help AFNIC to push for secure communication of LoRaWAN using PKI rather than PSK, which is a major issue for IoT device manufacturers, product owners, and service providers. AFNIC is also part of the IoT device on-boarding group, which intends to have a generic bootstrap mechanism for all IoT devices using MUD, BRSKI, and MASA. DINET will enable AFNIC to contribute to these standards at IETF. AFNIC is also a member of the EU Alliance for IoT Innovation, wherein DINET work will help us to contribute to the WG 02 (Research) and WG03 (Standardization).

NASK. The mission of NASK, as a state-owned research institute, is to develop and employ state-of-the-art technologies to maintain its expertise in key operation areas: cybersecurity and DNS support of networks for science and education. For NASK, the DINET project is an excellent environment for creating a technology that will be crucial for both cybersecurity and DNS. This involves standards and policy making, which eventually affect wider adoption of DNSSEC in general, whose advocate NASK has been for a long time. NASK perceives IoT with properly addressed identity and security management a prerequisite for safe and successful development of IT—the vision NASK strives for and benefits from.

SIDN. As the operator of the .nl ccTLD, one of the goals of SIDN is to enhance security and stability of the Internet and DNS. The SIDN research and development department, SIDN Labs, contributes to this goal with projects that include data-driven research, protocol standardization, and prototype development. SIDN Labs already works on IoT security, and with the experience from both that project and other experience as a DNS operator, can contribute to the design and requirements of this project, as well as run prototypes of server software. SIDN intends to incorporate the knowledge outcome as well as the tools in its daily operations to increase the security and stability of the Internet.

GANDI. Gandi is one of the major registrars in France and Europe. Gandi considers the domain name as the first component in building a digital identity. Giving this paradigm Gandi had made major efforts to focus on security within its infrastructure and above all making security as friendly as possible for customers providing auto SSL certification auto DNSSEC tools. In the frame of DINET Gandi is interested in exploring and providing new security mechanisms that are focused on IoT use cases. Thanks to DINET architecture and solutions Gandi aims to enforce its position as a safe registrar and take the lead in the IoT registrar market.

ODINS. OdinS is an ICT SME focusing on developing and selling more competitive products and solutions based on research and innovation results obtained in R&D collaboration projects. In DINET, the exploitation objectives for OdinS are to improve its cybersecurity techniques for IoT devices. In particular, we will integrate Manufacturer Usage Description (MUD) and Bootstrapping Remote Secure Key Infrastructure (BRSKI) in the on-boarding process to automate MUD generation as part of the DINET architecture. For OdinS, these improvements are essential for our cybersecuriy products to cover new cybersecurity scenarios of IoT deployments that are requesting cost-effective and secure solutions. OdinS will leverage the results of the DINET project to improve its IoT devices and platforms with avanced cybersecurity features that are constantly being enhanced by OdinS, thus creating more user-friendly interfaces for potential groups of non-technical users in IoT environments. With the innnovations of the DINET project, OdinS will extend its IoT devices and platforms to successfully address new niches in the growing market of cybersecure products that represent an excellent business opportunity.

SIEMENS. SIEMENS, in the frame of DINET, is interested in exploring and validating a DNS-based architecture to enhance the trust, security, and accountability in the Industrial IoT (IIoT) environment. SIEMENS brings in its expertise from the industrial world to contribute to the overall architecture design and requirement definition. As part of the validation of the DNS-based architecture in the IIoT, SIEMENS will compare the use of traditional PKI tools with the novel DNS-based approach proposed in DINET. In particular, within the scope of DINET, SIEMENS wants to gain a good understanding of security technologies (e.g. X509 compression, DNS based enrollment and validation techniques, etc.) that can obsolete, partially or entirely, a PKI as it is used today in IIoT. SIEMENS expects that the outcome of DINET will pave the way for a more streamlined and simpler approach to securing the IIoT device life-cycle management. Hence, SIEMENS will exploit the outcomes of DINET by bringing this technology to its IIoT product lines and businesses.

SIGNIFY. Signify is the industry leader in connected lighting—we are the lighting company for the Internet of Things. As of end Q2 2019, we have installed more than 53 million connected light points. Through its participation in DINET, SIGNIFY is interested in exploring, designing, and validating a DNS-based trust architecture for connected lighting in consumer and professional environments. Signify brings practical knowledge and requirements from successfully deploying connected lighting in homes, offices, industries and cities. Signify will also help design the architecture to ensure that it can be further used in its future product lines and businesses. The validation of the DNS-based architecture on connected lighting will prove the viability of this technology for commodity IoT in general and help adoption across other IoT industries.

TTI. The Things Industries is the company behind building the technology and operating The Things Network, the biggest global LoRaWAN network. The society expects the installed base of low power wide area network (LPWAN) devices to grow in the billions in the coming years. As conventional PKI does not fit constrained LoRaWAN devices, The Things Industries believes in the objectives of DINET, to simplify PKI and use the existing DNS as a trust-layer for (primarily) activating devices, while being fully compatible with LoRaWAN. Considering the complementary character, The Things Industries will also contribute the tangible outcomes of DINET via its Contributor membership level to the Technical Committee of the LoRa Alliance, in which it is already closely collaborating with the joint DINET partner AFNIC.

We present below a common plan for the universities, and then some additional aspects per partner.

All Universities. They aim at developing cutting edge research and exploit the research results through patents, licensing, and creating start-ups based on the developed mechanisms and prototypes. They will also take advantage of the research experience gained in DINET to enhance teaching and training as well as to further advance research in the field. The knowledge acquired in the project will be used to provide consulting services to business and industry as well as to amplify collaboration with a number of national and regional industrial partners.

INP. INP has plans for creating a startup company to offer services of dealing with the DNS infrastructure. We believe that there is a need for a company that placed between end-users, Domain Name Registrar, and Top-Level Domain Registries will provide a service of provisioning required cryptographic material and signatures in DNS, and registering/signing/verifying the identities of IoT owners or providers.

FUB. FUB is an academic institution that is not only renowed for scientific excellency but also for being successfully involved in research transfer. DINET will strengthen its research transfer capacity in two ways. First, it will expand standardization activities of the involved research group towards DNS, which will improve European visibility in global Internet standardization. At the moment, we are only involved in IETF working groups related to secure inter-domain routing and IoT. Second, as a co-founder of RIOT FUB works on improving the current state of this open source software used by leading companies such as Cisco, MSA, and Continental. DINET will enable FUB not only to continue maintaing RIOT but also to add utmost important security features. This will lead to a European, secure multi-purpose platform for constrained IoT. As a result, DINET will increase trust in IoT, finally improving existing products and services as well as creating new business opportunities.

INSA. INSA-Lyon will also use the project results to further advance research in Security, Privacy, and IoT.

UZH. The project will allow UZH to strengthen its experience and knowledge in security of DNS and IoT devices. It is worth noting that UZH has already successfully conducted several nationwide Innosuisse/CTI technology transfer projects[9]. Morover, CSG helped to establish a couple of start-up companies such as modum.io[10], axelra[11], or AirGap[12]. The gained experience will, therefore, allow UZH to run future technology transfer activities supported by public or private partners as attractiveness of UZH will increase.

WUT. WUT is strongly involved in teaching activities at various levels and will extend the curriculum for BSc and MSc students with a course on "Cybersecurity".

Contribution to Standards. The DINET consortium considers standardization as the key instrument for promoting the project results to the industry so our exploitation plan includes active participation in the standardization process. Several partners are already involved in the work of standardization committees and have the necessary expertise and the critical mass to strongly influence the standardization process. The main areas of expected contributions to standards are mainly related to IETF and ICANN as well as IEEE and LoRa Alliance.

IETF. Groups related to the project are the following: COSE (CBOR Object Signing and Encryption), DOH (DNS Over HTTPS), ANIMA (Autonomic Networking Integrated Model and Approach), DPRIVE (DNS PRIVate Exchange), LAKE (Lightweight Authenticated Key Exchange), DNSOP (Domain Name System Operations), OPSAWG (Operations and Management Area Working Group), ACME (Automated Certificate Management Environment), LPWAN (IPv6 over Low Power Wide-Area Networks), and DOTS (DDoS Open Threat Signaling). Other relevant groups include: DICE (DTLS In Constrained Environments), ACE (Authentication and Authorization for Constrained Environments), DNSSD (Extensions for Scalable DNS Service Discovery), CORE (Constrained RESTful Environments), and OAUTH (Web Authorization Protocol). Moreover, we will attend interoperability events that will be held in conjunction with the IETF and are related to DINET; we expect at least one such interop event per year. Furthermore, UZH will also explore its ties to IETF through the contacts acquired through the completed IPFIX WG, in which the Tiny IP Flow Information Export (tinyipfix) was specified for constrained devices [50].

ICANN. The Security and Stability Advisory Committee (SSAC) advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services such as WHOIS). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. SIDN is memeber of SSAC.

IEEE 802. The IEEE 802 holds activities on privacy consideration in network protocols and in particular on random and changing identifiers. INSA-Lyon participate to those activities and will work to promote solutions developed in DINET within related working groups.

LoRa Alliance. AFNIC and INP are members of the LoRa Alliance and will promote the results of DINET giving them as much visibility as possible.

Contribution to open source initiatives. DINET involves stakeholders of open source projects that are key for the IoT. For example, FUB is significantly contributing to steering the RIOT community. FUB regularly co-organizes the RIOT Summit, the yearly get-together of the RIOT community. To increase third party contributions and involvement from the very beginning, we will report about DINET at the Summit in the first year of the project. We will also organize bi-weekly developer meetings, including remote participation option. Regularly organized Hack'n'Acks will allow to meet personally and work face-to-face on open problems. Based on our previous experiences, Hack'n'Ack events will accelerate the completion of open code pull requests.

Research Data Management and Data Management Plan. The role of research data in our project is marginal. The project will generate some quantitative research data in the form of statistics, results of experiments,

[9] https://www.csg.uzh.ch/csg/en/research

[10] https://modum.io/

[11] https://www.axelra.com/

[12] https://airgap.it/

measurements, observations resulting from experiments and demonstrations. Nevertheless, we will develop a initial, intermediate, and final Data Management Plan. Research data will be managed in the project in line with the following principles: all research data will be used in accordance with the good ethical academic practices to achieve the project objectives and the ownership of the research data belongs to the researchers and corresponding partners.

2.2.1.3 Strategy for knowledge management and protection

The DINET project deals with innovative concepts and solutions for applications with a strong market potential. Hence, a significant amount of Intellectual Property (IP) will be most probably generated during the project and will require significant measures to be protected. The partners involved in the project have substantial prior experience in Research and Innovation collaborative projects: all have therefore agreed to the general principles on which IPR will be managed and allocated. These principles are in line with the Grant Agreement and will be translated in specific rules in the Consortium Agreement that will be signed by the partners before the start of the project.

The main aspects that will be included in the Consortium Agreement will concern the ownership of Foreground, the access rights to Foreground and Background, and the protection of Foreground. Concerning these aspects a consensus has been reached in the consortium about the principles to apply:

- Ownership of Foreground: The Foreground resulting from the project belongs to the partner generating it. When the Foreground is generated jointly by several partners, and it is not possible to distinguish their individual contributions, it will be jointly owned unless the partners concerned agree on a different solution..

- Access rights to Foreground: As for access rights to Foreground of each partner, the conclusion of specific agreements between the concerned partners must be required. Access rights to another partner's Foreground shall can be granted upon written request. The granting may shall be made conditional on the conclusion of specific agreements in order to ensure that the requested Foreground is used only for the declared purpose in the frame of the project and under a confidentiality engagement. It will be also possible to conclude agreements with the purpose of granting additional access rights, for example access rights to third parties. As general rule, access right to one partner's Foreground will be granted on a royalty-free basis to other members of the consortium in the frame of the project activities.

- Access rights to Background: Access rights to Background of one partner shall be granted to another partner upon written request provided that the requested Background is necessary to the partner to carry on its own work during the project. As for access rights to Background Foreground of each partner, the conclusion of specific agreements between the concerned partners must may be required. A specific list of partners' Background that will be excluded by this agreement will be established before the start of the project and included in the Consortium Agreement.

- Protection of Foreground: Where Foreground has a potential for industrial or commercial application, its owner shall provide for its adequate and effective protection, in conformity with relevant legal provisions and rules established in the Consortium Agreement. Dissemination of Foreground will be made in a way compatible with the protection of IPRs (Intellectual Property Rights), confidentiality obligations and legitimate interests of the owners. Therefore, before any Foreground is made available to the public, the other beneficiaries will be informed and may object if their legitimate interests in relation to the Foreground could suffer great harm (for instance, in case a protection of the Foreground is decided).

These principles have been used in the past successfully and will guarantee a strong foundation for managing the generated knowledge and intellectual property. They will be further developed in the Consortium Agreement that will legally bind all the partners.

2.2.1.4 Open Access to Publications

DINET commits to provide open access to all publications generated by the project. It will publish the results in journals, conference proceedings and selected open access journals. Open access to project publications will be provided according to the "gold" model: open access to the peer-reviewed publication is provided immediately, often by paying a fee to the publisher. We still provide a copy of the publication in the project repository. In addition, all public deliverables of the project will be made freely available on the project website.

2.2.2 Communication Activities

The project will undertake a strategically planned communication process that spans the duration of the project to communicate its activities and promote the results. We will consider multiple audiences, including the media and the public, and possibly engaging in a two-way exchange. For communication activities, the project will:

- identify target audiences and stakeholders, and define the objectives of communication measures tailored to the needs of the audiences,
- propose a solid communication strategy with a realistic plan on how to reach the objectives,
- set up the different channels, tools, and mechanisms to implement the communication plan and reach the target audiences,
- take advantage of monitoring the innovation progress and communicate on the innovation elaborated during the project,
- reach out to society and show the impact of adequate security and privacy solutions on IoT,
- monitor the impact of the communication and identify opportunities that can maximize visibility.

The potential target groups of the audience and communication objectives are as follows.

Potential target groups of the audience	**Communication objectives**
• Industry, SMEs, and Entrepreneurs. • Participants, project partners, and relevant stakeholders active in the IoT and Security European projects. • Technology Clusters (like IERC, Digital Business Innovation, Digital Agenda, Innovation Union), research communities, associations, federations (like TTN IFIP, NetFutures). • Researchers and academics working in universities, research centres, R&D departments of industry. • Policy Makers (EC Directorates and Units, Ministries and Governments, Regulatory Agencies, Standardisation Organisations (IETF, ICANN, IEEE, LoRa ALliance)). • General Public.	• Provide a clear view of the project goals and its results. • Create an active community of potential users and organizations interested in the project results. • Create awareness of the project among the full range of potential adopters and users. • Establish liaisons with other projects and initiatives for knowledge and innovation transfer. • Support the dissemination and exploitation of results by formulating adapted key messages, and prepare adapted communication material. • Make the results recognized by research communities, standardisation bodies, potential users, policy-maker institutions.

The project will implement the following communication measures:

- Project presentation templates – all Target Audience Groups.
- Project factsheet – all Target Audience Groups.
- Project website – all Target Audience Groups.
- External stakeholder engagement platforms – Industry, SMEs, and Entrepreneurs. Policy Makers
- Social channels (Twitter, LinkedIn, Facebook, Snapchat) – all Target Audience Groups.
- Video channel (YouTube) – all Target Audience Groups.
- Newsletters – all Target Audience Groups.
- Joint events, workshops, round tables – Industry, SMEs, and Entrepreneurs. Researchers and academics. Technology Clusters.
- Demonstration, show cases, exhibition stand – Industry, SMEs, and Entrepreneurs. Researchers and academics. Technology Clusters.

3 Implementation

3.1 Work plan — Work packages, deliverables, and milestones

3.1.1 Overall strategy of the work plan

DINET will achieve its objectives by conducting high quality research structured in seven work packages shown in Figure 6:

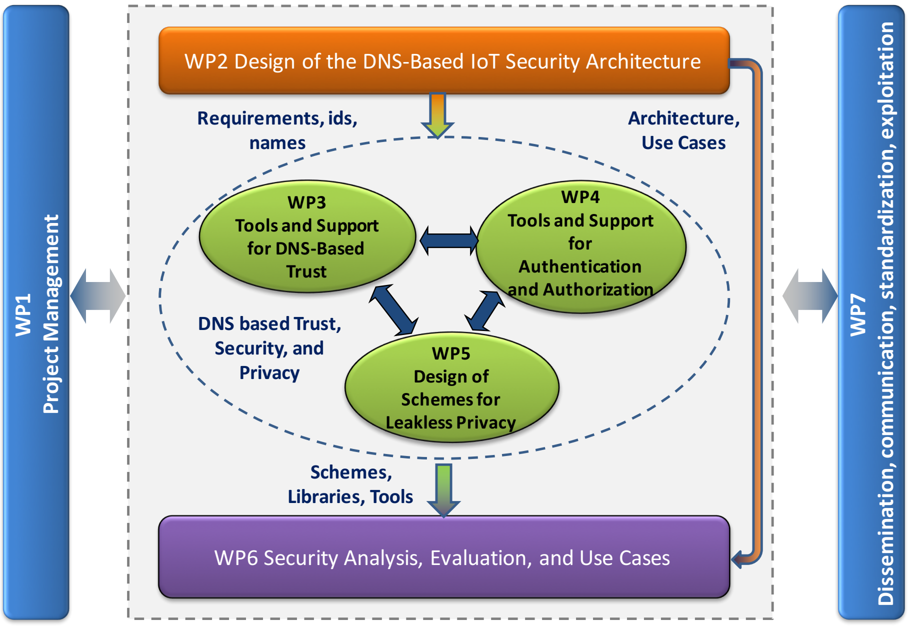

WP1
Project Management
WP2 Design of the DNS-Based IoT Security Architecture
Requirements, ids, names
Architecture, Use Cases
WP3
Tools and Support for DNS-Based Trust
WP4
Tools and Support for Authentication and Authorization
DNS based Trust, Security, and Privacy
WP5
Design of Schemes for Leakless Privacy
Schemes, Libraries, Tools
WP6 Security Analysis, Evaluation, and Use Cases
WP7
Dissemination, communication, standardization, exploitation

Figure 6: Structure of work packages.

WP1 Efficient project management and interaction with the Commission.

WP2 Designing an architecture for trusted, secure, accountable, and privacy preserving IoT based on open DNS standards and minimal extensions. This work package will consider all architectural issues related to building robust security solutions for IoT devices. It will provide a framework of requirements and use cases to other work packages.

WP3 Developing required mechanisms and solutions for trust support based on the DNS infrastructure. In this work package, we will define APIs and develop tools for provisioning of the required information in DNS records.

WP4 Designing and developing support for authentication and authorization of IoT devices. This work package will develop the DNS library for IoT devices, tools for secure device on-boarding, and inward and outward device protection.

WP5 Designing and implementing mechanisms and solutions for preserving privacy. In this work package, we will develop schemes for hiding identities and metadata, DNS query encryption, and privacy-enabling mechanisms based on machine learning to identify and visualize privacy leaking parts of communication.

WP6 Experimentally analyzing, evaluating, and validating the proposed mechanisms and solutions with target Use Cases. We commit to testbed deployment and experimental validation with three Use Cases: i) secure IoT device enrollment in LoRa and IEEE 802.15.4 networks, ii) secure deployment of RIOT IoT devices, and iii) secure management of Industrial IoT devices.

WP7 Wide communciation and dissemination of project results, pushing innovative solutions to standardisation bodies (IETF, ICANN, LoRa Alliance, IEEE), exploiting the technology developed in the project, and stimulating the reuse of project results in industry.

Figure 7 depicts the timeline (Gantt chart) of the project.

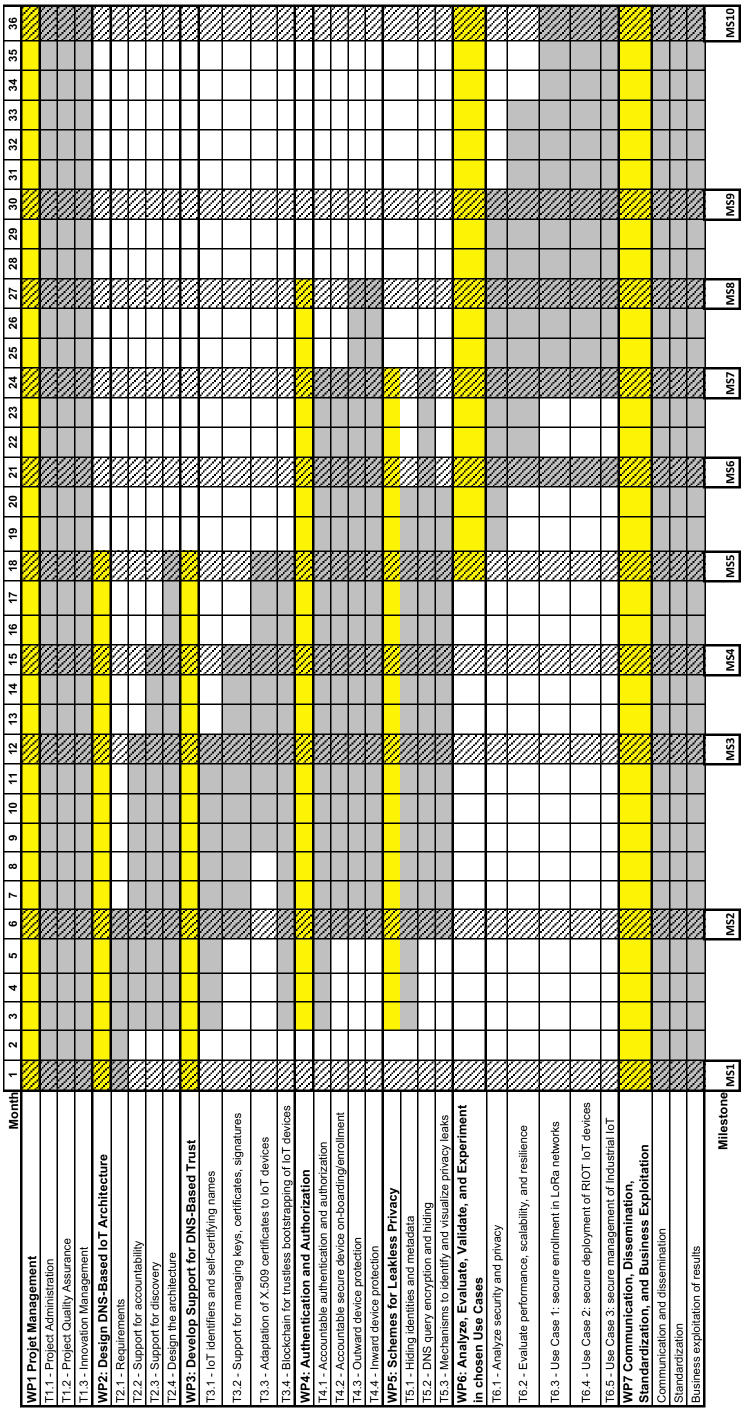


Figure 7: DINET Gantt chart.

3.1.2 Detailed work description

WP1

Project Management **Lead: INP**

No.	**1**	2	3	4	5	6	7	8	9	10
Partner	**INP**	AFNIC	NASK	SIDN	GANDI	FUB	INSA	UZH	WUT	AIRBUS
PMs	20	1	1	1	1	1	1	1	1	1
No.	11	12	13	14						
Partner	ODINS	SIEMENS	SIGNIFY	TTI						
PMs	4	1	1	1						

Start month: M1 End month: M36

Objectives: This work package will ensure that the project is successfully and efficiently managed. The specific objectives are the following:

- undertake the technical coordination and operational administration of the project, including an effective system of exchange and communication within the project consortium,
- ensure smooth and effective reporting to the EC, according to the H2020 requirements,
- monitor the overall performance of the project and ensure its progress according to the contractual obligations and the quality procedures,
- manage innovation emerging from technical activities and IPR,
- manage and mitigate identified risks.

Description of Work:

This work package will be in charge of the project coordination (both from the administrative and technical point of view), technical and financial reporting, risk and quality management, innovation and IPR management, promotion, and exploitation of the project results. INP and the Project Manager lead the work package, they are responsible for managing the project according to the grant agreement (GA) on behalf of all beneficiaries. ODINS, represented by the Innovation Manager, will support the Project Manager in innovation management and exploitation of project results.

Task 1.1 [Lead INP] – Project Technical, Administrative, and Financial Management (M1-M36).

Partners involved: all.

This task concerns project coordination, technical and financial reporting, risk management, quality management, and data management.

The Project Coordinator will schedule a project implementation plan and allocate sufficient administrative staff time to allow for the project to be operated in the predicted time frame and meet successfully its objectives. These actions include:

- project management structures and procedures,
- monitoring and supervising the project implementation plan,
- performing reviews, checking milestones and deliverables,
- organizing periodically the Project Coordination Committee,
- organize the project Advisory Board for including strong industrial and research participants in collaboration with the scientific and executive management and the partners, the financial management,
- definition of the initial, refined, and final data management plan,
- reporting procedure definition,
- meeting management,
- consortium agreement preparation and signing,
- administers funds according to the terms of the Grant Agreement and the consortium agreement,
- verifies with the coordinator that cost statements comply with performance and deliverable production, assures partners comply with the audit certificate requirements, collects cost statements and certificates for sending to the EU.

Additionally, the technical coordination is performed by the Technical Manager of DINET, which is performed in close observation of progress made in the technical fields in the context of all WPs, the co-ordination and monitoring of the WP leader activities, and the overview of all technical outcomes (reports, software, experimental data, etc.) produced within DINET. The task aims to help the Coordinator in monitoring the pace of the work, to guarantee the compatibility and complementarity of the followed approach, to preside over technical meetings and propose mitigation and resolution strategies to technical problems. Particularly, the activity includes:

- The monitoring of the technical results against the technological objectives of DINET.
- The inter-relation of the work between the different WPs, chaired by the Technical Manager.

Technical meetings will be organized to promote the sharing of knowledge and the synergies between the various work packages. Furthermore, guidelines and advice to partners on Intellectual Property Rights (IPR) issues and patent issues will be developed. Consulting will be provided to partners to ensure early and correct intellectual property rights protection, whilst the protection mechanisms and procedures themselves will be provided. Finally, procedures and tools are foreseen to perform fast and effective communication in the project. Activities to be performed in this task are related to the implementation and administration of an online platform for collaboration among the project partners.

- Tools for collaborative document handling.
- A Web-based git repository for collaborative software will be driven, installed, and operated by task lead due to the specification of the test-bed.
- Mailing Lists for easy communication.

This list is non-exhaustive and if needed, other necessary tools will be provided to facilitate the cooperation within the consortium. While this task is focused on technical support for the internal organization and efficiency, the activities related to Web-site set-up and maintenance fall within the scope of dissemination activities, since are also related to the communication outside the project.

INP will lead the Data Management Plan (DMP). DINET will collect and analyze data and DMP will define how research data will be handled. After its initial version at M6, DMP will evolve to take into account possible needs, expectations, and framework conditions.

INP will be supported by IESA (cf. definition of Third Parties) linked to INP as a Third Party under the option of 41.2 in the grant agreement (administration of a dedicated bank account).

Task 1.2 [Lead INP] – Quality Assurance (M1-M36).

Partners involved: INP.

Project quality control ensures technical progress and high quality of the expected outcome. The Project Manager supervises the project according to the implementation plan. The quality methodologies and procedures will refer to the following aspects:

- consistency between time schedules, activities, and milestones,
- respective responsibilities of the partners,
- supervising development, quality, testing, configuration, and maintenance
- appropriate tools for planning, monitoring, and progress reporting will be used.

Task 1.3 [Lead ODINS] – Innovation Management (M1-M36).

Partners involved: INP, ODINS.

This task mainly consists of the coordination of innovation and research activities carried out by the consortium among different work packages and the monitoring of the ongoing progress. We aim at regularly monitoring the innovation progress of each WP in order to ensure that technical objectives are met. The project coordinator will be informed of any visible deviation in the technical directions and time. The project proposes a process of innovation and IPR management capable of: i) monitoring the state of the art of the relevant technological developments and innovation, ii) identifying and managing IPR, and iii) managing the innovation emerging from the project. The results of this task will be presented in the periodic activity reports.

Deliverables:

D1.1 Project Implementation and Monitoring Plan (INP). M3
Full-scale plan for project management defining all necessary procedures.

D1.2 Initial Data Management Plan (INP). M6
Initial plan for the management of all data generated or collected in the project.

D1.3 First Periodic Activity Report (INP). M18

D1.4 Refined Data Management Plan (INP). M18
Refined plan for the management of all data generated or collected in the project.

D1.5 Final Data Management Plan (INP). M36
Final plan for the management of all data generated or collected in the project.

D1.6 Final Project Report (INP). M36

WP2

Design of the DNS-Based IoT Security Architecture — Lead: INP

No.	**1**	2	3	4	5	6	7	8	9	10
Partner	**INP**	AFNIC	NASK	SIDN	GANDI	FUB	INSA	UZH	WUT	AIRBUS
PMs	10	6	8	4	4	8	6	3	4	6
No.	11	12	13	14						
Partner	ODINS	SIEMENS	SIGNIFY	TTI						
PMs	8	10	10	1						

Start month: M1 End month: M18

Objectives: The objectives of this work package pertain to identifying the requirements and the Use Cases, and designing the overall security architecture. With the requirements and Use Cases at hand, we will design the overall DNS-based IoT security architecture and derive the technical specifications to guide further technical development in subsequent work packages. This work package will also define the names and roles of all entities to support for accountability and design support for discovery of IoT devices based on their properties. WP1 will prepare all the necessary input to WP2, WP3, and WP5. Some complementary work for WP2 may be necessary after M18.

Description of Work:

Task 2.1 [Lead SIEMENS] – Define requirements for IoT devices in each phase of the device life-cycle. (M1-M6).

Partners involved: INP, AFNIC, NASK, SIDN, GANDI, FUB, UZH, WUT, AIRBUS, ODINS, SIEMENS, SIGNIFY.

This task will perform requirements engineering to collect functional and non-functional requirements to support the entire life-cycle of consumer IoT and Industrial IoT (IIoT) devices. T2.1 will closely cooperate with T2.2-T2.4.

More specifically, the task will:

- identify and elicitate relevant requirements from industrial customers and consumers, e.g., via conducting workshops with stakeholders and surveys with consumers, and provide the input to WP3 on necessary tool-set, WP4 on accountability, and WP5 on privacy requirements.
- identify differences and similarities between the life-cycle of consumer IoT and IIoT devices, e.g., using Scope, Commonality, and Variability (SCV) analysis,
- finally, prioritize, and consolidate the requirements to support the use cases identified in WP6.

Task 2.2 [Lead ODINS] – Define support for accountability (M3-M12).
Partners involved: INP, AFNIC, NASK, FUB, INSA, WUT, ODINS, SIEMENS, SIGNIFY.
Using the results of T2.1 about the realisation of the IoT technical requirements, this task will derive the functional requirements to support the accountability within the DINET architecture compliant with suitably selected cybersecurity standards and frameworks. This task will be focused on designing the general architecture for supporting the accountability on IoT systems, defining both the components and roles of each entity of the architecture. The proposed architecture will be designed by replacing traditional PKI and multiple CAs with DNS acting as a trust anchor. This task will closely cooperate with T2.4 and provide input to WP4.

Task 2.3 [Lead INP] – Design support for discovery of IoT devices based on their properties (M3-M18).
Partners involved: INP, AFNIC, NASK, FUB, INSA, WUT, AIRBUS, ODINS, SIEMENS, SIGNIFY.
This task will design support for discovery of IoT devices. It will closely cooperate with T2.1 and T2.4. We will propose a naming scheme for expressing semantic information about the characteristics of devices. Geographic location is one of the characteristics that we want to encode in device names to enable queries on geographic regions. More specifically, the task will:

- provide a naming scheme for encoding device characteristics including geo-location,
- design a resolution scheme based on SRV DNS records and service discovery features to answer queries on device characteristics,
- support privacy with controlled disclosure of device characteristics to authorized entities in WP5.

Task 2.4 [Lead INP] – Design the overall DNS-based architecture (M3-M18).
Partners involved: INP, AFNIC, NASK, SIDN, GANDI, FUB, INSA, UZH, WUT, AIRBUS, SIEMENS, SIGNIFY, TTI.
This task will design the overall DNS-based architecture for trusted, secure, accountable, and privacy preserving IoT based on open IETF DNS standards and minimal extensions. We will take into account the requirements for security, privacy, and accountability defined in T2.1-T2.3, the constraints of IoT devices and their lifecycle, and the notions of device ownership and provisioning to establish the initial version of the architecture by defining all required elements and actors, and the interactions and interfaces between them. Based on the input from WP3, WP4, and WP5 on the evaluation of early prototypes, we will refine the architecture to provide the final version.

Deliverables:

D2.1 IoT security requirements and definition of Use Cases (SIEMENS). M6

This deliverable will gather the IoT security requirements, specify the details of the use cases, and define KPIs.

D2.2 Specification of the support for accountability (ODINS). M12

This deliverable will provide the specification of the mechanisms (roles, naming, logging, etc.) for accountability.

D2.3 Specification of the support for IoT device discovery (INP). M15

This deliverable will provide the specification of the support for discoverying IoT devices based on their properties while preserving privacy.

D2.4 Initial DNS-Based IoT Security Architecture (INP). M12

This deliverable will specify the initial architecture that takes into account all security, accountability, and privacy aspects.

D2.5 Final DNS-Based IoT Security Architecture (INP). M18

Based on the evaluation of early prototypes in WP3, WP4, and WP5, this deliverable will specify the final architecture.

WP3

Tools and Support for DNS-Based Trust **Lead: NASK**

No.	1	2	**3**	4	5	6	7	8	9	10
Partner	INP	AFNIC	**NASK**	SIDN	GANDI	FUB	INSA	UZH	WUT	AIRBUS
PMs	10	10	13	-	7	5	4	12	6	12
No.	11	12	13	14						
Partner	ODINS	SIEMENS	SIGNIFY	TTI						
PMs	7	4	4	1						

Start month: M3 End month: M18

Objectives: This work package aims at the development of the support for DNS-based trust based on DNSSEC and DANE. The project will define APIs and develop tools for provisioning names, keys, certificates, key hashes, and signatures. An important objective is to provide IoT devices with compact certificates or other types of information that enables lightweight authentication. Moreover, the project will propose a means based on a public permissioned blockchain for trustless bootstrapping of highly constrained IoT devices. This work package mainly concerns the scope of Registries and Registars (**REG**). The outcome of WP3 will provide the basis for the contributions in WP4 and WP5. It will also results in tools and support used in Use Cases in WP6. Some complementary work for WP2 may be necessary after M18.

Description of Work:

Task 3.1 [Lead AIRBUS] – Define IoT identifiers based on fingerprinting and self-certifying names. (M3-M12)

Partners involved: INP, AFNIC, NASK, GANDI, FUB, INSA, WUT, AIRBUS, ODINS, SIGNIFY.

This task will focus on the definition of identifiers for IoT devices. At the root of device identity is the identifier pushed by the device manufacturer into devices such as a serial number, a MAC address, an EUI-64, etc. While such identifiers are easily manageable, this kind of static information stored in memory can be extracted from a device by an attacker. To prevent this kind of attacks, the task will design and implement fingerprinting software to enable self-certification of devices based on a combination of a legacy identifier, memory footprint, and PUF (Physically Unclonable Functions). The task outcome will be a software library that can be added to device firmware to generate a unique and trustable identifier. The task will also design a scheme for self-certifying names derived from a public key to enable secure establishing of the identity of a device. The proposed architecture will use the names to support accountability of all entities. The close cooperation will be established with T3.2 on certificate management, T4.1-T4.2 on authentication and auditing, and with T6.1-T6.5 on verification of schemes developed. The leassons learnt will be provided to T2.4 for the architecture refinement.

Task 3.2 [Lead NASK] – Design and develop tools and support for managing keys, certificates, hashes, and signatures. (M6-M15)

Partners involved: INP, AFNIC, NASK, GANDI, FUB, INSA, WUT, AIRBUS, ODINS, SIEMENS, SIGNIFY.

In this task, functional requirements for DNS will get transformed into technical solutions. Necessary extensions for standard DNS capabilities will be identified, in order to support automated management of information specific to envisioned use cases. In particular, new resource record (RR) types with their use and data formats will be designed. This task is going to provide an operational API for actions corresponding to registration, revocation of certificates in traditional PKI, as well as storing extra data related to semantics of IoT usage. Implementation of API, which will be based as much as possible on existing renowned technologies and standards, will constitute the task's software outcome. The close cooperation will be established with T3.1 on IoT naming convention, T4.1-T4.2 on authentication and auditing, and with T6.1-T6.5 on verification of schemes developed. The leassons learnt will be provided to T2.4 for the architecture refinement.

Task 3.3 [Lead AFNIC] – Develop tools and mechanisms to adapt X.509 certificates to IoT constrained devices. (M9-M18).

Partners involved: INP, AFNIC, NASK, GANDI, FUB, WUT, AIRBUS, SIEMENS, SIGNIFY, TTI.

In this task, we will focus on developing tools (GUI or API) to easily enable DNSSEC signing, generate and verify TLSA resource records based on X.509 certificates created for IoT identifiers. We will evaluate the IETF standards and identify mechanisms for compressing X.509 certificate and adapting them to constrained IoT environments. We will focus on developing tools for the identified compression mechanisms so that these tools could be used in industries for a mass IoT scenario. T3.3 will closely cooperate with T2.4 and impact on T6.1-T6.5.

Task 3.4 [Lead UZH] – Design and develop a public permissioned blockchain for trustless bootstrapping of IoT devices (M3-M18).
Partners involved: INP, NASK, UZH, AIRBUS, ODINS, SIGNIFY.
This task will specify and implemented the blockchain suitable for IoT devices and its consensus mechanism. We will implement a full node that allows trust anchors to write data to the blockchain and a lightweight IoT client to provide read-only access to the blockchain. IoT devices will bootstrap trust based on a trusted list of IP addresses or DNS entries leading to the set of blockchain bootstrap nodes as well as a small sized genesis blocks embedded into the device. Then, it will extract the necessary information (e.g., DNS root key) from the blockchain. T3.4 closely cooperates with T3.3 to adopt the X.509 certificates for the IoT world and efficiently store the data in the blockchain (cf., COSE, EDHOC). It will cooperate with T6.1-6.5 to validate the architecture and evaluate its performance and with T2.4 on necessary architecture refinements.

Deliverables:

D3.1 Low-level identifiers and self-certifying names. (AIRBUS). M12

This deliverable will report on the outcome of Task 3.1 on the use of fingerprinting and PUF to derive identifiers, on the way of creating self-certifying, and encoding device properties in semantic names.

D3.2 Tools for managing keys and signatures. (NASK). M15

This deliverable will report on how API for management of DNS data necessary to accomplish the project goals was designed and implemented.

D3.3 Adaptation of X.509 certificates to constrained IoT devices (AFNIC). M18 This deliverable will produce a report on mechanisms to adapt X.509 to constrained IoT environments, will develop tools to create X.509 certificates for IoT devices for both IoT and the Internet, and will make available the open source version of the tools developed in the project under BSD-2 license category.

D3.4 Tests and evaluation of the tools developed in WP3 (NASK). M18

This deliverable will provide the results of the tests of the tools developed in this WP.

D3.5 Design and development of a blockchain for bootstrapping IoT devices (UZH). M18

This deliverable will report on the design and development of the blockchain developed in T3.4.

WP4

Tools and Support for Authentication and Authorization **Lead: AFNIC**

No.	1	**2**	3	4	5	6	7	8	9	10
Partner	INP	**AFNIC**	NASK	SIDN	GANDI	FUB	INSA	UZH	WUT	AIRBUS
PMs	11	13	4	13	-	7	4	4	14	5
No.	11	12	13	14						
Partner	ODINS	SIEMENS	SIGNIFY	TTI						
PMs	11	1	13	3						

Start month: M6 End month: M27

Objectives: This work package aims at designing a generic authentication and authorization framework based on scalable DNS naming and resolution schemes adapted for IoT devices. The project proposes to define the process of dynamic secure accountable device on-boarding/enrollment and develop tools for inward and outward device protection. This work package mainly concerns the scope of devices and networks (**DEV** and **NET**). WP4 will develop the main mechanisms for Use Cases in WP6.
Some preliminary/complementary work for WP4 may be necessary before M6 and after M27.

Description of Work:

Task 4.1 [Lead AFNIC] – Design and develop support for accountable authentication and authorization. (M3-M24).

Partners involved: INP, AFNIC, NASK, SIDN, FUB, INSA, UZH, WUT, AIRBUS, ODINS, SIGNIFY, TTI.

In this task, the specification and implementation of an Authentication, Authorization Infrastructure (AAI) becomes a ground basis for accounting materializing the Authentication, Authorization, and Accountability scheme in DNS. In particular, we will cover the following aspects:

- extending the RFC 7030 EST AAI scheme with Accounting providing an EST-based *Authentication, Authorisation, Accounting* (AAA) scheme,
- providing new techniques for automatic certificate management, e.g., blockchain based certificate registration as a service that allows the blockchain-based implementation of accountability. Close cooperation with T2.1-T2.4, T3.1-T3.2 is necessary to understand the requirements, properties, identities, and certificate management of IoT devices. T4.1 will be an enabler of accountability in T4.2. The outcome of T4.1 will be evaluated in T6.1-T6.5 and will refine the architecture in T2.4.
- prototype and evaluate an IoT authoritative registry.

Task 4.2 [Lead SIGNIFY] – Define and develop tools for dynamic accountable secure device on-boarding/enrollment. (M6-M24)

Partners involved: INP, AFNIC, NASK, FUB, INSA, UZH, WUT, AIRBUS, ODINS, SIGNIFY, TTI.

This task will concern the process of dynamic secure accountable device on-boarding/enrollment/off-boarding. We will define and develop tools for bootstrapping operational identity (e.g., certificate) of a device on an access network, obtaining the required authorization tokens, and setting up the network for controlled operation of the device based on MUD descriptors. MUD files are going to be used as a way to account and report in a standardized way, personal data collection from a particular device. In this sense, MUD model will be extended to reflect a more fine grained security configuration. Close cooperation with T2.1-T2.4, T3.1-T3.2, T4.1 is envisioned to materialize accountability of the system. The verification of this task will be provided in T6.1-T6.5.

Task 4.3 [Lead WUT] – Design support for outward device protection (M6-M27).

Partners involved: INP, AFNIC, NASK, SIDN, FUB, UZH, WUT, AIRBUS, ODINS, SIEMENS, SIGNIFY.

This task will design support to protect the network against possible attacks generated by compromised IoT devices (including DDoS attacks). The standarized MUD files are going to be used as a way to specify the expected network behavior of IoT devices. Then, in order to handle deviations from the expected behavior, the distributed Software Defined Networking (SDN)-based Intrusion Detection/Prevention System (ID/PS) will materialize the outward protection part of ID/PS. Moreover, the information and descriptions of detected anomalies provided by AI will serve as a mean to automatically generate typical network security features (e.g., whitelisting, blacklisting, signatures, etc.) that can be implemented among heavily constrained IoT devices. Close cooperation with T2.4, T3.1-T3.2 is required. Veirification of the methods developed is envisioned in T6.1-T6.5.

Task 4.4 [Lead WUT] – Design support for inward device protection (M6-M27).

Partners involved: INP, AFNIC, NASK, FUB, UZH, WUT, AIRBUS, ODINS, SIGNIFY.

This task will design protection schemes against intrusions based on Explainable AI. First, we will collect datasets for training algorithms (both from real-life traffic and synthetic simulations). Then, we will cast the problem of intrusion and DDoS attacks as an anomaly detection mechanism and develop methods based on different approached to model and detect malicious behaviors. Finally, we will extend existing methods for decision making in different AI techniques (also focusing on convolutional neural architectures, which can generalize any alphanumerical data including communication packets). The performance of the developed algorithms will be evaluated. The predicted data events will help to autonomously deploy an inward protection part of the distributed Software Defined Networking (SDN)-based Intrusion Detection/Prevention System (ID/PS). Close cooperation with T2.4, T3.1-T3.2 is required. Veirification of the methods developed is envisioned in T6.1-T6.5.

Deliverables:

D4.1 Support for accountable authentication and authorization (AFNIC). M21

This deliverable will report on the Authentication, Authorization, and Accountability scheme developed in T4.1.

D4.2 Tools for dynamic accountable secure device on-boarding/enrollment (SIGNIFY). M24

This deliverable will present the tools and support for dynamic secure accountable device on-boarding/enrollment.

D4.3 Support for outward device protection (WUT). M27

This deliverable will report on the support to protect the network against possible attacks generated by compromised IoT devices.

D4.4 Support for inward device protection (WUT). M27

This deliverable will present the protection schemes against intrusions developed in T4.3.

D4.5 Tests and evaluation of the tools developed in WP4 (AFNIC). M27

This deliverable will report on the results of the tests of the tools developed in this WP .

WP5

Design of Schemes for Leakless Privacy **Lead: INSA**

No.	1	2	3	4	5	6	**7**	8	9	10
Partner	INP	AFNIC	NASK	SIDN	GANDI	FUB	**INSA**	UZH	WUT	AIRBUS
PMs	9	4	3	-	2	-	15	3	6	-
No.	11	12	13	14						
Partner	ODINS	SIEMENS	SIGNIFY	TTI						
PMs	2	6	2	-						

Start month: M3 End month: M24

Objectives: This work package aims at developing new methods for improving privacy in networks with IoT devices. Even if we protect all communication with encryption, we need to check for information leaks and improve the quality of information hiding. The project will develop multiple ephemeral identifiers and names to preserve privacy and protect IP source addresses of devices from profiling when encrypting queries with DoT or DoH sessions. Finally, the work package will develop privacy-enabling mechanisms based on machine learning to identify and visualize privacy leaking parts of communication. This work package concerns the scope of devices and registries (**DEV** and **REG**). WP5 will provide tools and support further used in Use Cases in WP6. Some preliminary/complementary work for WP5 may be necessary before M3 and after M24.

Description of Work:

Task 5.1 [Lead INSA] – Design and develop schemes for hiding information through ephemeral identifiers and names. (M3-M18)

Partners involved: INP, AFNIC, INSA, UZH, ODINS, SIEMENS, SIGNIFY.

In this task, we will design and develop schemes for hiding information through ephemeral identifiers and names. We will design a scheme based on random resolvable identifiers: pseudonyms that can be identified by parties holding a secret and appear random to others. Those identifiers will be used by devices to prevent their exposure to tracking threats while still being able to 1) communicate with other elements 2) being discoverable by trusted parties. The cryptographic material (i.e. keys) required by those mechanisms will be managed and generated thanks to the DNS concepts developed in the project. In particular, we will design scheme that can derive identifiers from the certificates found in the DANE infrastructure. Input from T2.1, T2.3-T2.4 will drive the developments in this task. The verification will happen in T6.1-T6.5. Close cooperation between T5.1-T5.3 is requierd.

Task 5.2 [Lead INP] – Design and develop schemes for DNS query encryption and hiding source IP addresses. (M6-M24).

Partners involved: INP, AFNIC, NASK, GANDI, INSA, UZH, SIEMENS, SIGNIFY.

In this task, the project will design and develop schemes for hiding sources of queries when IoT devices use DoT or DoH. We will design a scheme based on forwarding resolvers in which a device encrypts its DNS queries, sends them over DoT or DoH to a forwarding resolver, which in turn relays the queries to the authoritative server of the target domain. This last server can decrypt the queried domain and proceed with its resolution. In this way, the forwarding resolver does not know the queried domain and the authoritative server does not know the IP address of the device. The task will prototype the operation of the scheme over an experimental IoT registry possibly set up by the partner TLD Registries. We will evaluate the proposed scheme and compare its performance to Oblivious DNS and the Cloudflare onion service. Input from T2.1, T2.3-T2.4 will drive the developments in this task. The verification will happen in T6.1-T6.5. Close cooperation between T5.1-T5.3 is requierd.

Task 5.3 [Lead WUT] – Develop privacy-enabling mechanisms based on machine learning to identify and visualize privacy leaking parts of communication (M6-M21).

Partners involved: WUT.

This task will focus on developing a machine learning algorithm that can identify parts of the communication containing privacy-sensitive information. First, we will create evaluation datasets (through synthetic creation and collection of real-life traffic). Then, we will design a Siamese architecture combined with a generative model that will be trained to identify and perturb parts of the traffic corresponding to individual identities. Finally, we will develop visualization algorithms to explain the reasoning behind selecting a given part of the packet by the trained machine learning algorithm, hence providing a novel approach that follows the Explainable AI paradigm. Input from T2.1, T2.3-T2.4 will drive the developments in this task. The verification will happen in T6.1-T6.5. Close cooperation between T5.1-T5.3 is requierd.

Deliverables:

D5.1 Schemes for hiding information through ephemeral identifiers and names. (INSA). M18

This deliverable will report on the proposed scheme based on resolvable identifiers developed in T5.1.

D5.2 Schemes for DNS query encryption and hiding source IP addresses (INP). M24

This deliverable will report on the proposed scheme based on forwarding resolvers and provide a comparison with Oblivious DNS and the Cloudflare onion service.

D5.3 Mechanisms to identify and visualize privacy leaks (WUT). M21

This deliverable will provide the results of T5.3 related to the machine learning algorithms for detecting and visualizing privacy leaks.

D5.4 Tests and evaluation of the tools developed in WP5 (NASK). M24

This deliverable will report on the results of the tests of the tools developed in this WP.

WP6

Security Analysis, Evaluation, and Use Cases **Lead: AIRBUS**

No.	1	2	3	4	5	6	7	8	9	**10**
Partner	INP	AFNIC	NASK	SIDN	GANDI	FUB	INSA	UZH	WUT	**AIRBUS**
PMs	5	8	9	6	2	12	7	10	17	14
No.	11	12	13	14						
Partner	ODINS	SIEMENS	SIGNIFY	TTI						
PMs	10	15	13	9						

Start month: M18 End month: M36

Objectives: The goal this work package is to analyze the security and privacy properties of the architecture and the developed tools, and evaluate their performance, scalability, and resilience. We will use three Use Cases to validate the project results:

- secure IoT device enrollment in LoRa and 802.15.4 networks,
- secure deployment of RIOT IoT devices,
- secure management of Industrial IoT devices.

WP6 will provide feedback to WP3, WP4, and WP5 based on analyses, evaluations, and tests.

Some preliminary work for WP6 may be necessary before M18.

Description of Work:

Task 6.1 [Lead WUT] – Security and privacy analysis. (M24-M30).

Partners involved: INP, AFNIC, NASK, SIDN, INSA, UZH, WUT, AIRBUS, SIGNIFY, TTI.

In this task, the project will analyze security and privacy of the proposed architecture, experiment with possible attacks against IoT devices, and consider the threats that IoT devices may cause in their networking environments. Moreover, the complete solution developed in DINET will be assessed from the security perspective.

In particular, the task will cover the following aspects:

- security audit of the developed solutions, i.e., establishing potential weak spots, identifying potential threats, and providing recommendations.
- robustness of the privacy preserving properties provided by schemes proposed in WP5 (ephemeral identifiers and names, DNS query encryption and source IP address hiding).

Task 6.2 [Lead SIGNIFY] – Evaluation of performance, scalability, and resilience of the proposed schemes. (M21-M33)

Partners involved: INP, AFNIC, NASK, GANDI, FUB, UZH, WUT, ODINS, SIEMENS, SIGNIFY, TTI.

This task evaluates and compares the developed DNS architecture solution in different setups. In particular, the security, privacy, and trust are being evaluated against a carefully selected KPIs proving that the developed solution meets the requirements of DINET.

Task 6.3 [Lead TTI] – Use Case 1: Secure enrollment constrained IoT devices in LoRa and IEEE 802.15.4 (M24-M36).
Partners involved: INP, AFNIC, FUB, UZH, WUT, AIRBUS, ODINS, SIGNIFY, TTI.
Use Case 1: the project will test and evaluate the developed tools in secure IoT device enrollment in LoRa, NB-IoT, and IEEE 802.15.4 networks. This task will use the tools and schemes developed in other WPs in the process of secure enrollment of constrained IoT devices in two IoT networks: LoRa and IEEE 802.15.4. For the LoRa network, we will use the TTN network run by TTI.

Task 6.4 [Lead FUB] – Use Case 2: Secure deployment of RIOT IoT devices (M24-M36).
Partners involved: AFNIC, FUB, INSA, WUT, AIRBUS, ODINS, SIGNIFY.
This task will design, implement, test, and evaluate software components for RIOT to prove the applicability of DINET solutions in a popular operating system for constrained devices. The software components will be developed with high abstraction and modularity in mind to allow for extensive reuse on multiple platforms, which is particularly important when hardware-specific cryptographic primitives are used. Challenges in this task will relate to system aspects to cope with limited hardware resources of class 0 and class 1 devices. Where applicable, the software components will be contributed upstream to the RIOT master codebase, which requires extensive testing and extensions of testing infrastructures. Based on these contributions, the RIOT community will be enabled securing existing and upcoming deployments.

Task 6.5 [Lead SIEMENS] – Use Case 3: Secure management of Industrial IoT devices. (M24-M36).
Partners involved: AFNIC, WUT, AIRBUS, SIEMENS, SIGNIFY.
Use Case 3: in this task, we will implement a proof of concept that will be used to evaluate the overall DNS-based architecture, as defined in WP2, WP3, WP4, and WP5, in an industrial IoT environment. As part of the evaluation:

- we will compare several aspects of traditional secure management of devices e.g., PKI-based, vs. the novel DNS-based device management method proposed in DINET.
- we will ensure that the requirements of IIoT with usually long product life-cycles are met. Such aspects span from usability, interoperability, scalability to crypto-agility, which is more important in Industrial IoT devices in comparison to consumer IoT devices.

Deliverables:

D6.1 Results of the security and privacy analysis. (WUT). M30

This deliverable will report on the security and privacy analysis and its recommendations.

D6.2 Results of the evaluation of performance, scalability, and resilience. (SIGNIFY). M33

This deliverable will provide the results of the evaluation in T6.2 of all tools and support developed in other WPs.

D6.3 Evaluation of the proposed architecture in Use Case 1. (TTI). M36

This deliverable will provide the results of the evaluation of the proposed architecture in Use Case 1.

D6.4 Evaluation of the proposed architecture in Use Case 2. (FUB). M36

This deliverable will provide the results of the evaluation of the proposed architecture in Use Case 2.

D6.5 Evaluation of the proposed architecture in Use Case 3. (SIEMENS). M36

This deliverable will provide a proof of concept that will allow to evaluate the overall DNS-based architecture in the IIoT environment.

D6.6 Final validation report. (INP). M36

This deliverable will summarize the results of evaluations in all Use Cases.

WP7

Communication, Dissemination, Standardization, and Business Exploitation **Lead: ODINS**

No.	1	2	3	4	5	6	7	8	9	10
Partner	INP	AFNIC	NASK	SIDN	GANDI	FUB	INSA	UZH	WUT	AIRBUS
PMs	3	6	4	3	4	3	4	3	4	4
No.	**11**	12	13	14						
Partner	**ODINS**	SIEMENS	SIGNIFY	TTI						
PMs	6	3	4	3						

Start month: M1 End month: M36

Objectives: This work package is set up to ensure the best wide-scale communication and synergetic presentation of the project results. It will promote the results, disseminate them to the scientific community via journals and conferences, and contribute to standardization bodies, thereby maximizing the project expected impact as defined in Section 2.1. It will follow the exploitation plan detailed in Section 2.2. The detailed objectives are the following:

- promote and disseminate the results of the project as they become available in reputable journals, magazines, conferences.
- disseminate evolving project results by actively participating in exhibitions and/or organise events, such as conferences, workshops, special issues in magazines/journals.
- involve stakeholders (industrial or service companies, end-users, technology partners) in the research activities of the project thus leading to significant long term impact,
- contribute to standardization bodies such as detailed in Section 2.2.
- create a framework for the successful exploitation of project results and specify the exploitation plans of the project as a whole and for each partner individually.

Description of Work:

Task 7.1 [Lead GANDI] – Communication and Dissemination (M1-M36).

Partners involved: all.

Within this task, we will widely communicate on the project activities and disseminate the project results to the scientific, technical and industrial communities. This task will play the key role of making sure that the project achievements are disseminated to the interested groups of audience, each with the most appropriate scope and level of details. It will study the targeted audience, the channels through which they can be reached, customization suggestions, and the activities through which the consortium will trigger widespread awareness. Dissemination activities will be designed and executed with market outreach and exploitation activities in mind. It is planned to split the work into the following communication processes:

- Interactive Web presence including the project Web site online polls and linked to social media: Facebook and Twitter (including Twitter coverage of events).
- Media presence: e-newsletter produced every 6 months, articles and reports in the general press, press releases following milestones and press conferences at meeting/events.
- Project events: a midterm event (Open Project Workshop to report on preliminary results and gain feedback on the project progress) and a final event (Conference and Workshop to disseminate the project results to stakeholders). Joint workshops may also be organized with other H2020 projects.
- Open days: yearly events for people interested in the project who can visit project sites, learn about the work, and see a demonstration of what it can do, as well as other relevant events.
- Publications in international scientific journals and conferences (mostly IEEE and ACM, please see Section 2.2 for a comprehensive list). Project publications will be available for Open Access according to the Gold model.
- Participation in sector specific events, work-groups, and task forces at the international level.
- Integration with the existing communication channels of the partners (e.g., Web-sites/newsletters/events).

Task 7.2 [Lead AFNIC] Standardization (M1-M36).
Partners involved: INP, AFNIC, NASK, SIDN, GANDI, FUB, INSA, UZH, WUT, AIRBUS, ODINS, SIGNIFY, TTI.
This task aims at promoting the main technical results generated by the project in the relevant standardization fora. The consortium counts on some partners already active in standardization and involved in several working groups or task forces such as: IETF groups, LoRa alliance, IEEE, RIPE, and ENISA. This task will explore the possibilities of standardizing the results obtained from the DINET project, to offer new opportunities to organizations to implement and build cybersecurity services into their systems. To achieve that, the DINET consortium will create a plan to disseminate effectively all innovations made within DINET (e.g. RFCs, Best Current Operational Practices (BCOP) to the European Networks Community as part of RIPE, LoRa alliance specifications etc.). In particular, the consortium will try to impact the international standardisation bodies indicated in the Section 2.2. At the end of the project, all the results will be summarized in a deliverable on recommendations for the standard evolution (D7.3) delivered to relevant standardization bodies.
Task 7.3 [Lead ODINS] Business exploitation of results (M12-M36).
Partners involved: all.

This task aims to create an effective plan for exploiting the resulting product of DINET. This will include a business model and a plan for using the acquired knowledge and data. The exploitation plan will describe activities and impact beyond project lifetime. It will present a long-term business strategy with tangible measures, timeframes, and actions describing sustainability and market access of the project innovation. It will first consider the initial business and exploitation plan in Section 2.2 as a starting point. During the project, we will extend the plan to reflect the current status of the project and its achievements. More in details, this task will create a market and competition analysis, focusing on the identification of the exploitable results and formulating the exploitation strategy. A joint strategy will be decided for the exploitation of the results, both in general and, if possible, for individually exploitable products. Along with the exploitation plan, the task will also work on a sustainability analysis for the business and the continuous life of the project results, creating appropriate business models for the products and services which DINET produces. Finally, this task will also contribute to the exploitation models creating a storytelling around DINET aligned with its commercial exploitation.

Deliverables:

D7.1 Communication and Dissemination Plan. (GANDI). M3

Strategic plan for the detailed project communication and dissemination activities.

D7.2 Recommendations for Evolution of Standards. (AFNIC). M30

Overall report of recommendations developed throughout the project.

D7.3 Business and Exploitation Plan (ODINS). M30

Long term plan for exploitation of the project results.

D7.4 Final report on communication and dissemination activities. (GANDI). M36

Final report on accomplished communication and dissemination activities.

The table below summarizes the roles of partners within the project.

Partner Name	**Role in DINET**
INP	• Project Coordination (WP1 Leader) – Contributing to technical, administrative and financial Management • WP2 Leader – Leading (T2.3): Designing support for IoT discovery services • Contributes to developing tools and support for DNS-based trust (WP3), tools, and support for Authentication and Authorization (WP4) • Leads (T5.2): design and develop schemes for DNS query encryption and hiding source IP addresses • Contributes to Security and Privacy analysis (T6.1), evaluation of proposed schemes (T6.2), secure enrollment of IoT devices in LoRa and IEEE 802.15.4 (T6.3), communication and dissemination (7.1), standardization (7.2), and business exploitation (T7.3)
AFNIC	• Contributes to DNS security requirements (T2.2), adapting DNS-SD to IoT (T2.3), designing the overall DNS-based architecture (T2.4) • Leads adapting X.509 certificates to IoT constrained devices (T3.3), and contributes to designing support for managing cryptographic keys • Leads design of accountable authentication and authorization (T4.1), contributes to DNS query encryption, hiding (T5.2), security and privacy analysis (6.1), secure enrollment of IoT devices (T6.3) • Leads standardization (T7.2) and contribute to communication and dissemination (7.1), and business exploitation (T7.3)
NASK	• Contributes to the design of the DINET architecture (T2.4) • WP3 Leader – Leads designing support for managing cryptographic keys (T3.2), contributes to derivation of semantic names (T3.1), and adapting X.509 certificates to IoT constrained devices (T3.3) • Contributes to DNS query encryption, hiding (T5.2), security and privacy analysis (T6.1), and evaluation of the proposed schemes (T6.2) • Contributes to communication and dissemination (7.1), standardization (T7.2), and business exploitation (T7.3)

SIDN	• Contributes to the design of the DINET architecture (T2.4), to the design of the support for outward device protection (T4.3), security and privacy analysis (T6.1), and evaluation of the proposed schemes (T6.2), communication and dissemination (7.1), standardization (T7.2), and business exploitation (T7.3)
GANDI	• Contributes to the design of the DINET architecture (T2.4), designing support for managing cryptographic keys (T3.2), contributes to the design of semantic names (T3.1) and adapting X.509 certificates to IoT constrained devices (T3.3), DNS query encryption, hiding (T5.2), security and privacy analysis (T6.1), and evaluation of the proposed schemes (T6.2) • Leads communication and dissemination (7.1) and contributes to standardization (T7.2) and business exploitation (T7.3)
FUB	• Contributes to the design of the DINET architecture (T2.4), contributes to the design of semantic names (T3.1), support for managing cryptographic keys (T3.2), adapting X.509 certificates to IoT constrained devices (T3.3), using MUD for secure on-boarding (T4.3) • Leads secure deployment of RIOT IoT devices (T6.4), and contributes to evaluation of the proposed schemes (T6.2), secure enrollment of IoT devices (T6.3) • Contributes to dissemination (7.1), standardization (T7.2), and business exploitation (T7.3)
INSA	• Contributes to the design of the DINET architecture (T2.4), design of low level IoT identifiers and self-certifying names (T3.1), design of accountable authentication and authorization (T4.1), secure device on-boarding (T4.2) • WP5 Leader – leads the design and develops schemes for hiding information through ephemeral identifiers and names (T5.1) and contributes to DNS query encryption, hiding (T5.2) • Contributes to security and privacy analysis (T6.1) for RIOT devices (T6.4), communication and dissemination (7.1), standardization (t7.2), and business exploitation (T7.3)
UZH	• Contributes to requirements for IoT devices in each phase of the device life-cycle (T2.1), defines support for accountability (T2.2), the design of the DINET architecture (T2.4) • Leads public permissioned blockchain design and development (T3.4), contributes to (T3.1) with device identifiers based on PUFs as well as (T3.3) for certificate compression of IoT devices, contributes to authentication (T4.1) and accountability (T4.2) • Contributes to all tasks on security (T6.1) and performance evaluation (T6.2) as well as on the support of Use Cases by concentrating on solutions developed in WP2, WP3, and WP4 • Contributes to communication and dissemination (7.1), standardization (T7.2), and business exploitation (T7.3)
WUT	• Contributes to requirements for IoT devices in each phase of the device life-cycle (T2.1), define support for accountability (T2.2) and the design of the DINET architecture (T2.4) • Contributes to (T3.1) for designing low-level device identifiers based on PUFs, support for managing cryptographic keys (T3.2), adapting X.509 certificates to IoT constrained devices (T3.3) • Leads the design of the support for outward (T4.3) and inward device protection (T4.4) • Leads the development of the privacy-enabling mechanisms based on machine learning (T5.3) and contributes to developing schemes for hiding information through ephemeral identifiers and names (T5.1) • Leads security and privacy analysis (T6.1) and contributes to performance evaluation (T6.2) • Contributes to communication and dissemination (7.1), standardization (T7.2), and business exploitation (T7.3)

AIRBUS	• Contributes to the definition of the use cases and the design of the DINET architecture (T2.4) • Leads definition of IoT identifiers based on fingerprinting and self-certifying names and contributes to support for managing cryptographic keys (T3.2), adapting X.509 certificates to IoT constrained devices (T3.3) • Contributes to secure enrollment process definition (T4.2), based on its expertise, will also support activities related to authorization and bootstrapping based in manufacturing environment (T4.1) • Leads WP6 and contributes to all tasks in WP6 except that of performance evaluation (T6.2) • Contributes to communication and dissemination (7.1), standardization (T7.2), and business exploitation (T7.3
ODINS	• In charge of Innovation management in WP1 (T1.3) • Leads the definition ofthe specification for IoT accountability (T2.2) and contributes to the design of the DINET architecture (T2.4), • Contributes to the design of low-level device identifiers based on PUFs (T3.1), support for managing cryptographic keys (T3.2) and adapting X.509 certificates to IoT constrained devices (T3.3), outward device protection by MUD descriptions and the BRSKI protocol (T4.3), implementation support for accountable authentication and authorization (T4.1), and secure enrollment process definition (T4.2) • Contributes to the development of the schemes for hiding identities and metadata with ephemeral identifiers and names (T5.1), contributes to evaluation of performance, scalability, and resilience of the developed schemes and protocols in Use Cases 1 and 2 (T6.1, T6.3, T6.4) • Contributes to communication and dissemination (7.1), standardization (T7.2), and business exploitation (T7.3
SIEMENS	• Leads (T2.1) defining requirements for IoT device in each phase of the device life-cycle and will actively contribute to the definition of the Industrial IoT and contributes to the definition of the Industrial IoT devices Use Case and the design of the DINET architecture (T2.4) • Contributes to T3.2 and T3.3 in the design and development of support tools for the certificate life-cycle management and usage as well as X.509 certificate compression • Contributes to T4.3 by providing guidance based on its expertise with industrial environments • Contributes to the design and development of privacy enhancements for the DNS-based architecture activities in T5.1 and T5.2 • Leads Use Case 3: Secure management of Industrial IoT devices (T6.5) and contributes to analysis of security and privacy of the proposed architectures evaluating performance, scalability, and resilience in T6.2. • Contributes to communication and dissemination (7.1), standardization (T7.2), and business exploitation (T7.3
SIGNIFY	• Contributes to the use case definition and requirements for consumer and professional IoT systems (T2.1) and the design of the DINET architecture (T2.4) • Contributes to Tasks T3.1, T3.2, and T3.3 to ensure that tools for managing identifiers and PKI meet the process flows requirements in consumer and professional IoT systems • Leads tothe definition and the design of tools for dynamic accountable secure device onboarding/enrollment (T4.2) and contributes to T4.2 for designing tools and support for accountable authentication and authorization with a focus on Industry (T4.1) that meet IoT deployment flows used in practice • Contributes to T5.1, T5,2 and T5.3 to ensure privacy design and tools meet the requirements for IoT systems • Leads T6.2 and contributes to evaluation of performance, scalability and reliability, and contributes to all other tasks on evaluating different use cases T6.3, T6.4 and T6.5 • Contributes to communication and dissemination (7.1), standardization (T7.2), and business exploitation (T7.3

TTI	• Contributes to T3.3 in the design and development of support tools for X.509 certificate compression, accountable authentication and authorization (T4.1) and secure on-boarding (T4.2) • Leads evaluation in LoRaWAN and IEEE 802.15.4 (T6.3) and contributes to security and privacy analysis (T6.1) and performance evaluation (T6.2) • Contributes to communication and dissemination (7.1), standardization (T7.2), and business exploitation (T7.3

Table 3.8: Role of partners in the project

3.1.3 List of Work Packages

Table 3.9 summarizes of staff effort distributed over work packages.

Table 3.9: List of Work Packages

Work Package No.	**Work Package Title**	**Lead Partic. No.**	**Lead Partic. Short Name**	**Person Months**	**Start Month**	**End Month**
1	Project Management	1	INP	36	M1	M36
2	Design DNS-Based Architecture for Trusted, Secure, Accountable, and Privacy-Friendly IoT	1	INP	88	M1	M18
3	Develop Support for DNS-Based Trust	4	NASK	95	M1	M18
4	Design and Implement Support for Authentication and Authorization of IoT Devices	2	AFNIC	103	M3	M27
5	Design and Implement Schemes for Leakless Privacy	7	INSA	52	M3	M24
6	Analyze, Evaluate, Validate, and Experiment in chosen Use Cases	10	AIRBUS	137	M18	M36
7	Communication, Dissemination, Standardization, and Business Exploitation	11	ODINS	54	M1	M36
Total PMs				**565**		

The above table presents the effort supported by the European Commission. The actual effort of the consortium may be higher during progress of the work.

3.1.4 List of Deliverables

In total, we will provide 36 deliverables summarized in Table 3.10.

Table 3.10: List of Deliverables

Deliverable		**WP**	**Lead**	**Type**	**Diss. level**	**Deliv. date**
D1.1	Project Implementation and Monitoring Plan	1	INP	R	CO	M3
D1.2	Initial Data Management Plan	1	INP	R	CO	M6
D1.3	First Periodic activity report	1	INP	R	CO	M18
D1.4	Refined Data Management Plan	1	INP	R	CO	M18
D1.5	Final Data Management Plan	1	INP	R	CO	M36
D1.6	Final project report	1	INP	R	CO	M36

D2.1	IoT security requirements and definition of Use Cases	2	SIEMENS	R	PU	M6
D2.2	Specification of the support for accountability	2	ODINS	R	PU	M12
D2.3	Specification of the support for IoT device discovery	2	INP	R	PU	M15
D2.4	Initial DNS-Based IoT Security Architecture	2	INP	R	PU	M12
D2.5	Final DNS-Based IoT Security Architecture	2	INP	R	PU	M18
D3.1	Low-level identifiers and self-certifying names	3	AIRBUS	R	PU	M12
D3.2	Tools for managing keys and signatures	3	NASK	R	PU	M15
D3.3	Adaptation of X.509 certificates to constrained IoT devices	3	AFNIC	R	PU	M18
D3.4	Tests and evaluation of the tools developed in WP3	3	NASK	R/DEM	PU	M18
D3.5	Design and development of a blockchain for bootstrapping IoT devices	3	UZH	R	PU	M18
D4.1	Support for accountable authentication and authorization	4	AFNIC	R	PU	M21
D4.2	Tools for dynamic accountable secure device on-boarding/enrollment	4	SIGNIFY	R	PU	M24
D4.3	Support for outward device protection	4	WUT	R	PU	M27
D4.4	Support for inward device protection	4	WUT	R	PU	M27
D4.5	Tests and evaluation of the tools developed in WP4	4	AFNIC	R/DEM	PU	M27
D5.1	Schemes for hiding information through ephemeral identifiers and names	5	INSA	R	PU	M21
D5.2	Schemes for DNS query encryption and hiding source IP addresses	5	INP	R	PU	M24
D5.3	Support for QNAME minimization	5	SIDN	R	PU	M21
D5.4	Tests and evaluation of the tools developed in WP5	5	NASK	R/DEM	PU	M24
D6.1	Results of the security and privacy analysis	6	WUT	R	PU	M30
D6.2	Results of the evaluation of performance, scalability, and resilience	6	SIGNIFY	R	PU	M33
D6.3	Evaluation of the proposed architecture in Use Case 1	6	TTI	R/DEM	PU	M36
D6.4	Evaluation of the proposed architecture in Use Case 2	6	FUB	R/DEM	PU	M36
D6.5	Evaluation of the proposed architecture in Use Case 3	6	SIEMENS	R/DEM	PU	M36
D6.6	Final validation report	6	INP	R	PU	M36
D7.1	Communication and Dissemination Plan	7	GANDI	R	CO	M3
D7.2	Recommendations for Evolution of Standards	7	AFNIC	R	CO	M24
D7.3	Business and Exploitation Plan	7	ODINS	R	PU	M30
D7.4	Final report on communication and dissemination activities	7	GANDI	R	PU	M36

3.1.5 Project Milestones

We have structured the work in the DINET project according to ten milestones defined in the table below. The milestones mostly coincide with the release of work package deliverables (documents or software/tools) and major reporting periods.

Table 3.11: List of Milestones.

MS No.	Milestone Name	Related Work Package(s)	Due date	Means of Verification
MS1	Kickoff	WP1	M1	Kickoff meeting. Project Web site, collaboration tools, and project management procedures set up.
MS2	Initial	WP2	M6	Requirements of the architecture delivered in D2.1. Communication and Dissemination plan established in D7.1. Initial Data Management plan established in D1.2.
MS3	1st year	WP2, WP3	M12	Initial version of the architecture. IoT identifiers, self-certifying and semantic names defined. D2.2, D2.4, D3.1 delivered.
MS4	Intermediate 1	WP2, WP3	M15	Support for discovery and for managing keys, certificates, and signatures designed. D2.3, D3.2 delivered.
MS5	Mid	WP2, WP3	M18	Final version of the architecture. The blockchain designed and developed. Adaptation of certificates designed and tested. D2.5, D3.3, D3.4, D3.5 delivered. Refined Data Management plan established in D1.4.
MS6	Intermediate 2	WP5	M21	Privacy mechanisms designed and developed. D5.1, D5.3 delivered.
MS7	2nd year	WP4	M24	Schemes for accountable authentication and authorization designed and developed. Secure device onboarding/enrollment designed and developed. D4.1, D4.2, D5.2, D5.4 delivered.
MS8	Intermediate 3	WP4	M27	Schemes for outward and inward device protection designed and developed. D4.3, D4.4, D4.5 delivered.
MS9	Intermediate 4	WP6	M30	Security and privacy analyzed in D6.1. Recommendations for evolution of standards delivered in D7.2. Business and exploitation plan delivered in D7.3.
MS10	Final	all	M36	All proposed schemes, mechanisms, and tools evaluated. The architecture and the proposed schemes validated in three Use Cases. D6.2, D6.3, D6.4, D6.5, D6.6 delivered. Final report on dissemination activities delivered in D7.4. Final Data Management plan established in D1.5.Final report on the project results delivered in D1.6.

3.2 Management structure and procedures

This section describes the organisational structure and decision-making mechanisms of the project, matched to the complexity and scale of DINET.

3.2.1 Overall Management Strategy

The overall strategy of the DINET project management is illustrated in Figure 8.

Project Steering Committee (PSC). PSC is the highest management level of the project and will include one representative from each partner. Its role is to make decisions relating to any substantial changes necessary to the work programme or the consortium and to make strategic decisions. It will meet every 12 months.

PSC will also have the responsibility of:

- validating the proposed directives for the formulation of the Consortium joint exploitation strategy and