September 27th 2021

Extending DNS and its ecosystem for IoT

Afnic's in brief

ESTABLISHED IN 1997, AFNIC IS THE ACRONYM FOR **ASSOCIATION FRANÇAISE POUR LE NOMMAGE INTERNET EN COOPÉRATION**, THE FRENCH NETWORK INFORMATION CENTRE

Since our creation, we have managed the domain name registry in France (currently more than 3.7 million *.fr* domain names), in connection with the entire Internet ecosystem in France.

Because the ***.fr* ccTLD is a public good**, our role is considered one of general interest, consisting in **contributing on a daily basis to:**

- **a secure and stable internet;**
- **open to innovation;**
- **in which the French internet community plays a leading role.**

Afnic is involved in international bodies to promote the French vision of a secure and stable internet open to innovation.

In France, we are committed to promoting *.fr*, which embodies these same values, in order to accelerate the digital transition that will bring with it economic development but also solidarity.

That is the intent of the Afnic Foundation for Digital Solidarity, financed since 2015 by the profit generated from managing.*fr*, thus ensuring that the revenue from the common good that is the national TLD is returned to the community.

afnic | Labs

R&D Team

Doctors
Engineers
PhD Students

R&D collaborative projects

DINS*
DNS Naming and Services for Secure Seamless IoT

PIVOT*
Privacy-Integrated design and Validation in the constrained IoT

COMAR*
Classification of Compromised versus Maliciously Registered Domain

Internet standards, Alliance, Tech and Innovation WG

IETF, RIPE NCC, CENTR, Cap Digital, Systematic, IMA



Internal projects

DNS Protocol
Data analysis
Registry services innovation

Scientific Council

JCSA

Publications



DNS & IoT

Internet ≠ Internet Of Things



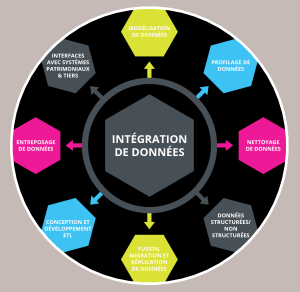
Identifier



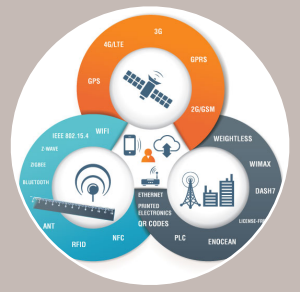
Device



Connectivity



Gateways



Networks



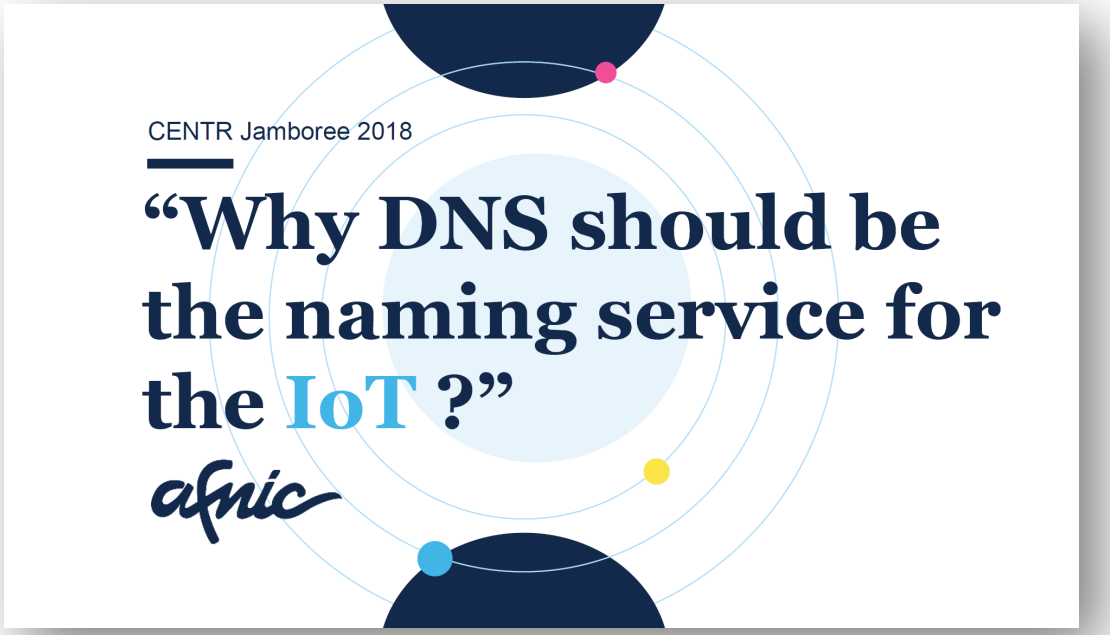
Applications



Our initial works

About naming

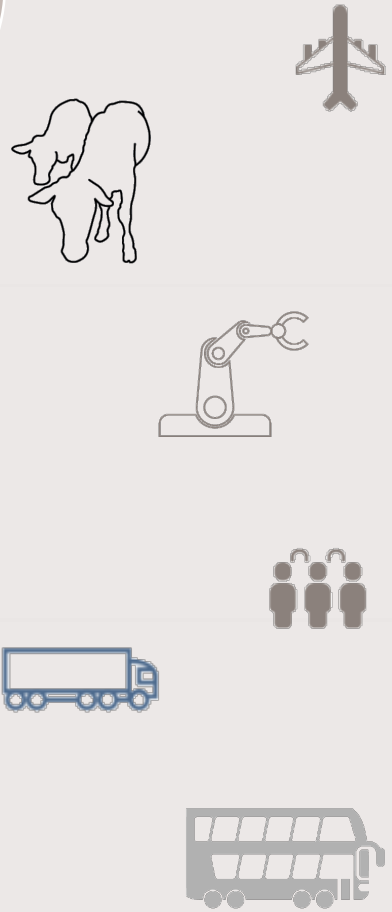




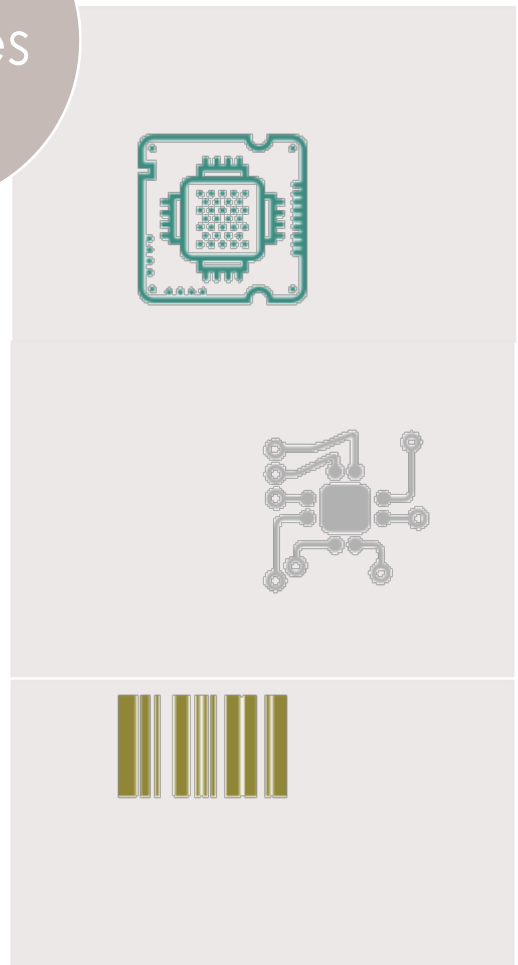
IoT : One basic concern

Making the things identifiable

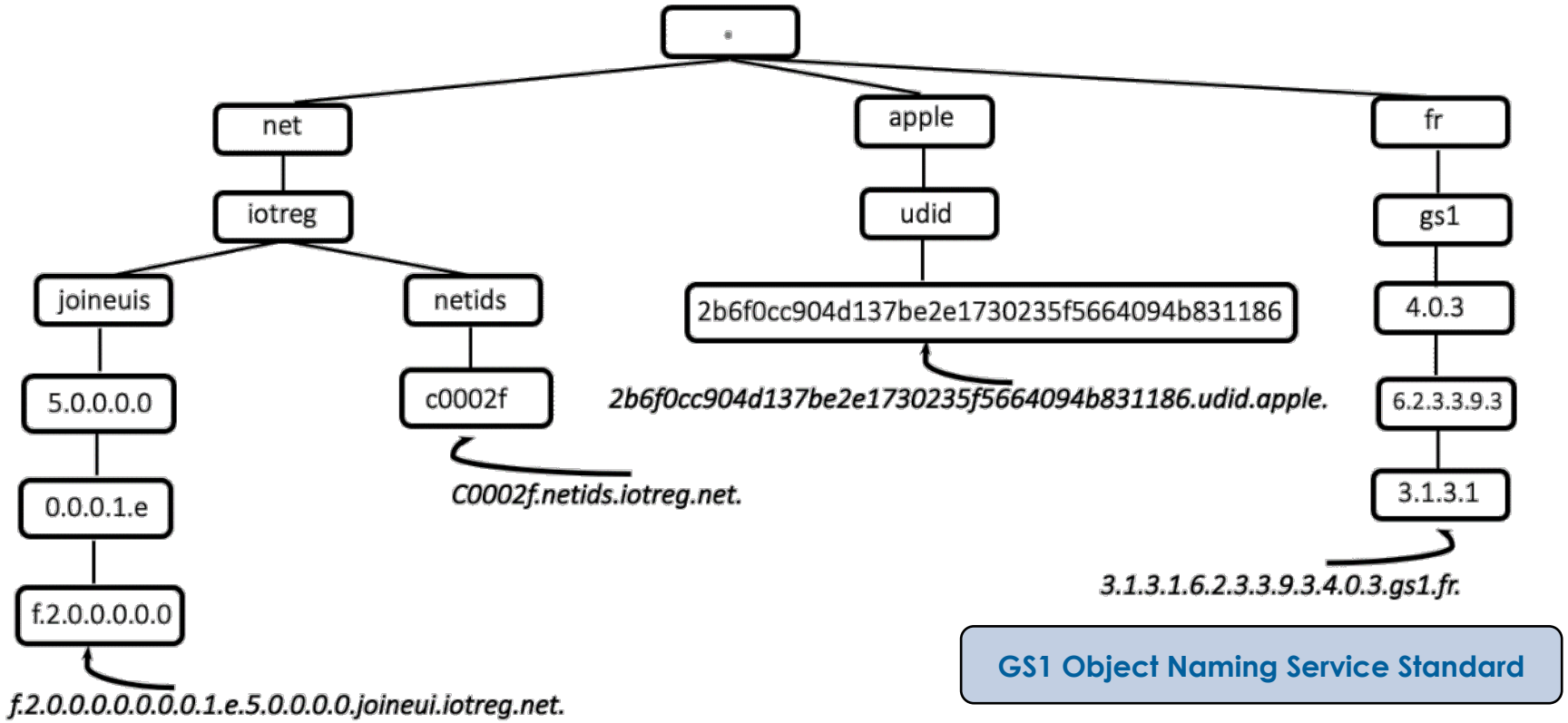
Entity of Interest



Devices



It’s about converting naming conventions into DNS zones



LoRaWAN Backend Interfaces specification

GS1 Object Naming Service Standard

As DNS registry, we know how to do it

```
$ORIGIN tld.
$TTL 5m

example         IN      SOA     ns1.example.tld. hostmaster.example.tld. (
                                90              ; serial
                                4h              ; refresh
                                15m             ; retry
                                8h              ; expire
                                4m)             ; negative caching TTL
                IN      NS      ns1.example.tld.
                IN      NS      ns2.example.tld.
                MX      10      mail.example.tld.
                IN      A       127.0.0.1

                IN TXT "v=spf1 a mx a:mail.example.tld a:www.example.tld ?all"

$ORIGIN example.tld.

ns1                     IN      A       127.0.0.2
ns2                     IN      A       127.0.0.3
www                     IN      CNAME   example.tld.
mail                    IN      AAAA    ::1
mail                    IN      A       127.0.0.4
```

Requirements for a naming service

Must be scalable

Must work for legacy and new naming conventions

Should work for hierarchical and flat identifiers

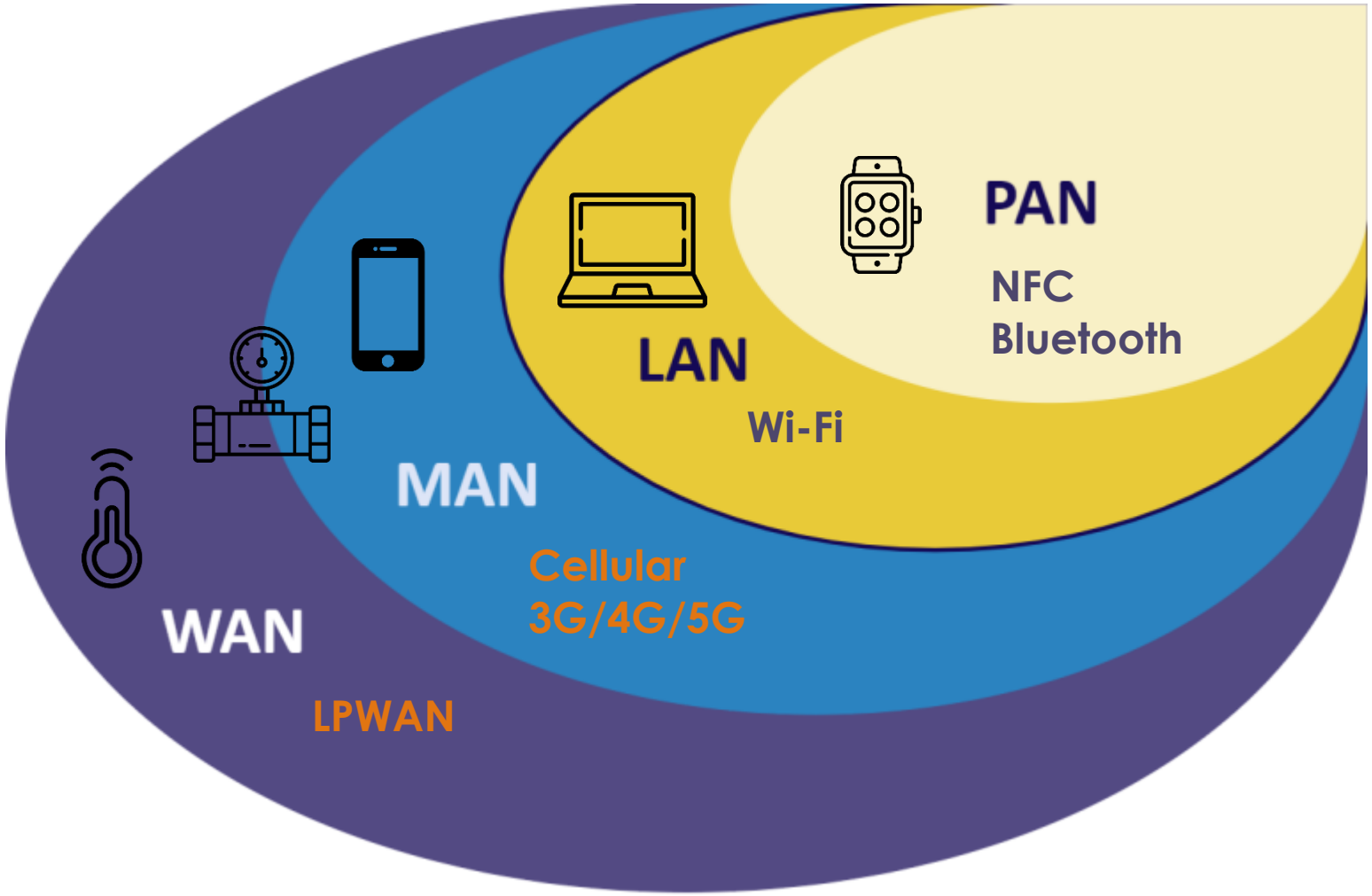


DNS satisfies all the requirements



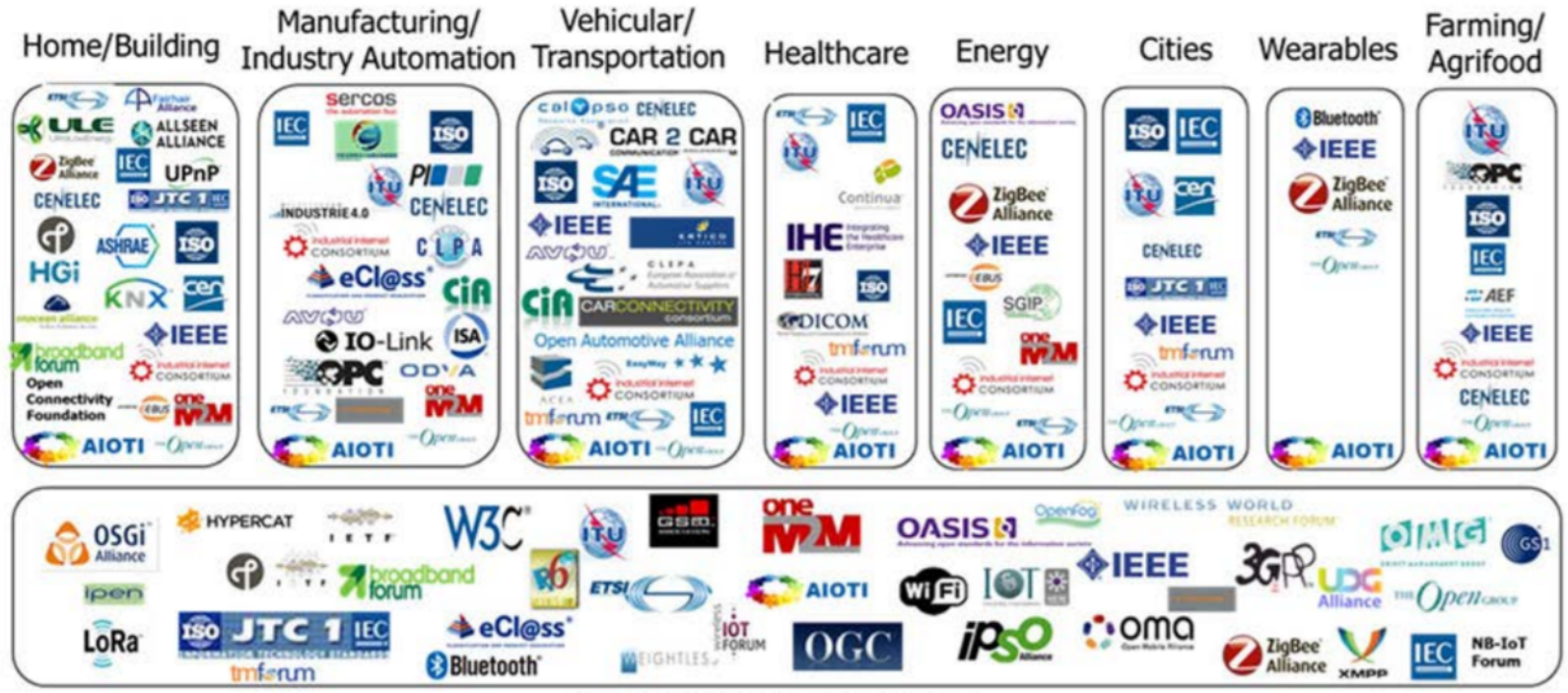
image: Freepik.com

Different ranges, different networks



Source : https://pacbasics.org/basic-network-design-principles-for-electrical-engineers/

IoT SDOs and Alliances landscape (Vertical and Horizontal domains)



Source: AIOTI WG3 (IoT Standardisation) – Release 2.6

Extending our studies

LEVERAGING THE DNS BY ADOPTING AN EVOLUTIONARY ATTITUDE

- using existing technologies

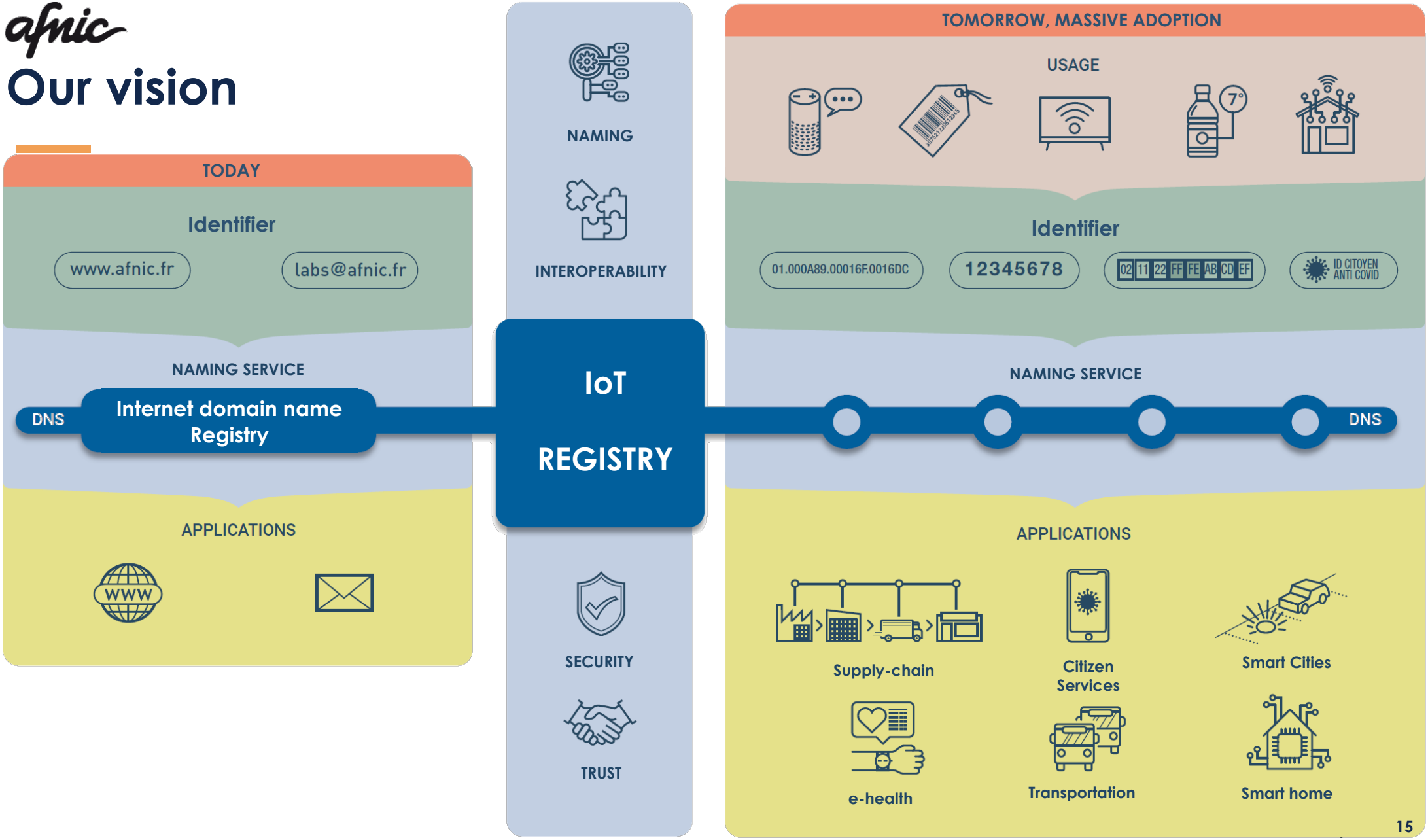
which has withstood the operational strains of the Internet
which has been there from the beginning of the Internet and still remains it's corner stone.

- adapting them to new requirements

DNS Camel



Our vision


TODAY
Identifier
www.afnic.fr
labs@afnic.fr
NAMING SERVICE
DNS
Internet domain name Registry
APPLICATIONS
WWW
NAMING
INTEROPERABILITY
IoT
REGISTRY
SECURITY
TRUST
TOMORROW, MASSIVE ADOPTION
USAGE
Identifier
01.000A89.00016F.0016DC
12345678
02 11 22 FF FE AB CD EF
ID CITOYEN ANTI COVID
NAMING SERVICE
DNS
APPLICATIONS
Supply-chain
Citizen Services
Smart Cities
e-health
Transportation
Smart home

Our contributions

Using DNS for leveraging IoT protocols and infrastructures

It’s not obvious but backing DNS in IoT services and infrastructures could help to :

- Better Interoperability
- Improve end-to-end security
- Less straightforward : optimize back-end communications and even device radio communications ➔ save energy !

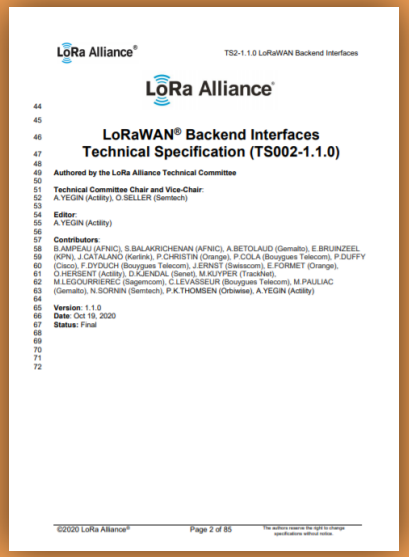


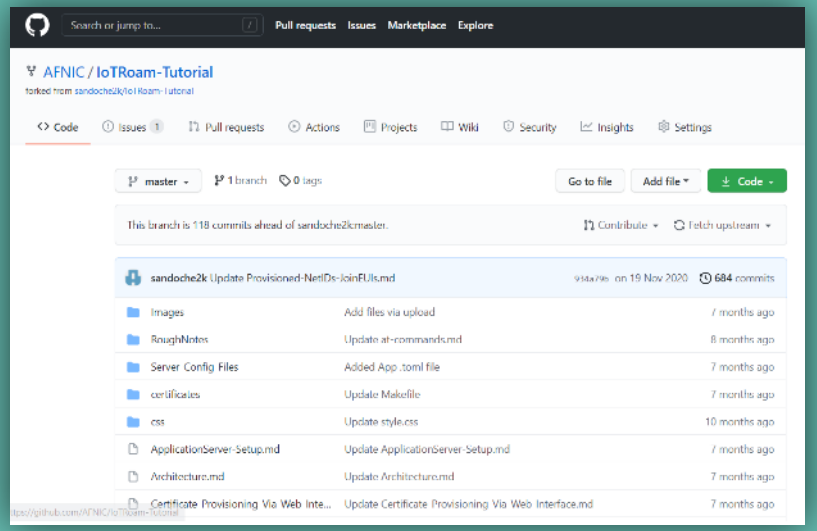
Designed by katemangostar / Freepik

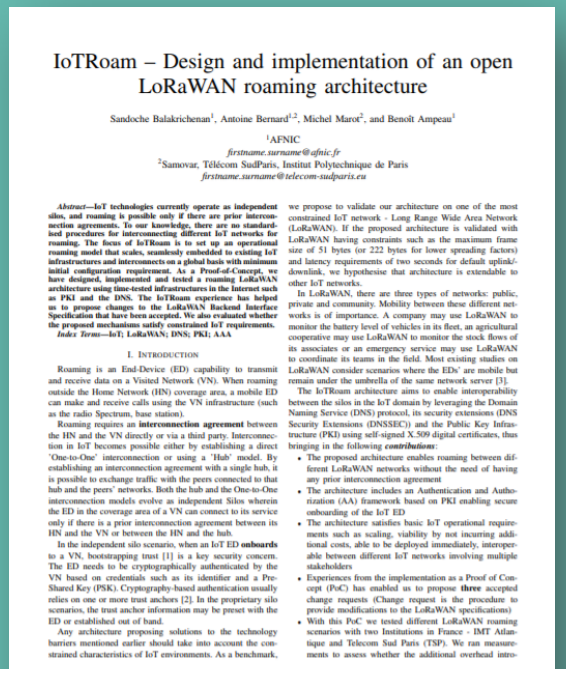
Standards / Protocols specifications

contributions









IoTRoam – Design and implementation of an open LoRaWAN roaming architecture

Sandoche Balakrichenan[1], Antoine Bernard[1,2], Michel Marot[2], and Benoît Ampeau[1]

[1]AFNIC
firstname.surname@afnic.fr
[2]Samovar, Télécom SudParis, Institut Polytechnique de Paris
firstname.surname@telecom-sudparis.eu

***Abstract*—IoT technologies currently operate as independent silos, and roaming is possible only if there are prior interconnection agreements. To our knowledge, there are no standardised procedures for interconnecting different IoT networks for roaming. The focus of IoTRoam is to set up an operational roaming model that scales, seamlessly embedded to existing IoT infrastructures and interconnects on a global basis with minimum initial configuration requirement. As a Proof-of-Concept, we have designed, implemented and tested a roaming LoRaWAN architecture using time-tested infrastructures in the Internet such as PKI and the DNS. The IoTRoam experience has helped us to propose changes to the LoRaWAN Backend Interface Specification that have been accepted. We also evaluated whether the proposed mechanisms satisfy constrained IoT requirements.**

***Index Terms*—IoT; LoRaWAN; DNS; PKI; AAA**

I. Introduction

Roaming is an End-Device (ED) capability to transmit and receive data on a Visited Network (VN). When roaming outside the Home Network (HN) coverage area, a mobile ED can make and receive calls using the VN infrastructure (such as the radio Spectrum, base station).

Roaming requires an **interconnection agreement** between the HN and the VN directly or via a third party. Interconnection in IoT becomes possible either by establishing a direct 'One-to-One' interconnection or using a 'Hub' model. By establishing an interconnection agreement with a single hub, it is possible to exchange traffic with the peers connected to that hub and the peers' networks. Both the hub and the One-to-One interconnection models evolve as independent Silos wherein the ED in the coverage area of a VN can connect to its service only if there is a prior interconnection agreement between its HN and the VN or between the HN and the hub.

In the independent silo scenario, when an IoT ED **onboards** to a VN, bootstrapping trust [1] is a key security concern. The ED needs to be cryptographically authenticated by the VN based on credentials such as its identifier and a Pre-Shared Key (PSK). Cryptography-based authentication usually relies on one or more trust anchors [2]. In the proprietary silo scenarios, the trust anchor information may be preset with the ED or established out of band.

Any architecture proposing solutions to the technology barriers mentioned earlier should take into account the constrained characteristics of IoT environments. As a benchmark, we propose to validate our architecture on one of the most constrained IoT network - Long Range Wide Area Network (LoRaWAN). If the proposed architecture is validated with LoRaWAN having constraints such as the maximum frame size of 51 bytes (or 222 bytes for lower spreading factors) and latency requirements of two seconds for default uplink/-downlink, we hypothesise that architecture is extendable to other IoT networks.

In LoRaWAN, there are three types of networks: public, private and community. Mobility between these different networks is of importance. A company may use LoRaWAN to monitor the battery level of vehicles in its fleet, an agricultural cooperative may use LoRaWAN to monitor the stock flows of its associates or an emergency service may use LoRaWAN to coordinate its teams in the field. Most existing studies on LoRaWAN consider scenarios where the EDs' are mobile but remain under the umbrella of the same network server [3].

The IoTRoam architecture aims to enable interoperability between the silos in the IoT domain by leveraging the Domain Naming Service (DNS) protocol, its security extensions (DNS Security Extensions (DNSSEC)) and the Public Key Infrastructure (PKI) using self-signed X.509 digital certificates, thus bringing in the following ***contributions***:

- The proposed architecture enables roaming between different LoRaWAN networks without the need of having any prior interconnection agreement
- The architecture includes an Authentication and Authorization (AA) framework based on PKI enabling secure onboarding of the IoT ED
- The architecture satisfies basic IoT operational requirements such as scaling, viability by not incurring additional costs, able to be deployed immediately, interoperable between different IoT networks involving multiple stakeholders
- Experiences from the implementation as a Proof of Concept (PoC) has enabled us to propose **three** accepted change requests (Change request is the procedure to provide modifications to the LoRaWAN specifications)
- With this PoC we tested different LoRaWAN roaming scenarios with two Institutions in France - IMT Atlantique and Telecom Sud Paris (TSP). We ran measurements to assess whether the additional overhead intro-

Open platform

A Federated IoT roaming infrastructure using LoRaWAN

IEEE GLOBECOM®
IEEE Global Communications Conference
7-11 December 2021 // Madrid, Spain // Hybrid: In-Person and Virtual Conference
Connecting Cultures around the Globe

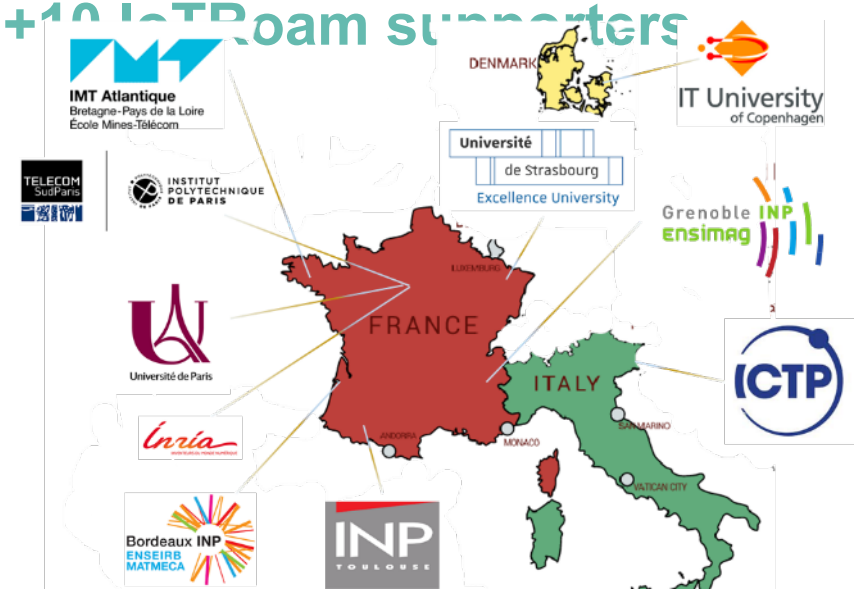
afnic

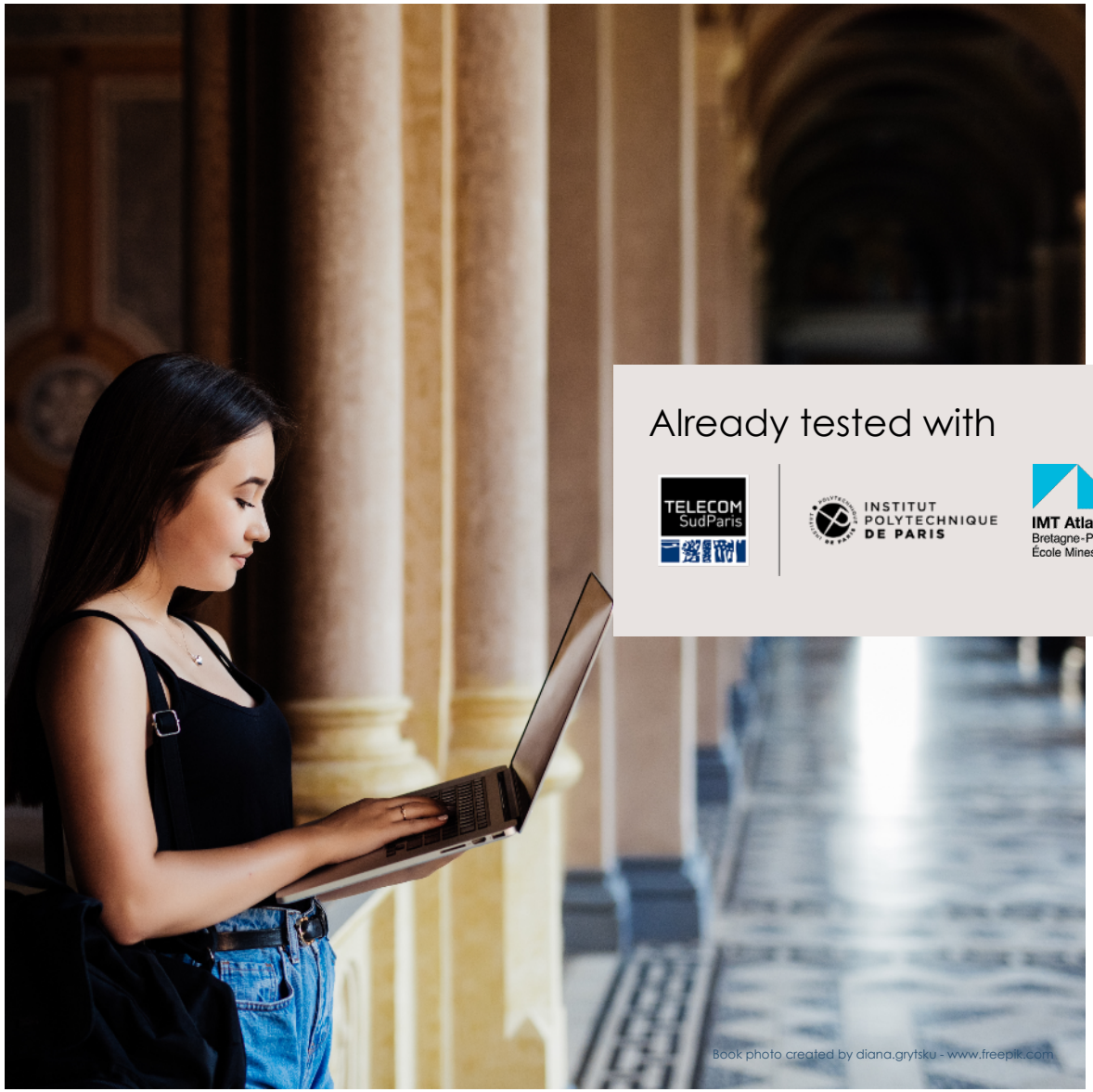
IoTRoam

A Federated IoT roaming infrastructure using LoRaWAN

USE-CASE eduroam

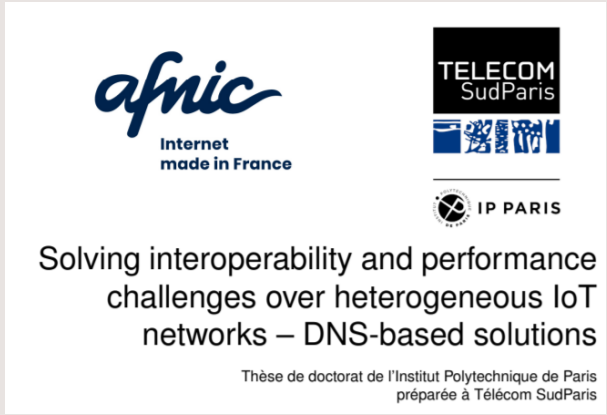
+10 IoTRoam supporters





PhD Thesis

- Improving system scalability
- Header compression mgt
- Device Transmission suppression
- Improving devices mobility
- Roaming
- DNS Prefetching scenarios



afnic

Collaborative research projects

Collaborative projects in a row

DONE

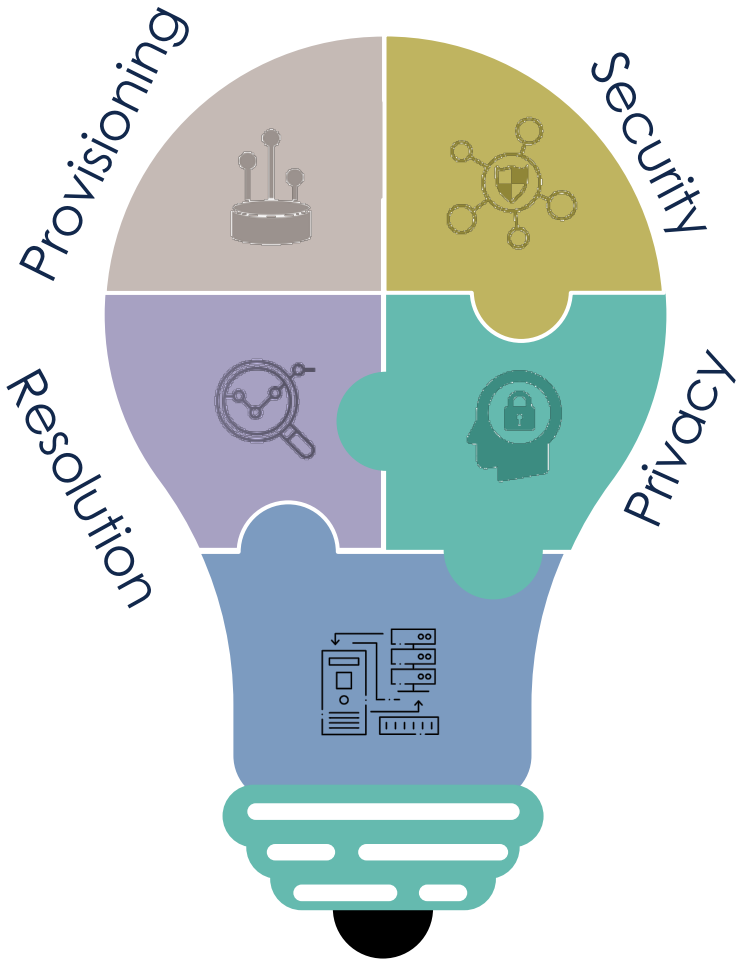
WINGS

Widening interoperability for networking Global supply Chains

Done

LoRa Alliance®

DNS Service



ONGOING

DINS*

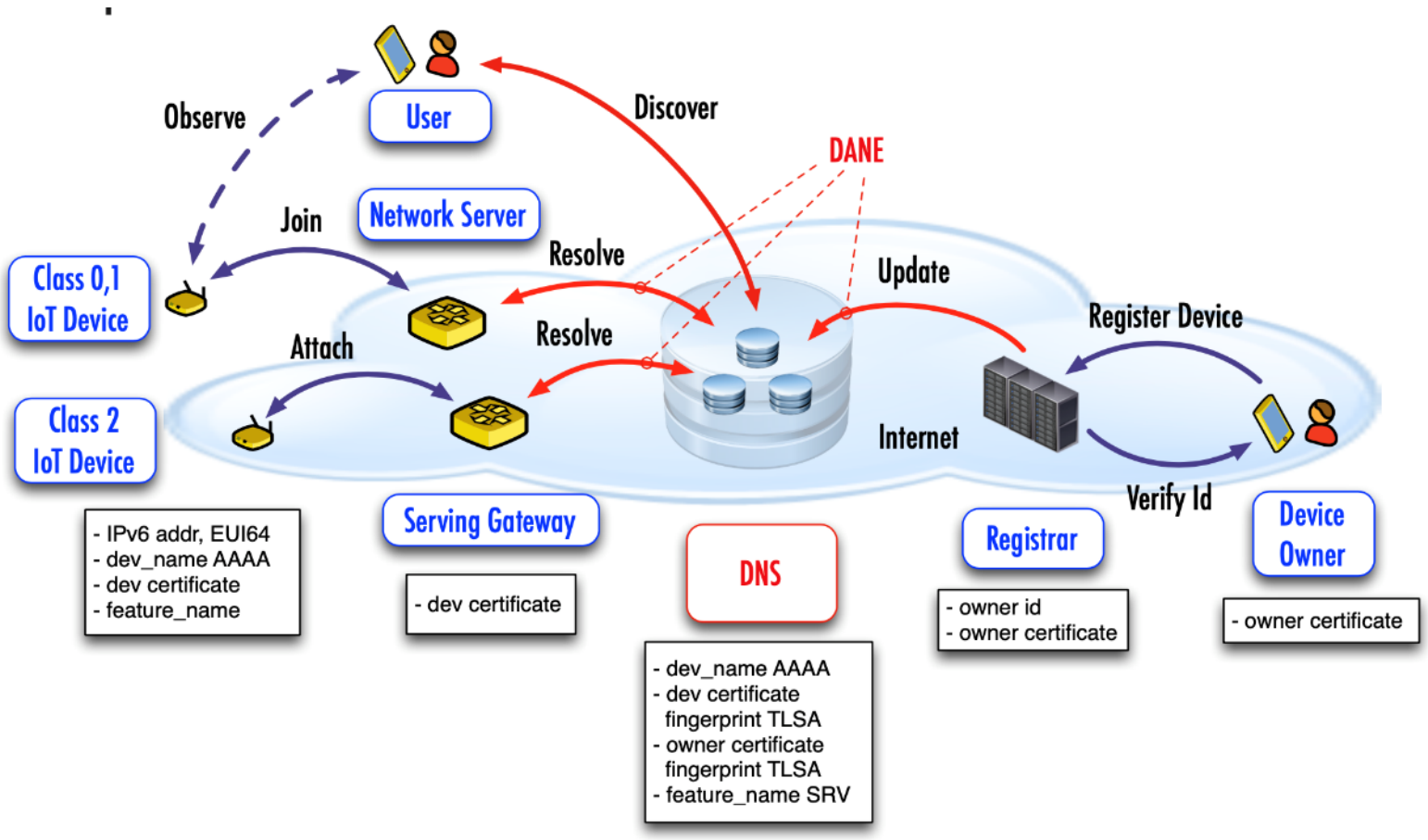
DNS Naming and Services for Secure Seamless IoT

ONGOING

PIVOT*

Privacy-Integrated design and Validation in the constrained IoT

DiNS Project



PIVOT – French German collaboration

- Privacy by design – Object Security

- Multi-stakeholder name management that preserves privacy requirements and generates, allocates, and resolves IoT names globally—regardless of the IoT applications or networks.

- Privacy friendly crypto library framework for ultra constrained IoT devices integrated to RIOT OS

https://pivot-project.info/about



Other contributions

IoT and Digital Sovereignty report

Overview on technologies and evolutions on connected objects

Industrial and regulatory challenges

Conclusion



People vector created by pch.vector - www.freepik.com

The DNS

WHY THE DNS IS STILL A PROTOCOL / SERVICE TO CONSIDER

- Known protocol for the Internet community
- Various open-source implementations for clients, servers or within frameworks
- Fairly open and up-to-date community
- New use-cases and improvements that keep the DNS up-to-date based on network paradigms developed by the industrial world or the research community.

The DNS in the IoT context

CISCO, INTERNET OF EVERYTHING : 99,4% OF THE PHYSICAL OBJECTS ARE STILL NOT YET CONNECTED

- **IoT**
- applications encounter the same issues as the Internet
- technologies are riddled with scalability, interoperability, mobility and roaming, transmission efficiency, availability, reliability and other security issues such as trust and privacy

- **DNS**
- contributes to solving many of these issues on the Internet
- is already a solution to some problems of interoperability and security of exchanges/ communication
- Federated model, “business compatible” service
- It’s widely distributed, it scales



Background vector created by rawpixel.com - www.freepik.com

QUIZZ :

Is the “Internet of everything” ready ?

Delete as appropriate ☹

Global
Interoperable
Open
Free – no centralized control
End-to-end
User-centric
Robust and reliable
Secure

Acting at our level to break the silos and provide standardized interconnection procedures for interconnecting different IoT networks is a first step

« DNS is everything »*

Will the Internet of everything adopt DNS ?

* Geoff Huston - APNIC - DNS evolution https://www.youtube.com/watch?v=Fy_c49yXcb0

Merci !

benoit.ampeau@afnic.fr

Director of Partnerships & Innovation

Internet made in France

Association Française pour le Nommage Internet en Coopération

Immeuble Stephenson, 1 rue Stephenson, 78180 Montigny-le-Bretonneux, France
Tel. +33 (0)1 39 30 83 00

www.afnic.fr | contact@afnic.fr | Twitter : @AFNIC | Facebook : facebook.com/afnic.fr