Extending DNS and its ecosystem for IoT

Sandoche BALAKRICHENAN

Oct. 8th 2021

afnic
Internet made in France

Afnic in brief

- French Network Information Center (NIC)
-
- Non-profit organization established in 1977

- Internet registry for .fr and French overseas territories (.*gf, .bl, .gp, .mf, .mq, .pm, .re, tf, .wf, .yt*)

- Technical Backend operator (.*paris*, *.bzh*, *.alsace*,*.corsica*, *.sncf*, *.mma*, *.ovh*, *.leclerc*, *bostik*, *.total*, *.aquarelle*, *.lancaster* & *.museum)*

- On a daily basis, we strive to contribute to:
  - Secure & Stable Internet
  - Innovation
  - French Internet playing a leading role

afnic | Labs

R&D Team

Doctors
Engineers
PhD Students

R&D collaborative projects

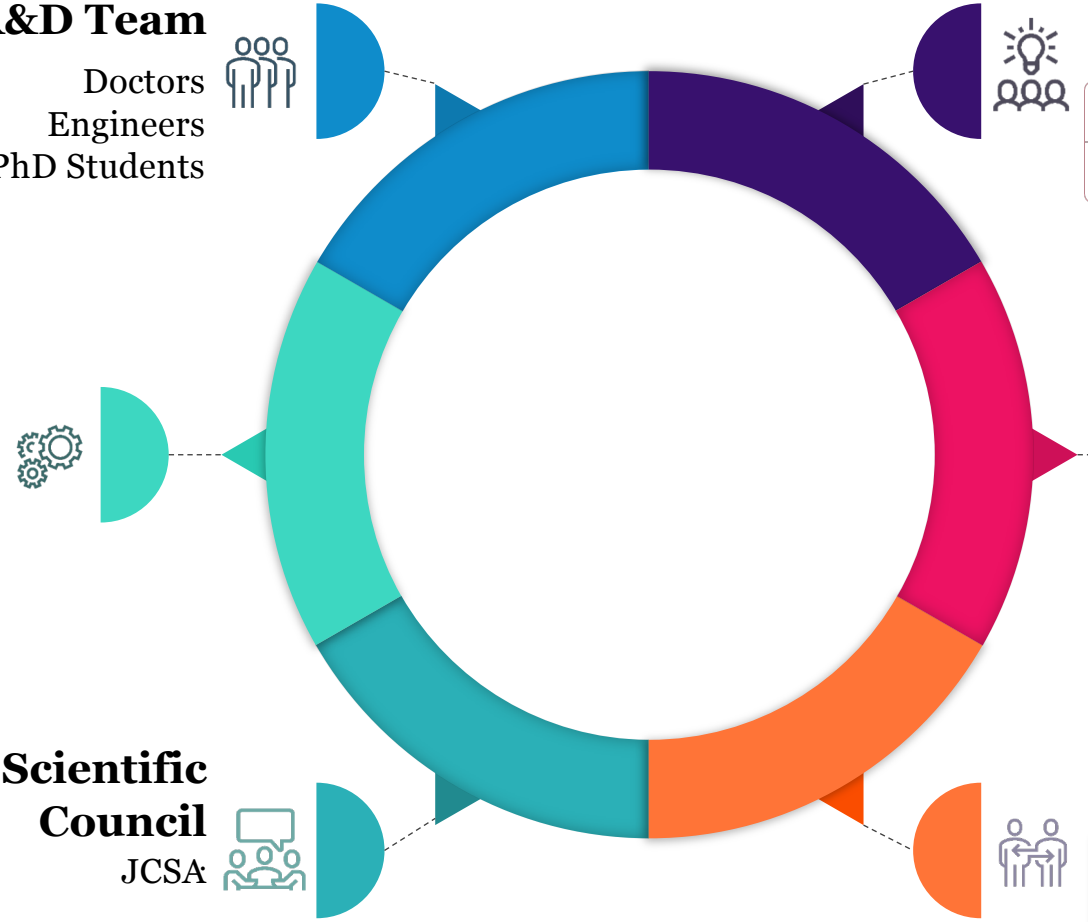
DINS*
DNS Naming and Services for Secure Seamless IoT

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, IGF, LoRa Alliance



Internal projects

DNS Protocol
Data analysis
Registry services innovation

Scientific Council

JCSA

Publications




INTRODUCTION
A

afnic | Labs Terminologies

- Identity – definable and recognizable
  - ”Sandoche-Macbook” is my Computer’s identity
  - No unicity requirement
- Identifier – Need not be recognizable
  - IPv4, IPv6, MAC
  - Social Security number, Passport Number
  - Required to identify in a group. Unicity requirement in the group
- Address – Defines access Points and need not be recognizable
  - Phone number, IP addresses (Addresses and Identifiers could be the same)
  - Required to access the identity in a group
  - Unicity requirement in the group scope

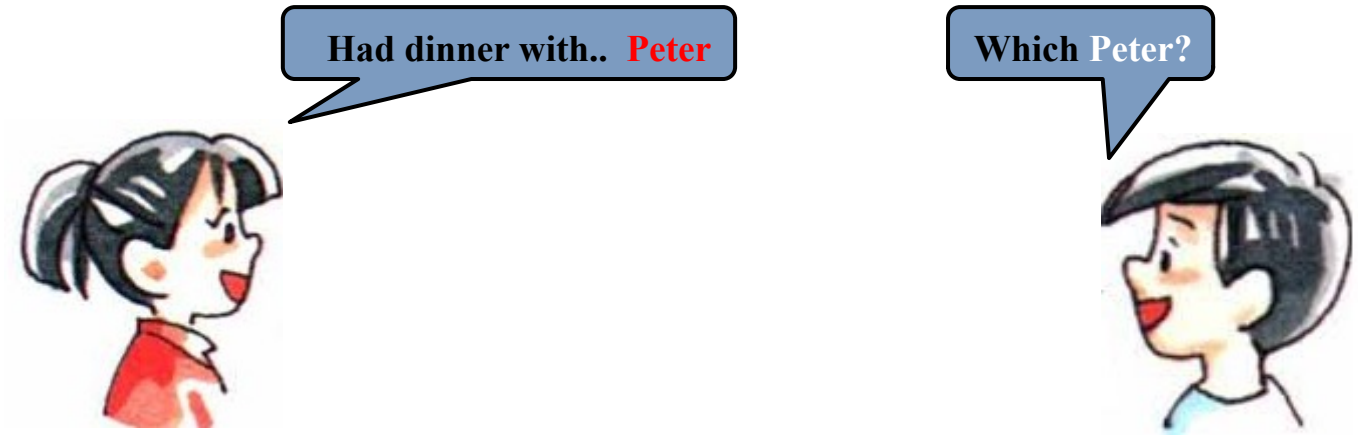
afnic | Labs

Human's can infer Identity based on Context



afnic | Labs

Ask Questions if it is not possible to infer the context



afnic | Labs

Issue with Computing Systems



Conventions for Identifiers & Addresses

- Domain name
  - balakrichenan.fr, .இந்தியா

- IP Address
  - 192.134.4.84, 2001:db8:85a3:8d3:1319:8a2e:370:7348

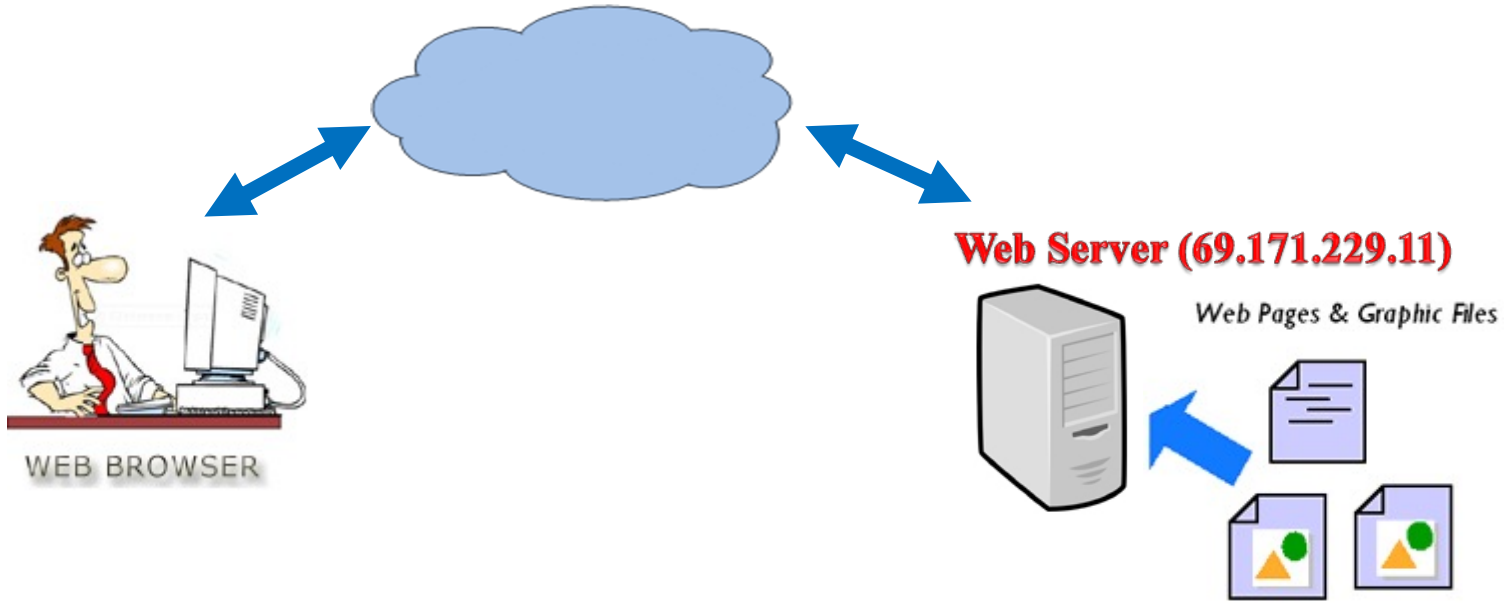
> **"A name indicates what we seek. An address indicates where it is. A route indicates how we get there."**
>
> —Jon Postel, RFC 791

afnic | Labs

Humans are bad in remembering numbers and good in remembering names



DNS is needed to link both domain names & IP address



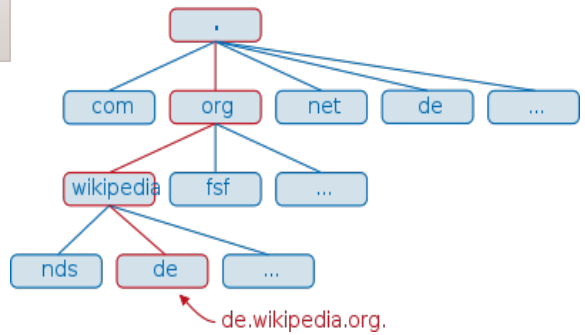
Three steps to resolve an Identifier in the Internet

1. Naming Conventions

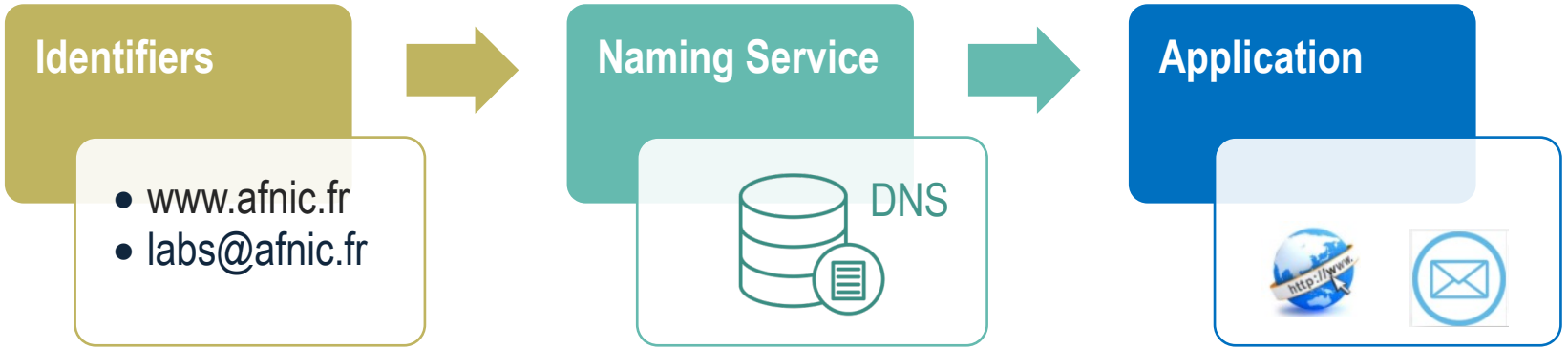
IETF is the SDO

- **Domain names, URI**
- **IP Addresses (IPv4/IPv6)**

2. Provisioning



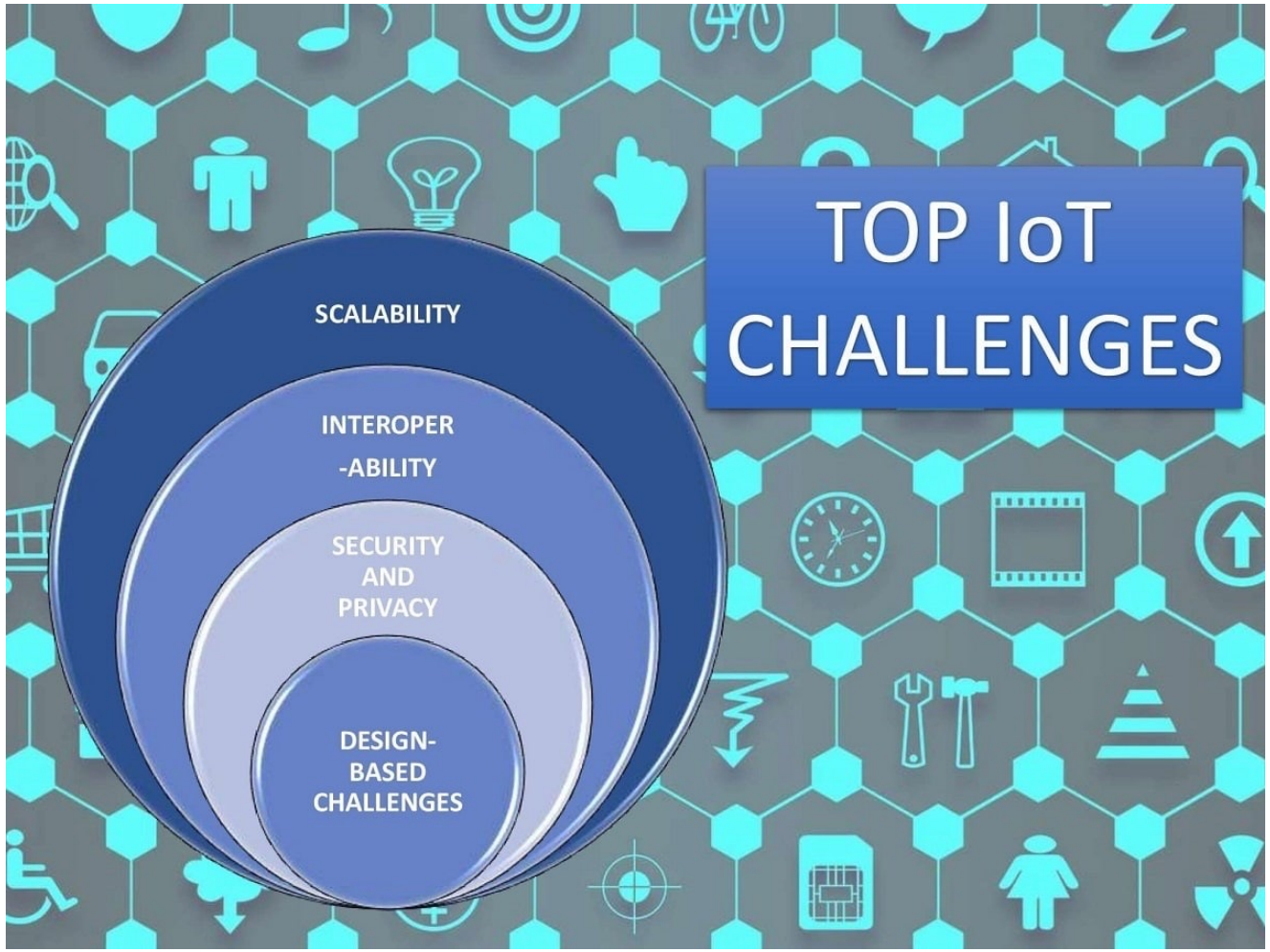
3. Resolution




Don't forget to buy milk!

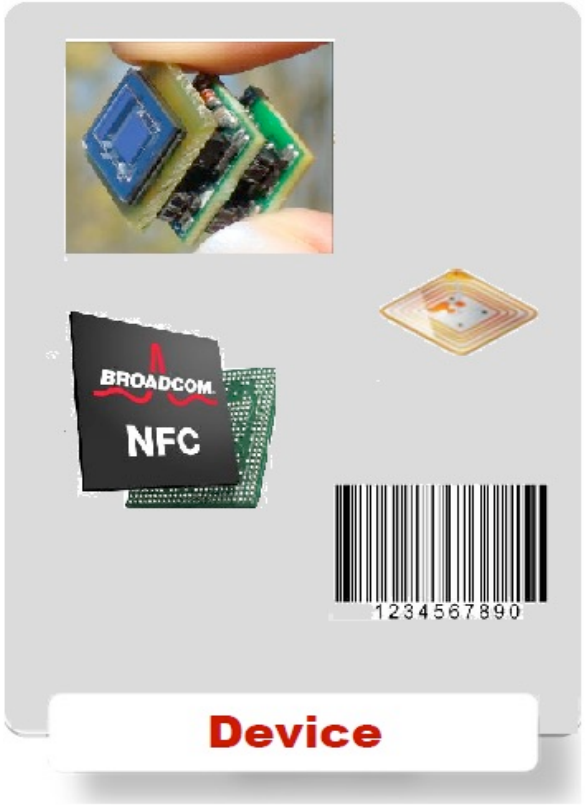
afnic | Labs

Top Challenges in IoT



Making the ‘T’ Identifiable in IoT





Naming Conventions in IoT

RFC 2396
URI

ISO/IEC 15459
Products & Packages

ISO/IEC 29161
IoT Identification

ISO 14223
RFID for Animals

IEEE 1451
Smart Transducers

ISO 2108
Books

BS 7666
UK Property Reference Number

GS1 GTIN
Trade Items

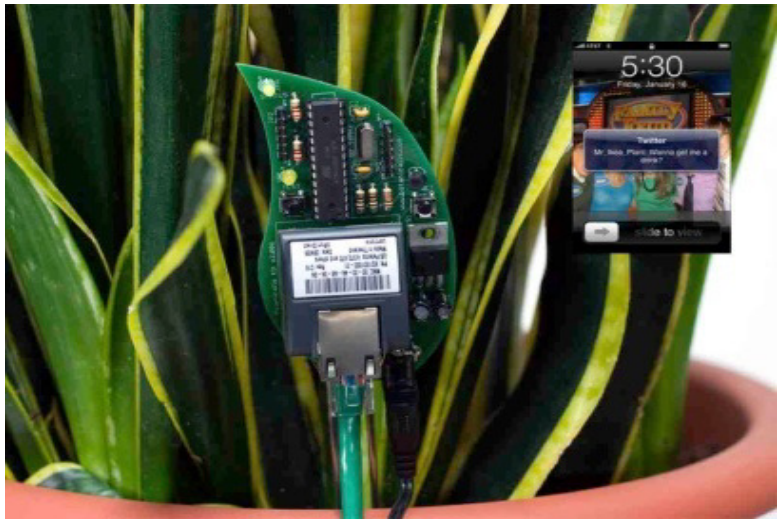
ISO 16739
Construction & Facility Management

afnic | Labs

Currently IoT => I(ntranet)oT

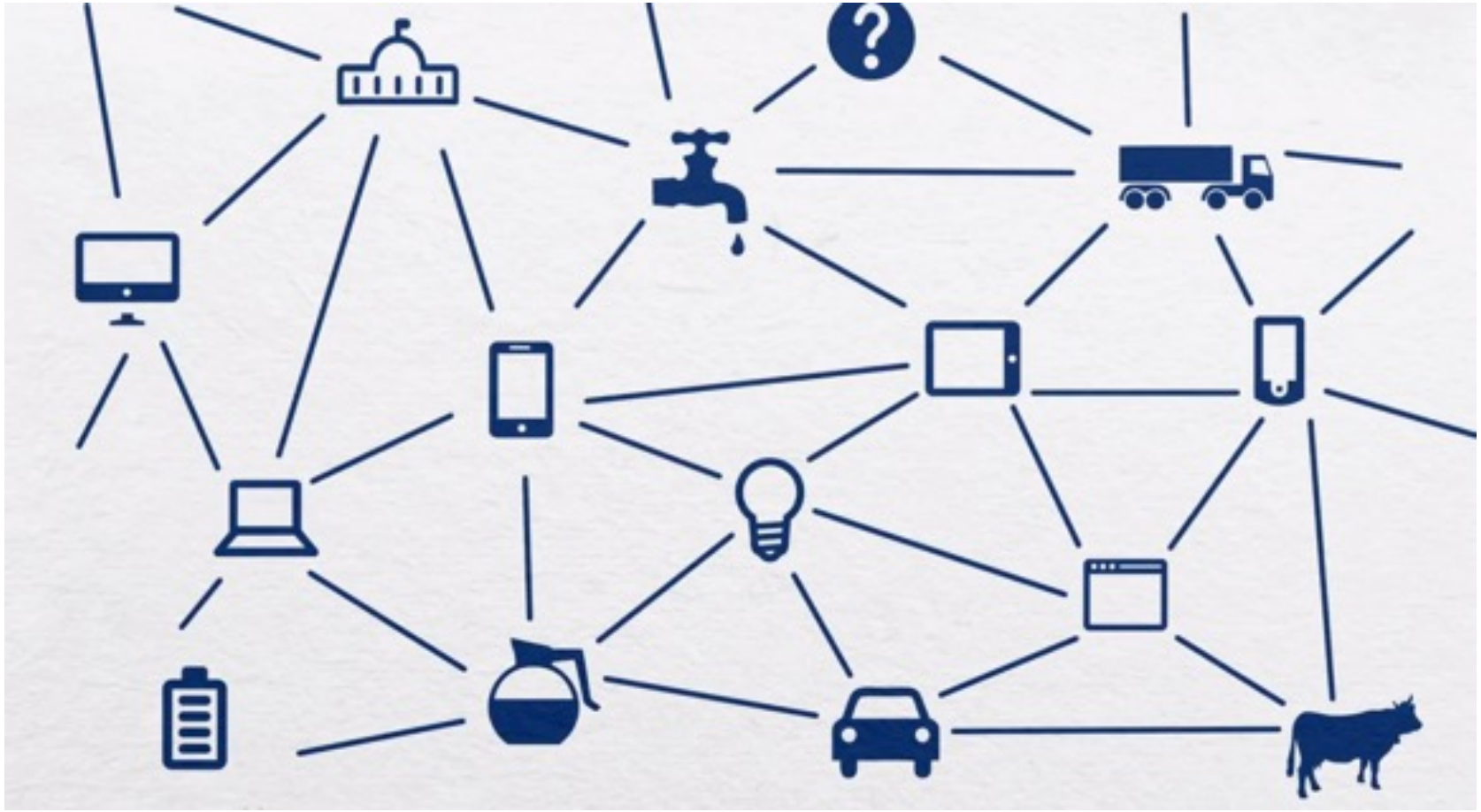


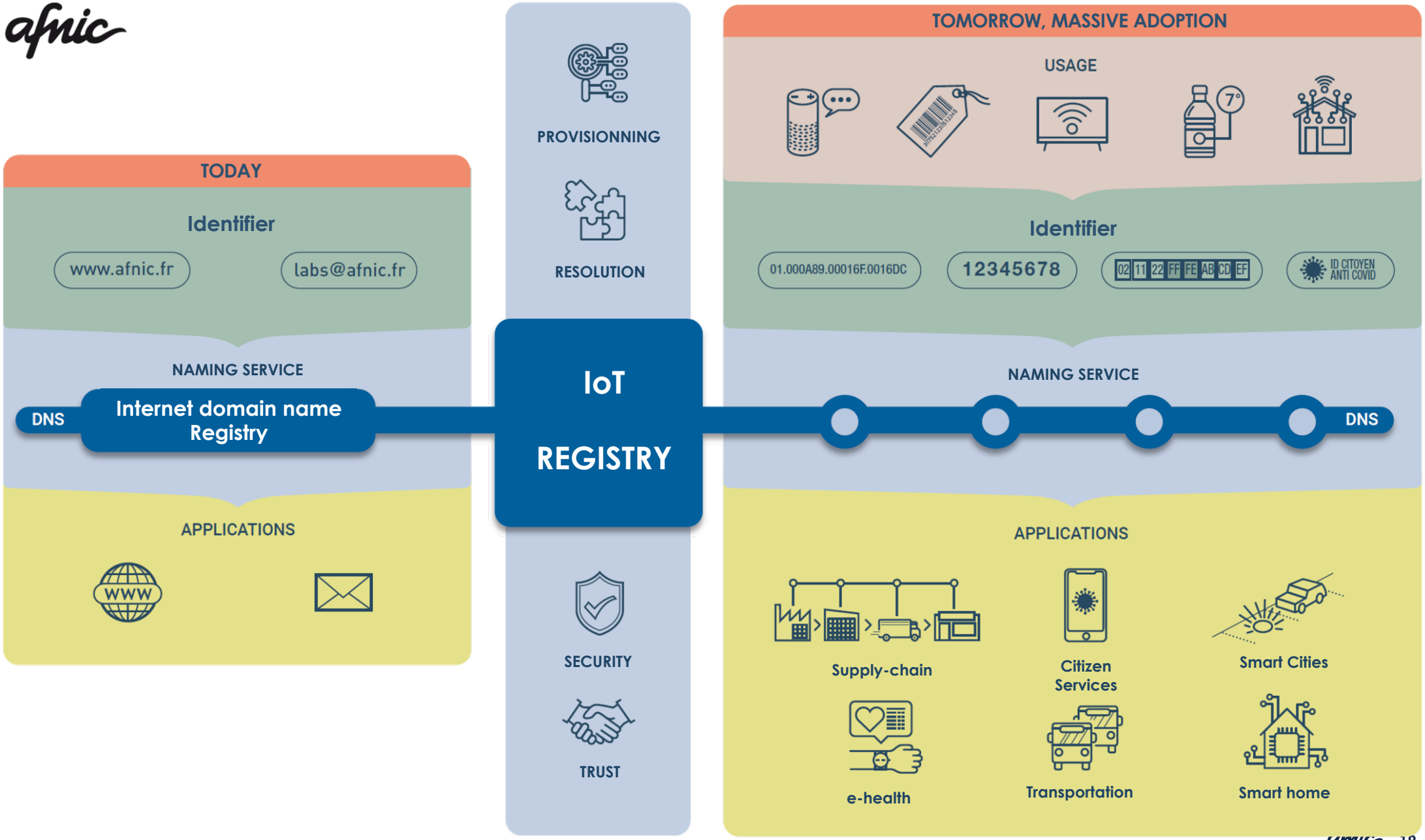




afnic | Labs

Need = I(nternet)oT




TODAY
Identifier
www.afnic.fr
labs@afnic.fr
NAMING SERVICE
DNS
Internet domain name Registry
APPLICATIONS
WWW
PROVISIONNING
RESOLUTION
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

afnic | Labs

Naming Conventions, SDOs and Naming Services in IoT

Naming Conventions	SDO	Naming Service
URI (e.g. Domain names)	IETF	DNS
EPC	GS1	ONS
OID	ITU and ISO/IEC	ORS
DOI	ISO	Handle

Objective: IoT Registry (More than 10 years of R&D)

DONE

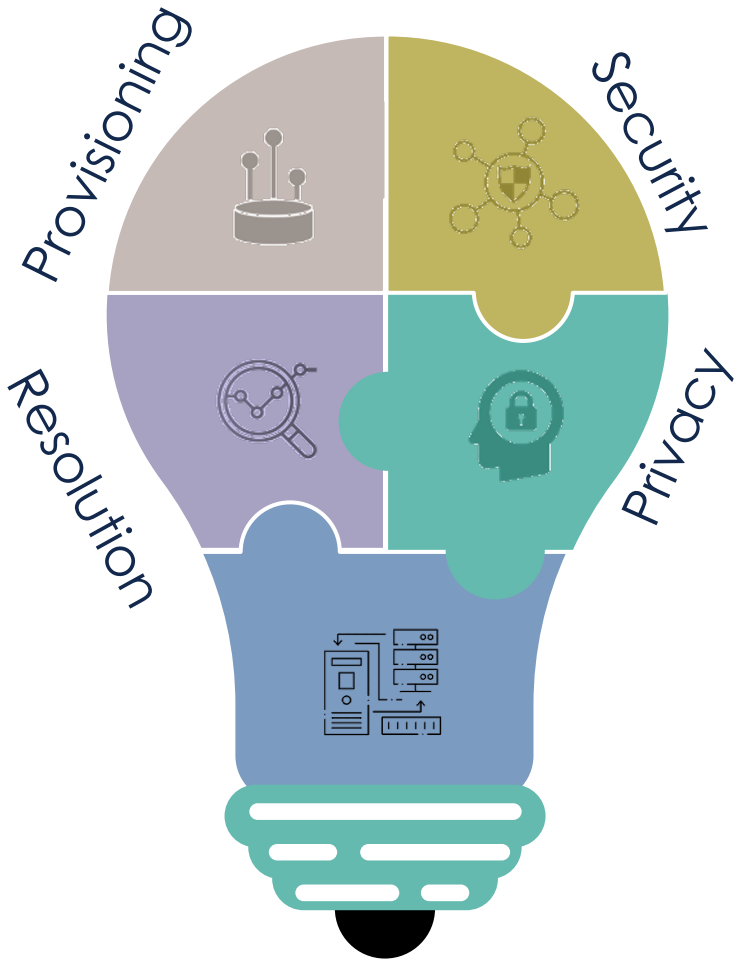
WINGS

Widening interoperability for networking Global supply Chains

PoC

LoRa Alliance®

DNS Service



ONGOING

DINS*

DNS Naming and Services for Secure Seamless IoT

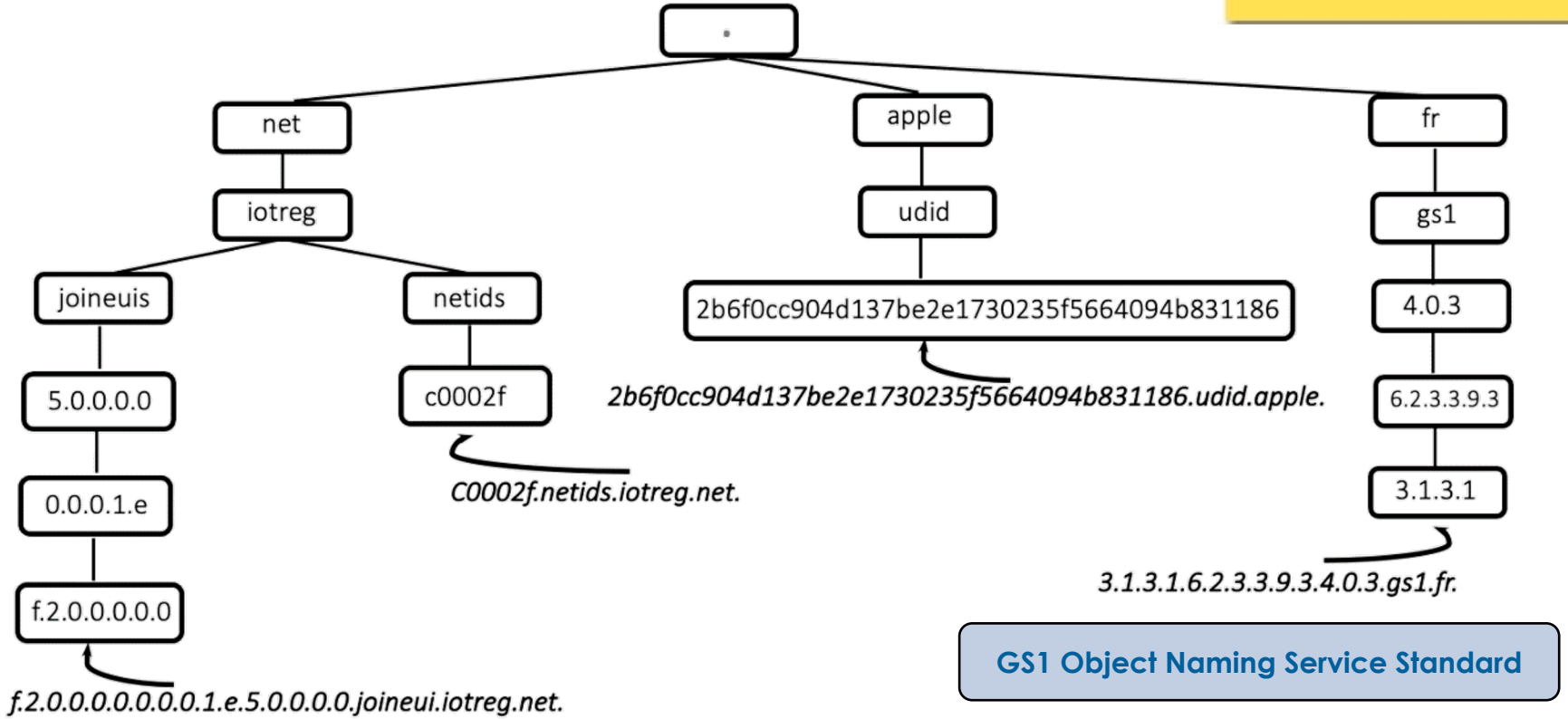
ONGOING

PIVOT*

Privacy-Integrated design and Validation in the constrained IoT

Provisioning = Establishing the route

> "A name indicates what we seek. An address indicates where it is. A route indicates how we get there."
>
> —Jon Postel, RFC 791



LoRaWAN Backend Interfaces specification

GS1 Object Naming Service Standard

afnic | Labs Contributions in Provisioning & Resolution

DNS for leveraging IoT protocols and infrastructures

- ONS : Standard

- LoRaWAN : Backend Specifications

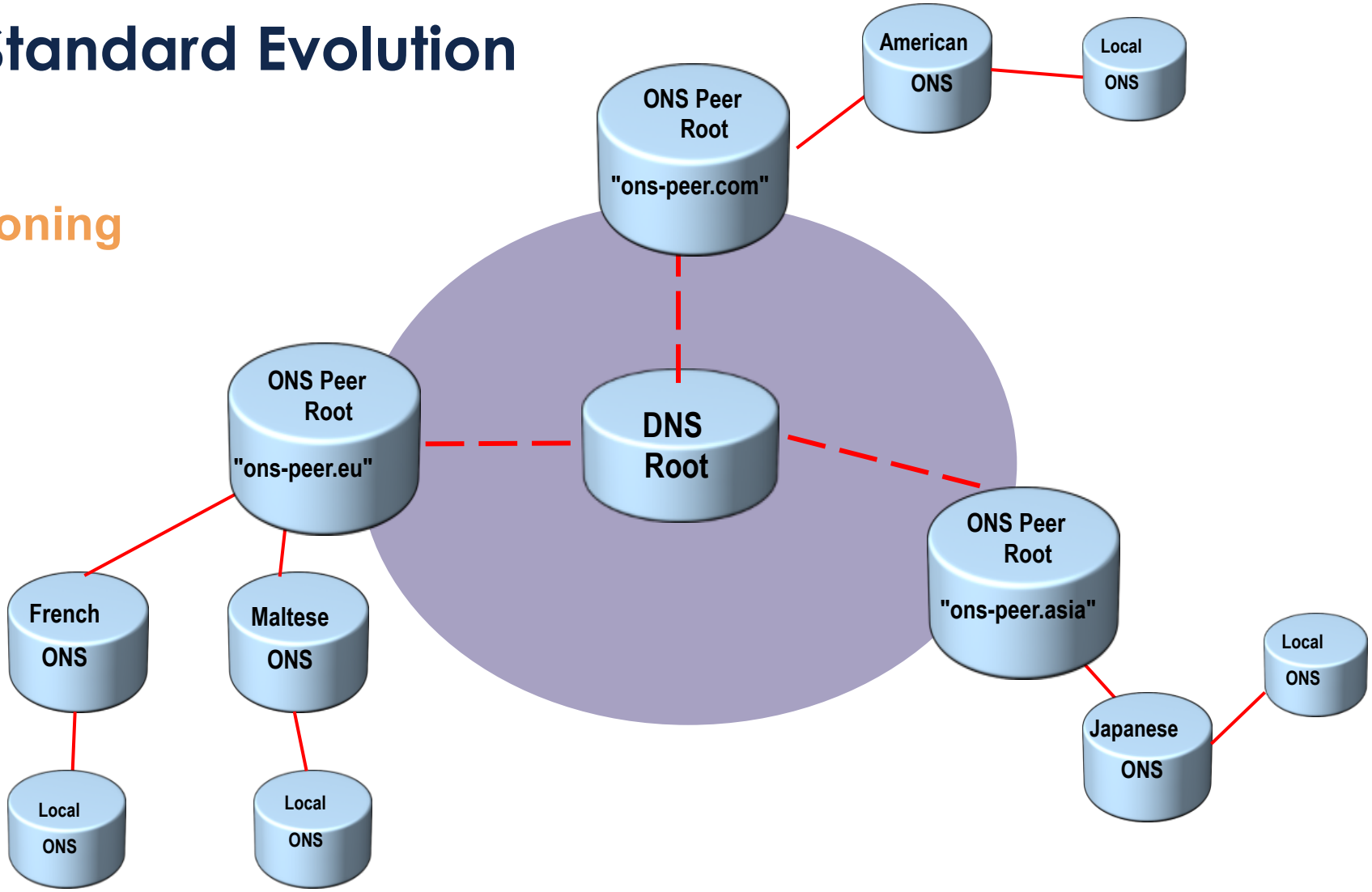
ONS

Contribution



ONS Standard Evolution

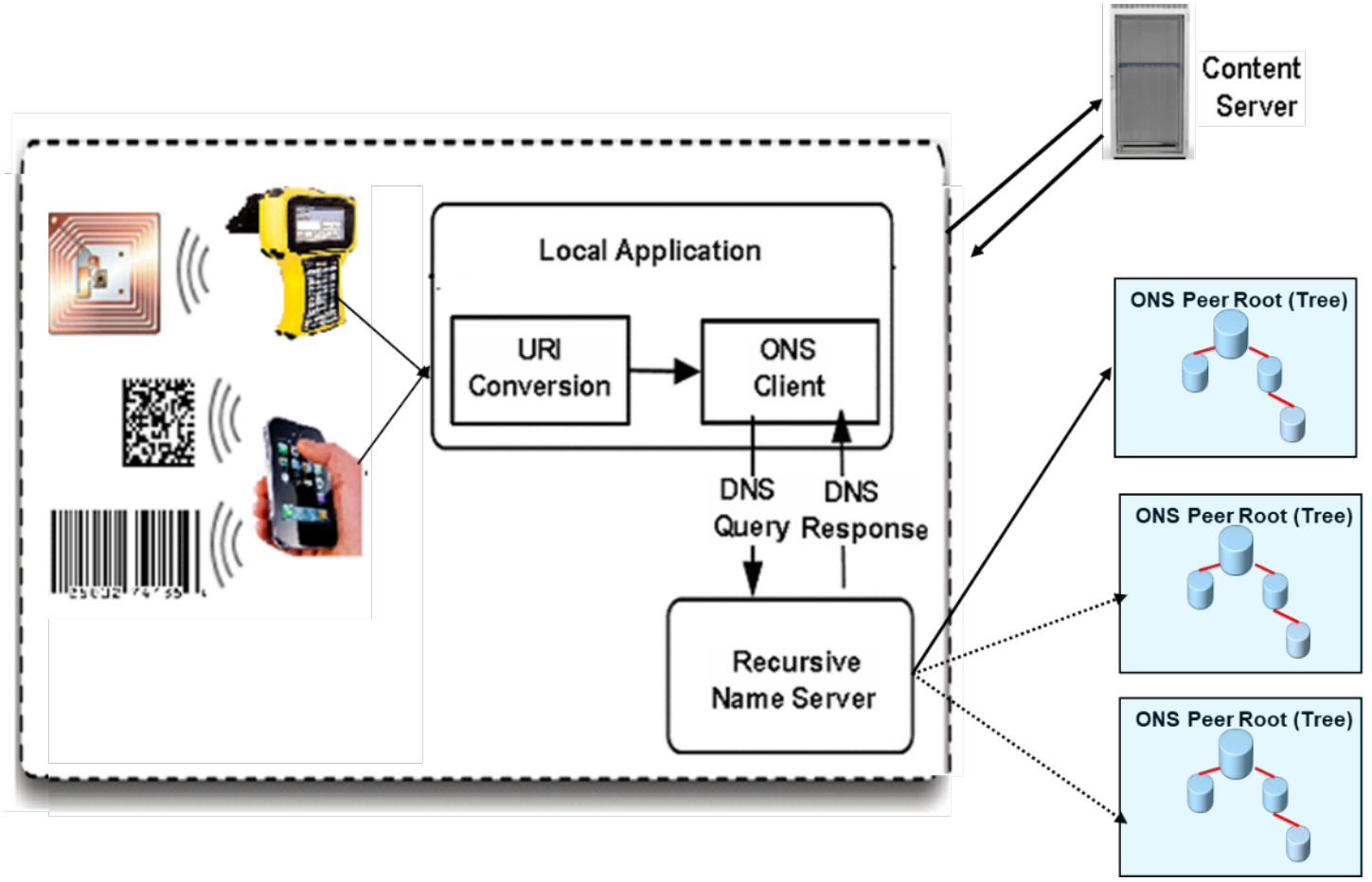
Provisioning



ONS Standard Evolution

Resolution

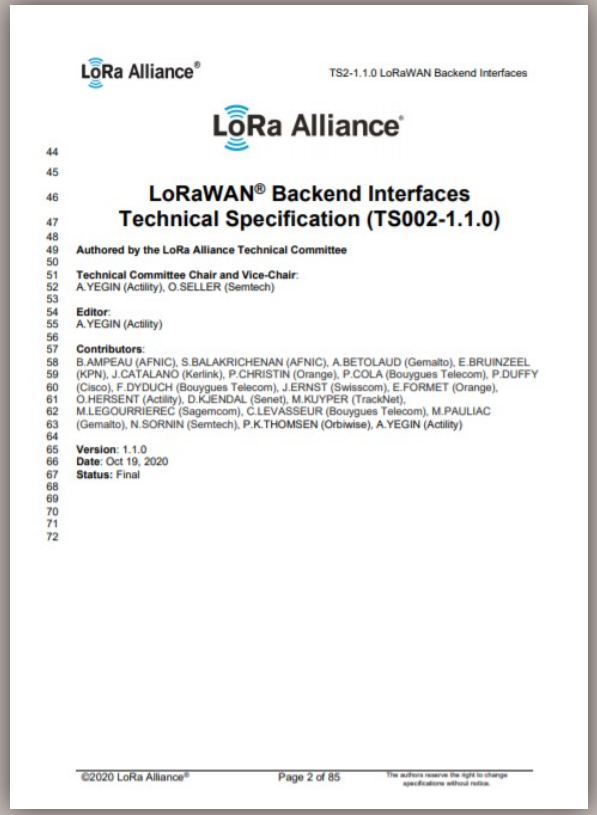




LoRaWAN

Low Power, Wide Area (LPWA) networking protocol

Contribution



LoRa Alliance® TS2-1.1.0 LoRaWAN Backend Interfaces

LoRa Alliance

LoRaWAN® Backend Interfaces
Technical Specification (TS002-1.1.0)

Authored by the LoRa Alliance Technical Committee

Technical Committee Chair and Vice-Chair:
A.YEGIN (Actility), O.SELLER (Semtech)

Editor:
A.YEGIN (Actility)

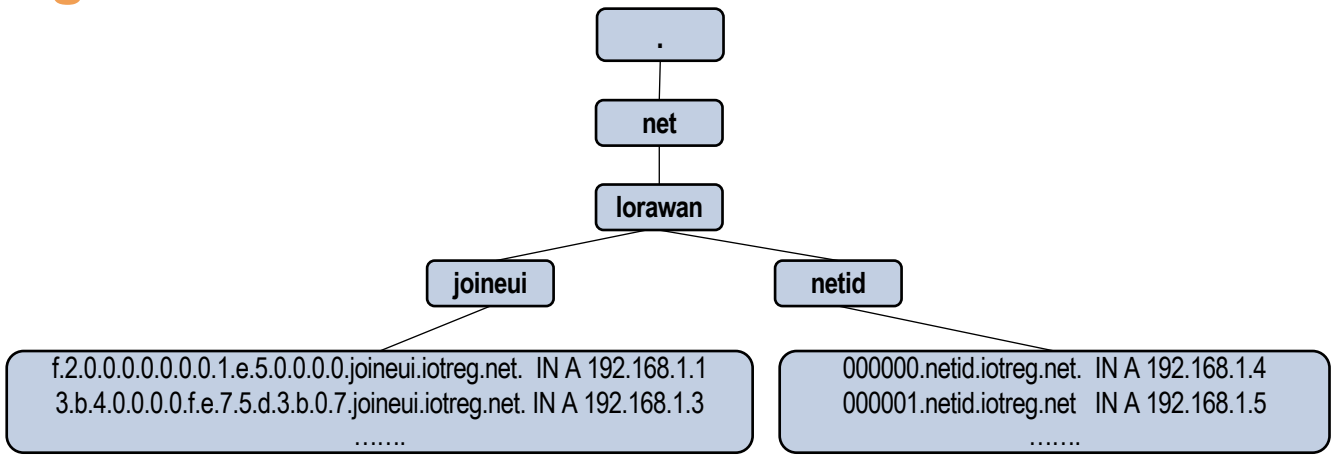
Contributors:
B.AMPEAU (AFNIC), S.BALAKRICHENAN (AFNIC), A.BETOLAUD (Gemalto), E.BRUINZEEL (KPN), J.CATALANO (Kerlink), P.CHRISTIN (Orange), P.COLA (Bouygues Telecom), P.DUFFY (Cisco), F.DYDUCH (Bouygues Telecom), J.ERNST (Swisscom), E.FORMET (Orange), O.HERSENT (Actility), D.KJENDAL (Senet), M.KUYPER (TrackNet), M.LEGOURRIEREC (Sagemcom), C.LEVASSEUR (Bouygues Telecom), M.PAULIAC (Gemalto), N.SORNIN (Semtech), P.K.THOMSEN (Orbiwise), A.YEGIN (Actility)

Version: 1.1.0
Date: Oct 19, 2020
Status: Final

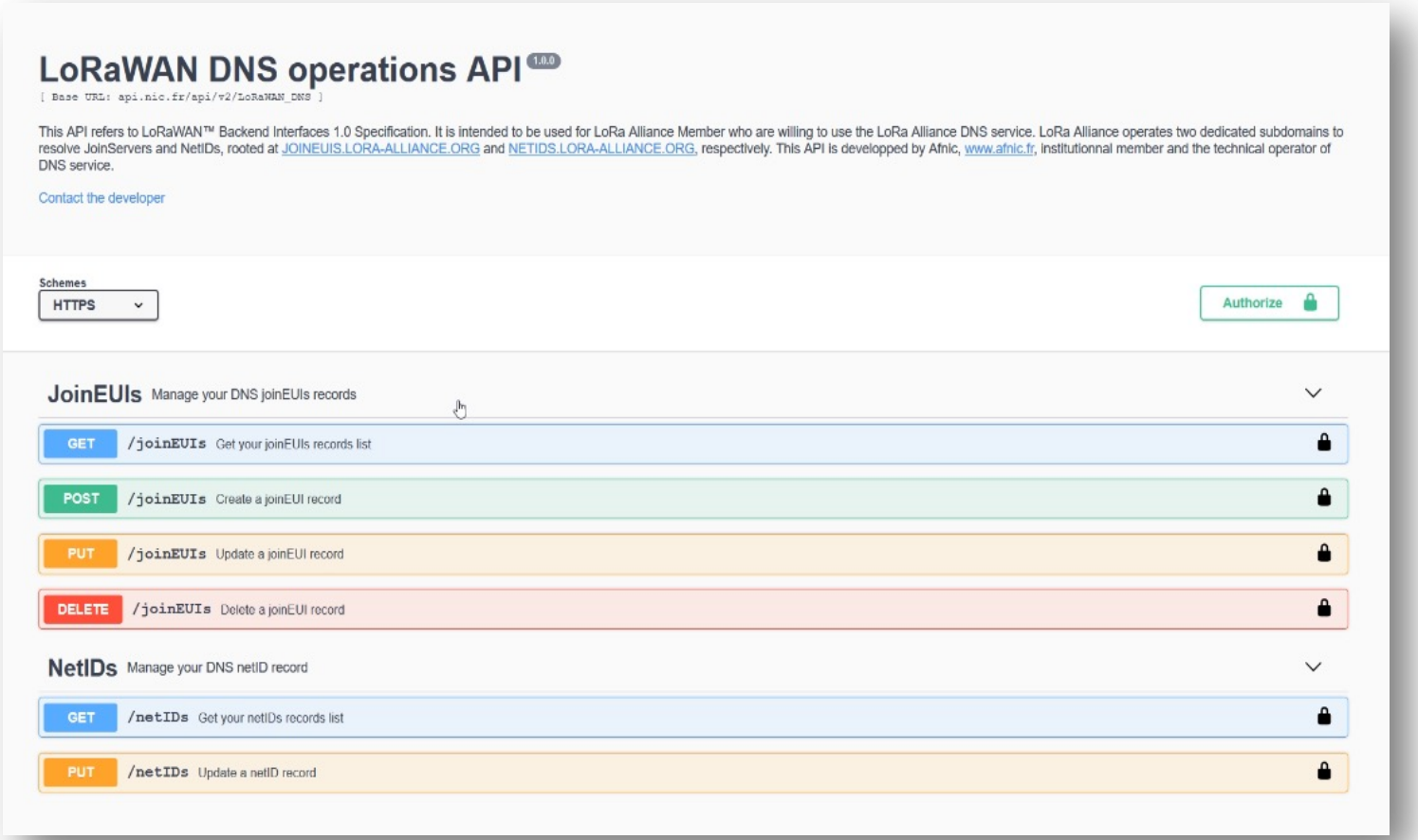
©2020 LoRa Alliance® Page 2 of 85 The authors reserve the right to change specifications without notice.

LoRaWAN Backend Specifications

Provisioning

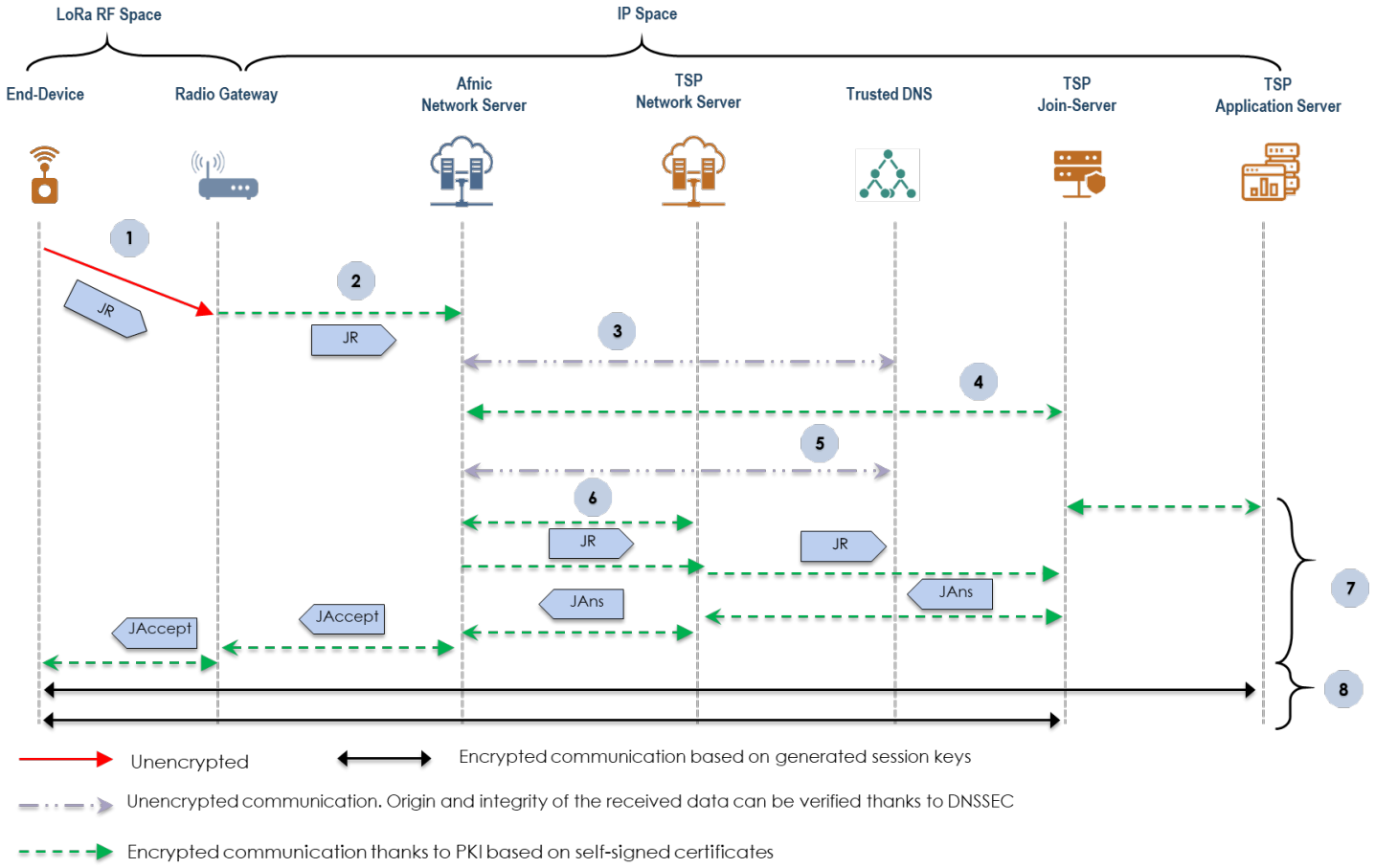


Dedicated LoRaWAN DNS Service



LoRaWAN Backend Specifications

Resolution



afnic | Labs Ongoing research in Security & Privacy

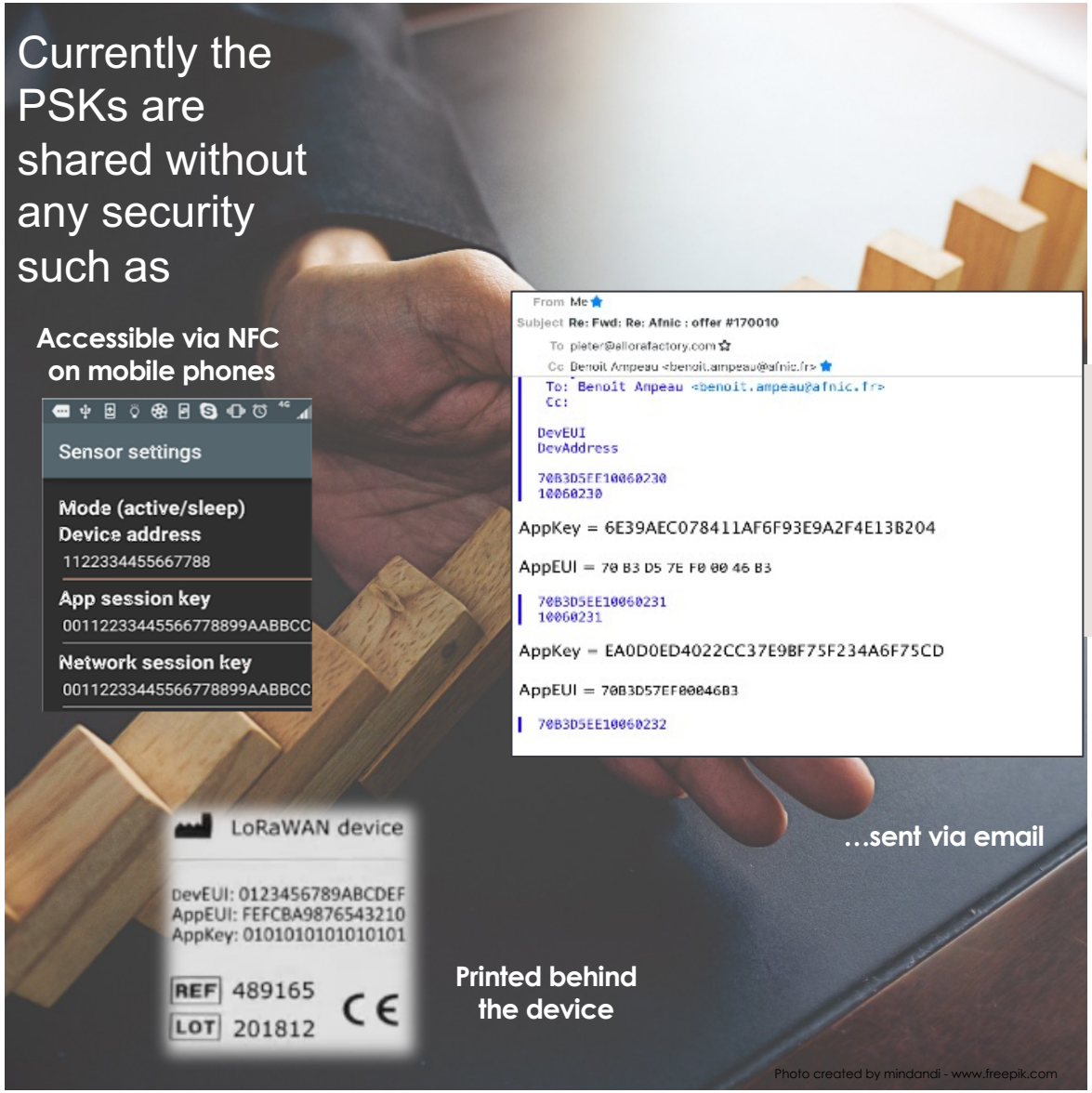
DNS for leveraging IoT protocols and infrastructures

- IoTRoam
- DINS
- PIVOT

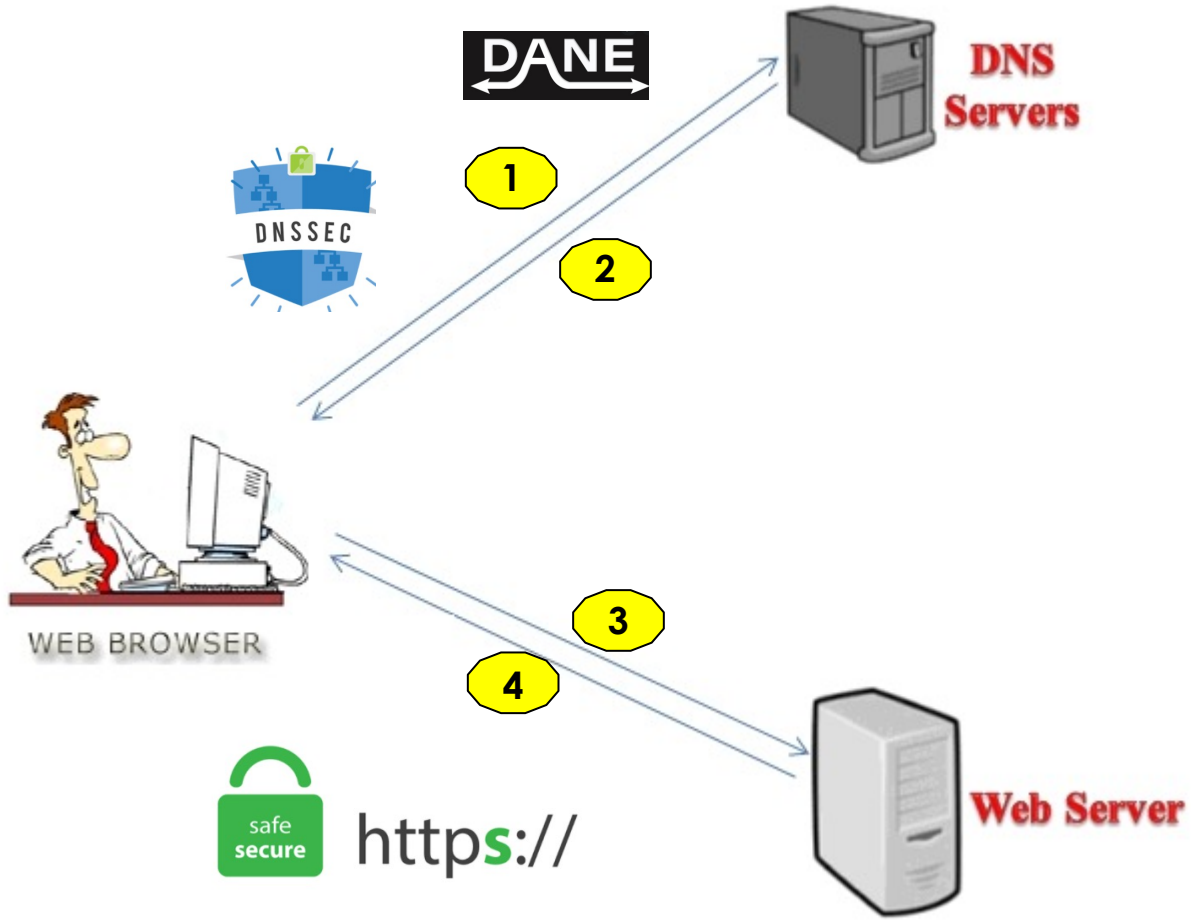
Problem statement

Currently Pre-shared Keys (PSKs) are used for securing IoT communication with the AAA server

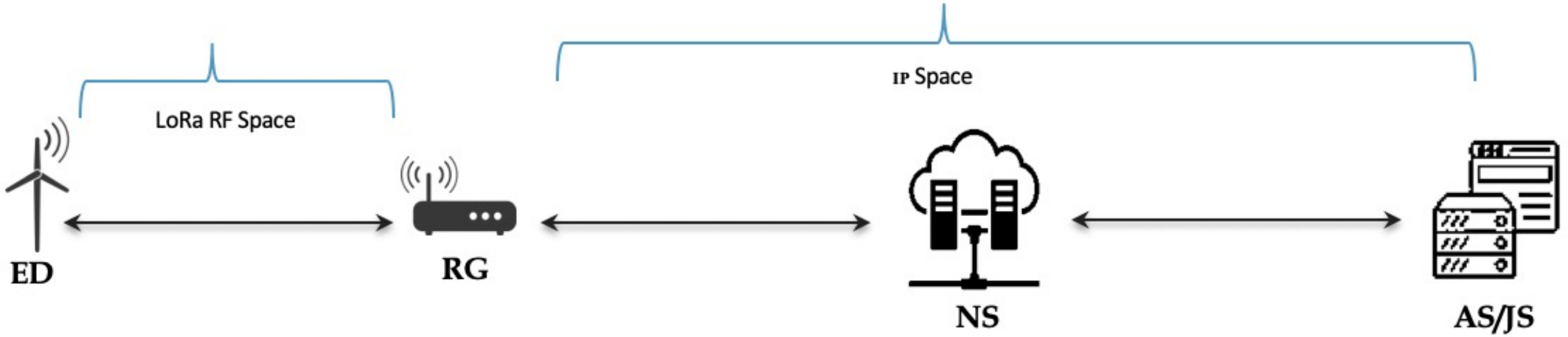
Sharing the PSKs is an operational nightmare

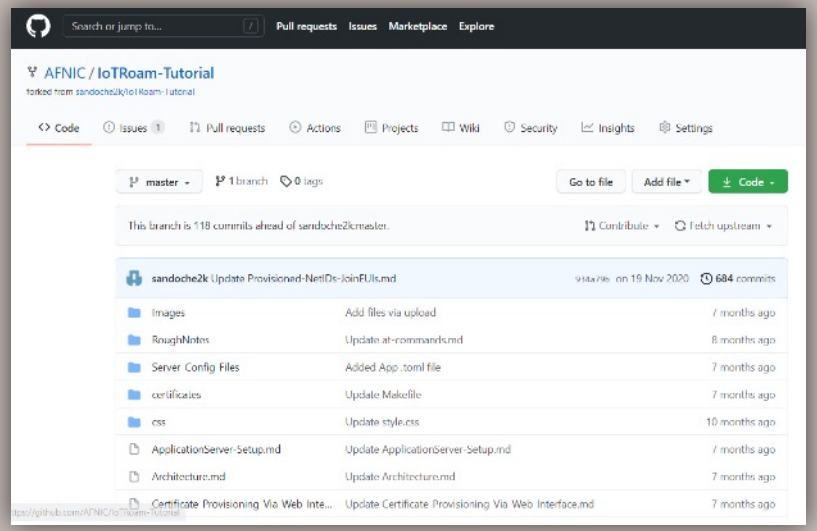


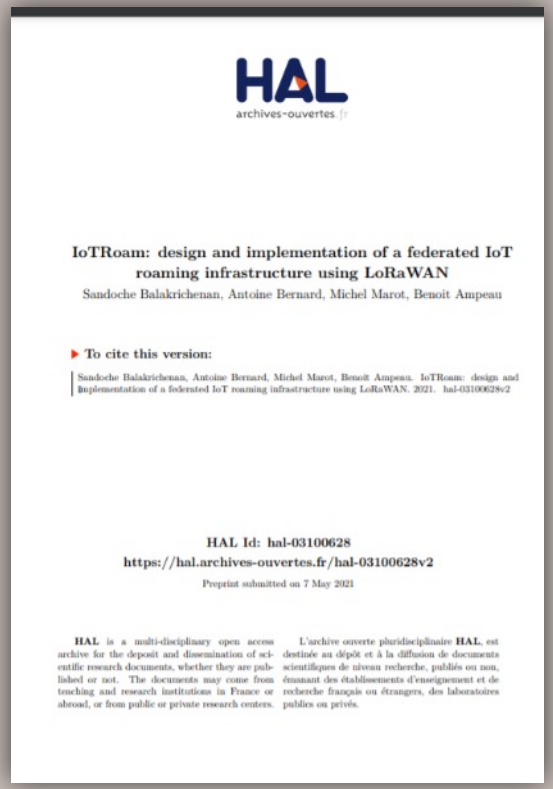
Asymmetric Keys as in the Internet



Objective DINS => End-to-End Security







IoTRoam

A Federated IoT roaming infrastructure using LoRaWAN

IoTRoam

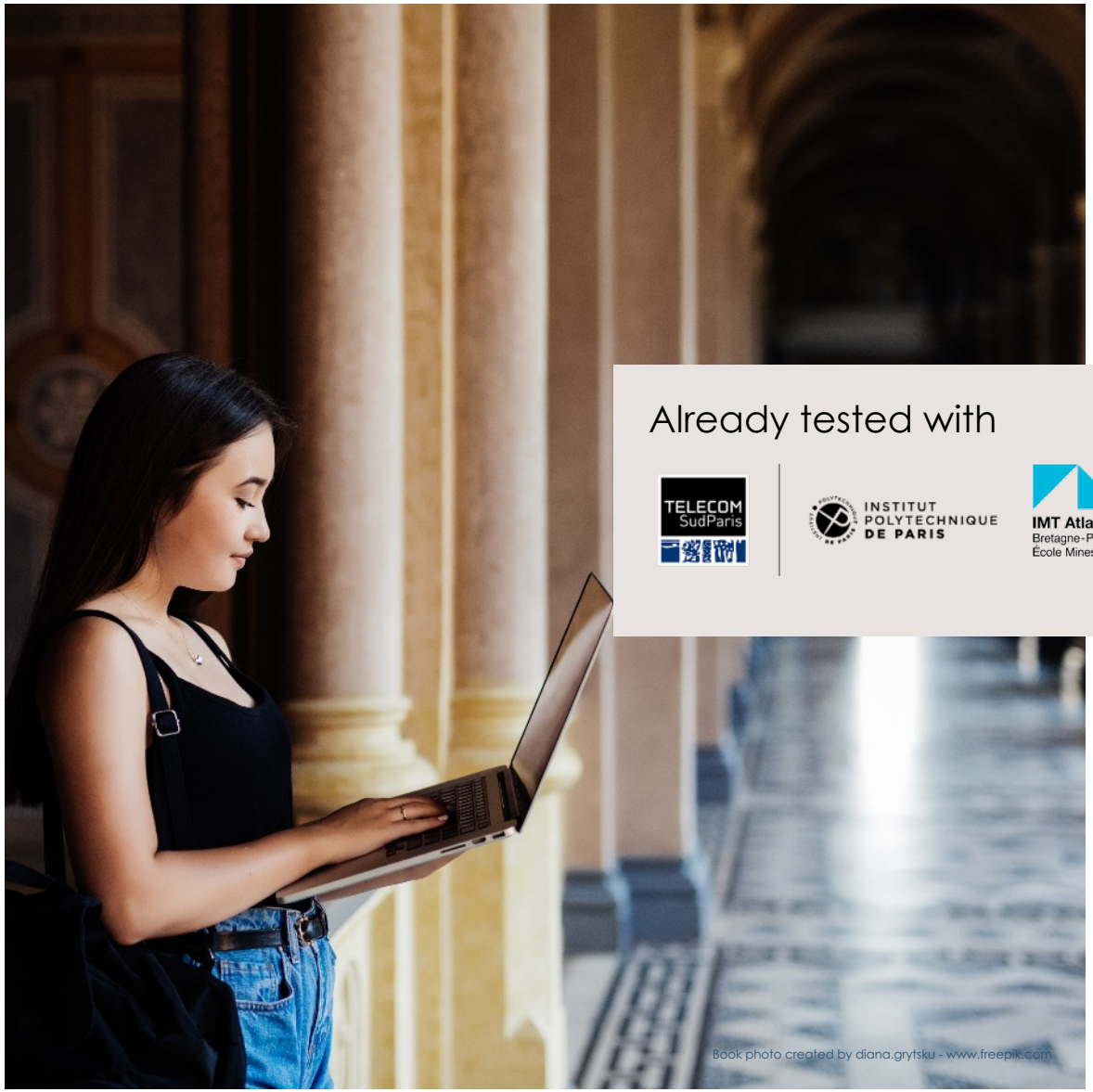
A Federated IoT roaming infrastructure using LoRaWAN

USE-CASE

eduroam

+10 IoTRoam supporters

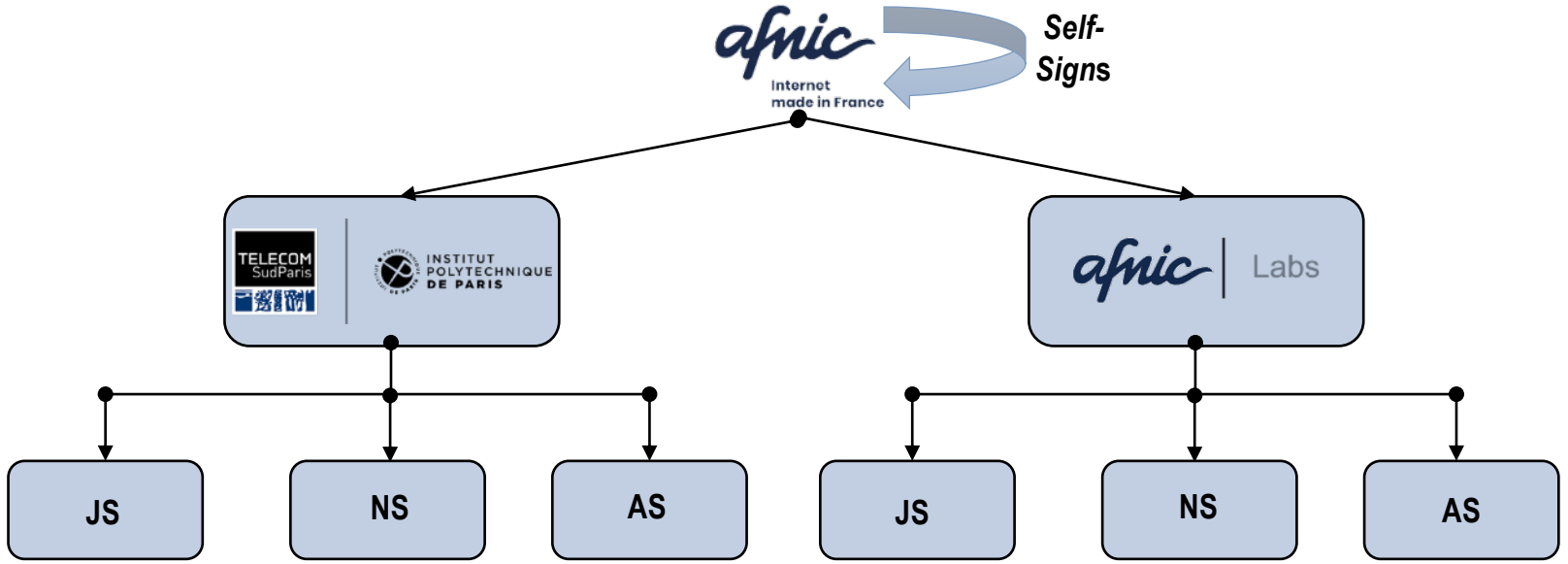


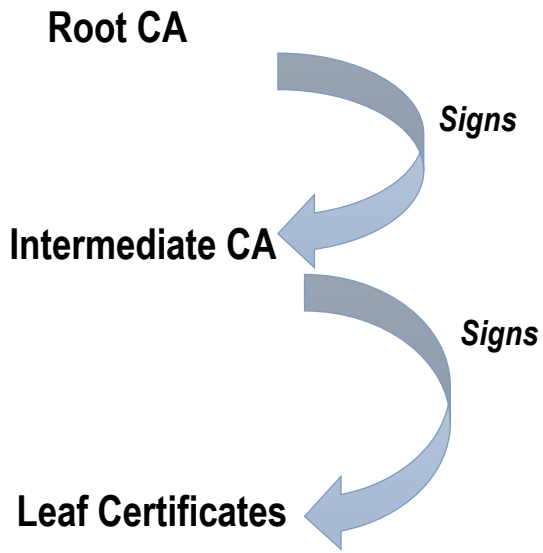


Already tested with

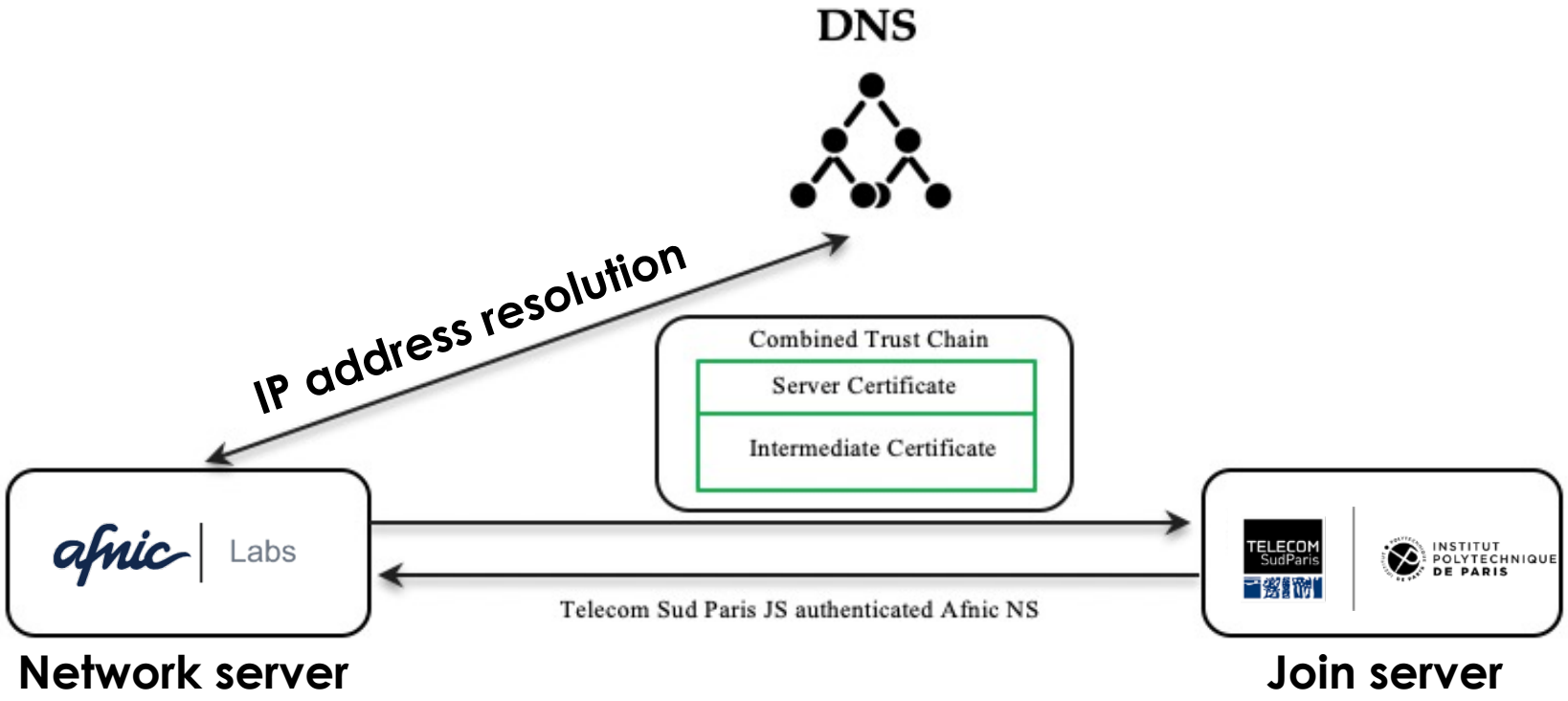
TELECOM SudParis | INSTITUT POLYTECHNIQUE DE PARIS | IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom

IoTRoam – Certificate Provisioning

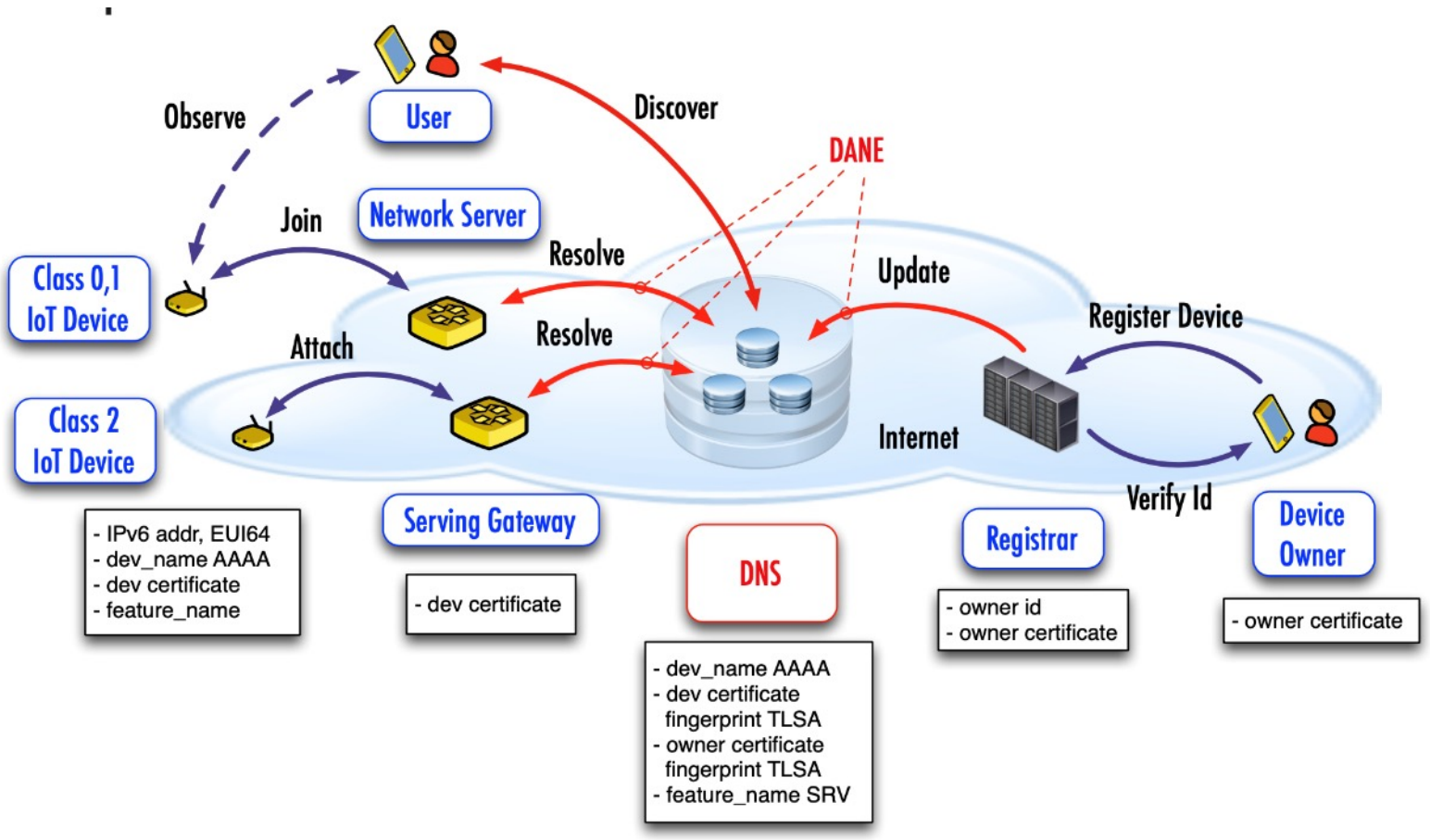




IoTRoam – Certificate Validation



DiNS Project



afnic | Labs

Is it possible to use Asymmetric Keys as in the Internet

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.

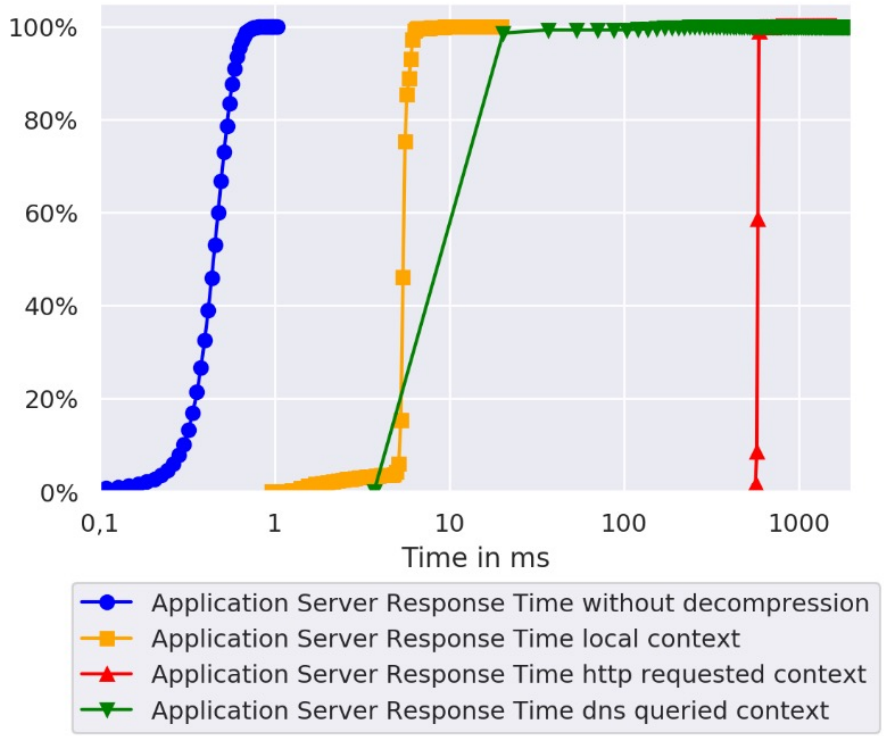
- Privacy friendly crypto library framework for ultra constrained IoT devices integrated to RIOT OS

Other Research work

Using DNS for Rule resolution – SCHC

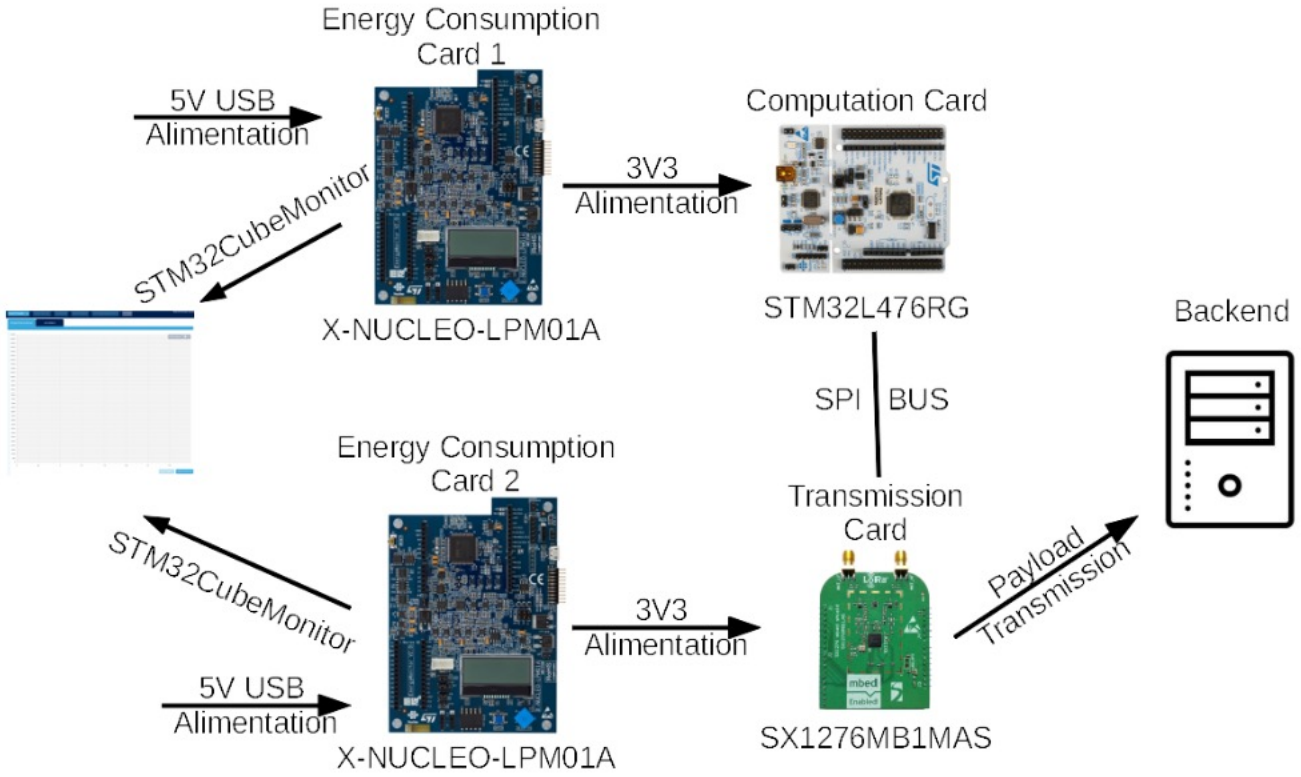
DNS-based dynamic context resolution for SCHC

ICC 2020 - 2020 IEEE International Conference on Communications (ICC)
https://doi.org/10.1109/ICC40277.2020.9148910



Provisioning LSTM Models in DNS

***Embedding ML Algorithms onto LPWAN Sensors for Compressed Communications* – PIMRC 2021**



Merci !

Contact us !

sandoche.balakrichenan@afnic.fr
benoit.ampeau@afnic.fr

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