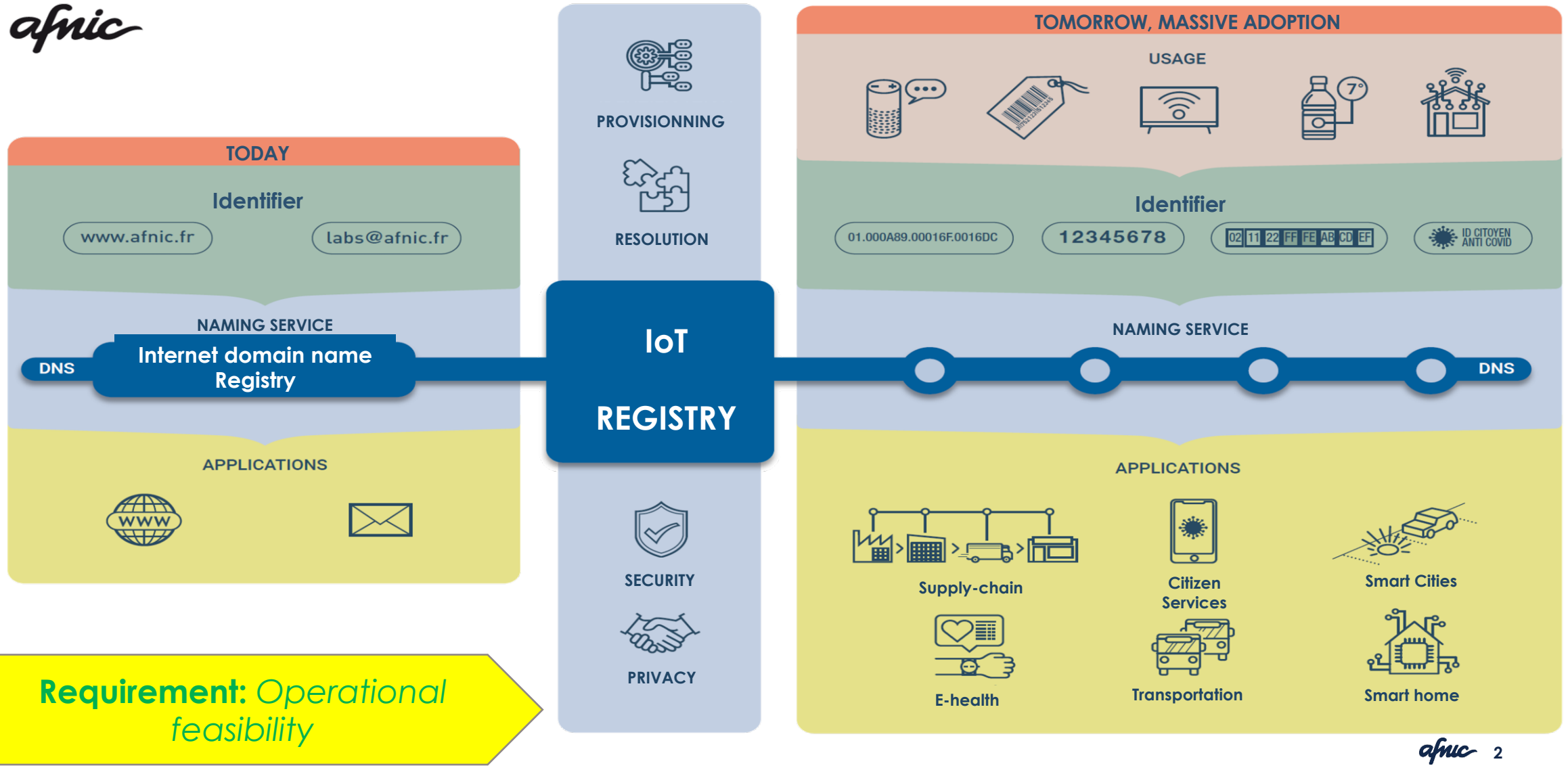
# The path from an Internet registry to an IoT registry based on DNS

Sandoche
BALAKRICHENAN

Nov. 16th 2021

afnic
Internet
made in France

# Hypothesis




**Requirement:** *Operational feasibility*

# How we are planning to achieve this vision?

**DONE**

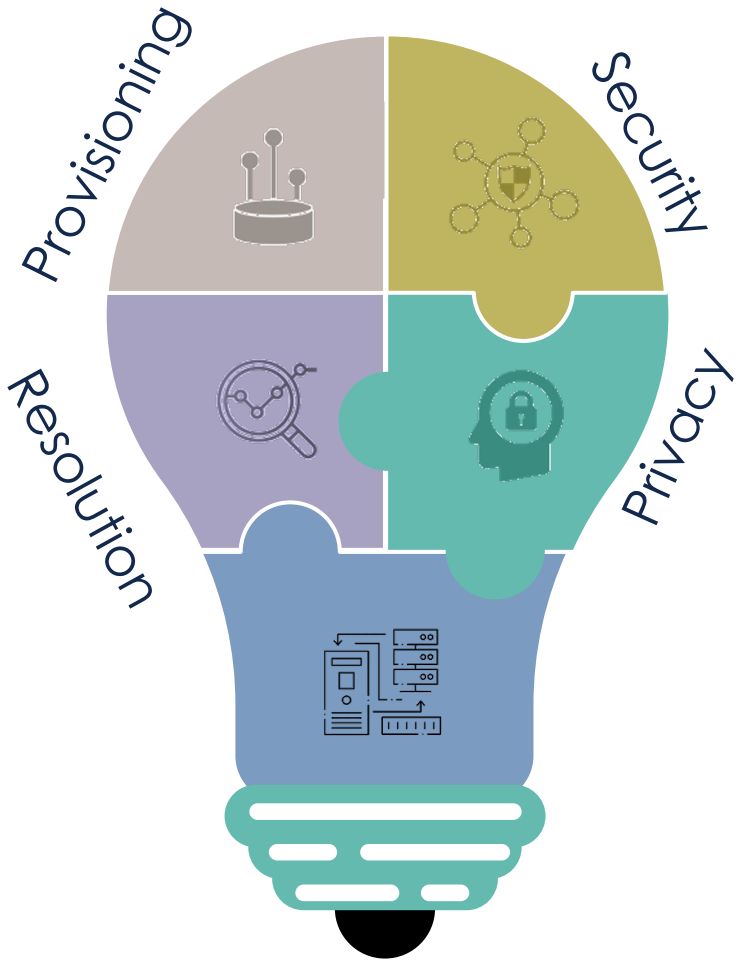
## WINGS

Widening interoperability for networking Global supply Chains

**PoC**

LoRa Alliance®

**DNS Service**




**ONGOING**

## DINS*

DNS Naming and Services for Secure Seamless IoT

**ONGOING**

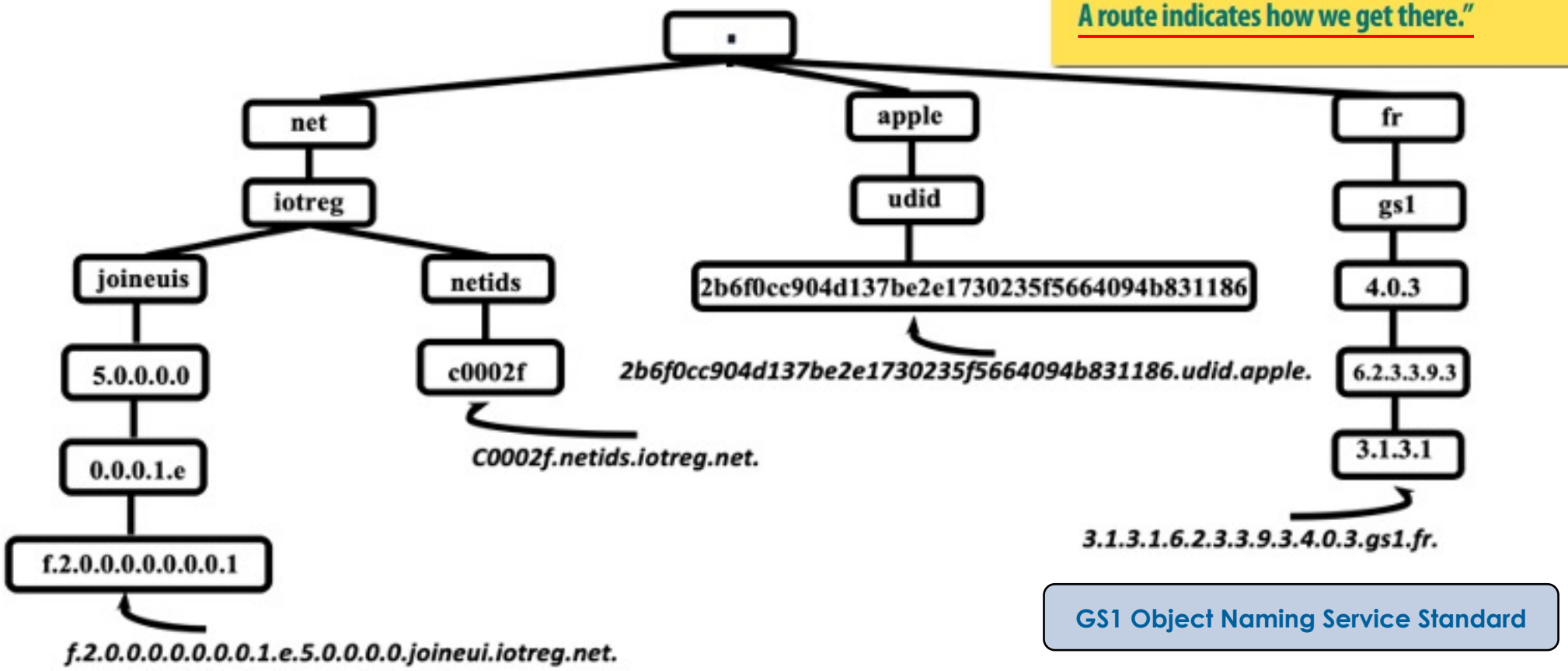
## PIVOT*

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."

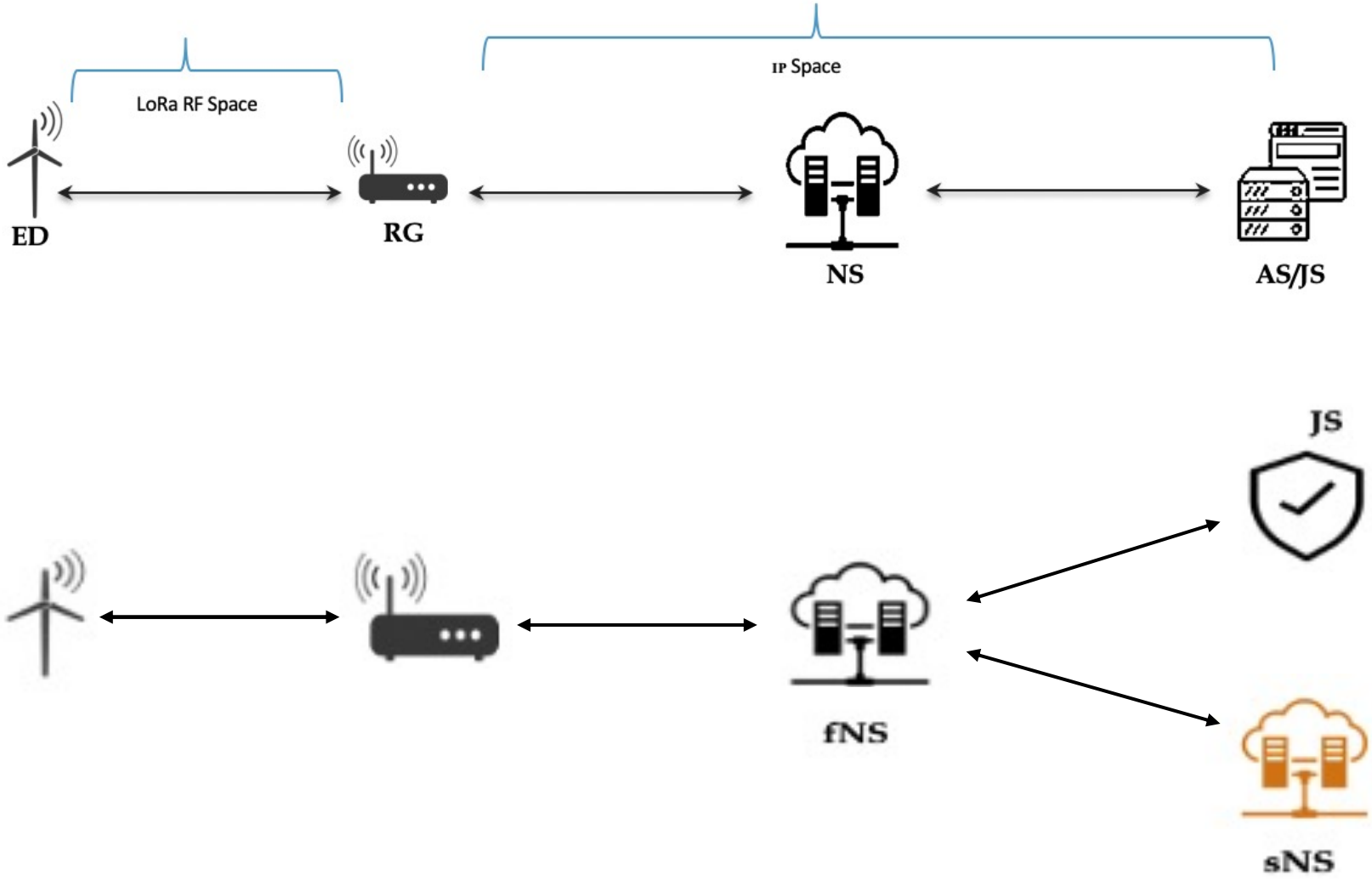
—Jon Postel, RFC 791




LoRaWAN Backend Interfaces specification

GS1 Object Naming Service Standard

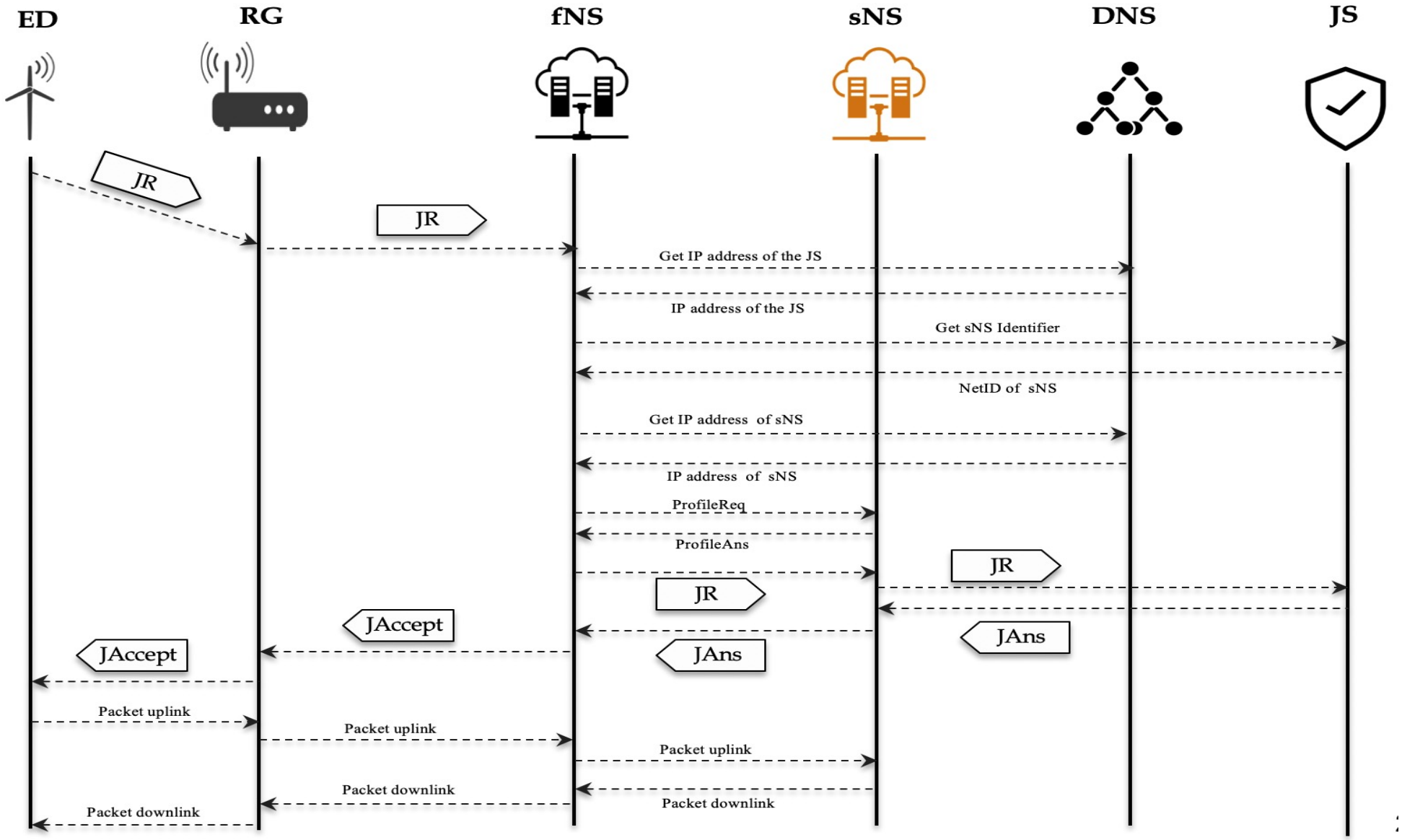
# LoRaWAN Architecture basic vs Roaming



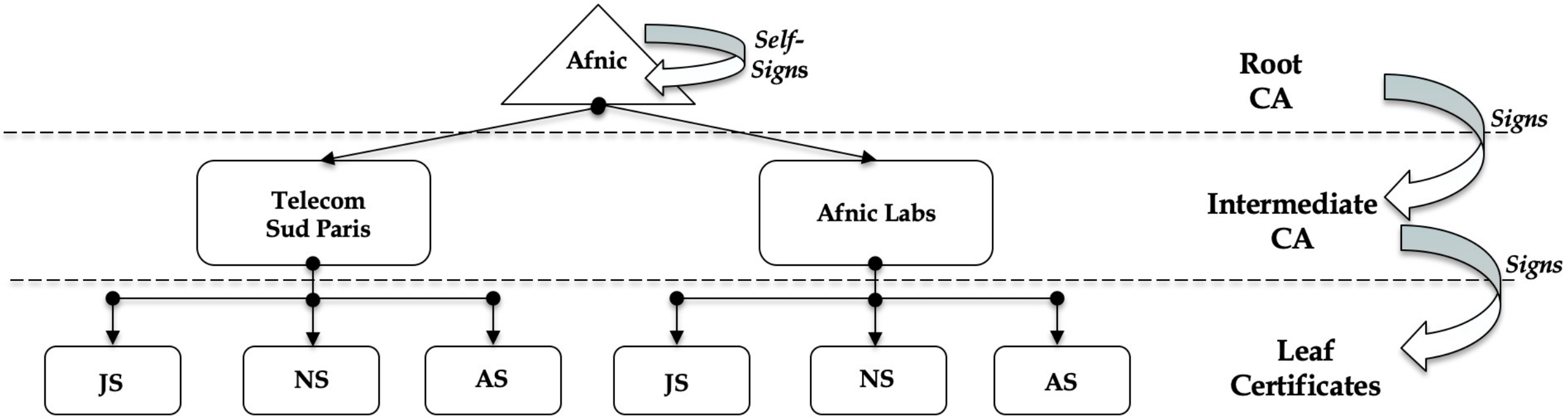
# Prior Configuration Parameters for Roaming

| |
|---|
| Peer Net-ID |
| Roaming Policy |
| Peer's channel plan |
| Peer's fNS URL |
| Peer's sNS URL |
| Peer's NS IP address |
| Peer JS URL |
| Peer JS IP Address |
| Peer JS Http Credentials |

# Roaming with minimum prior configurations – DNS Resolution

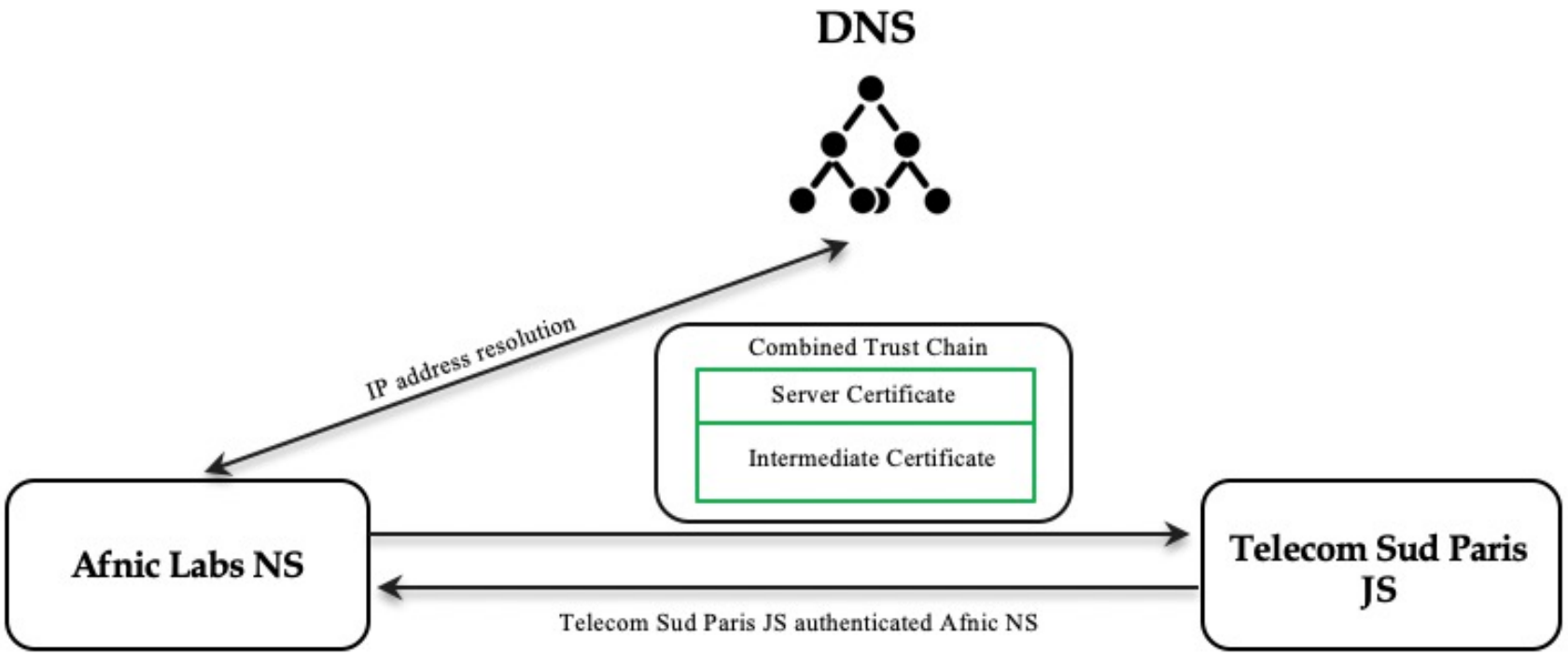


# Adding Security – Certificate Provisioning – IoTRoam PoC

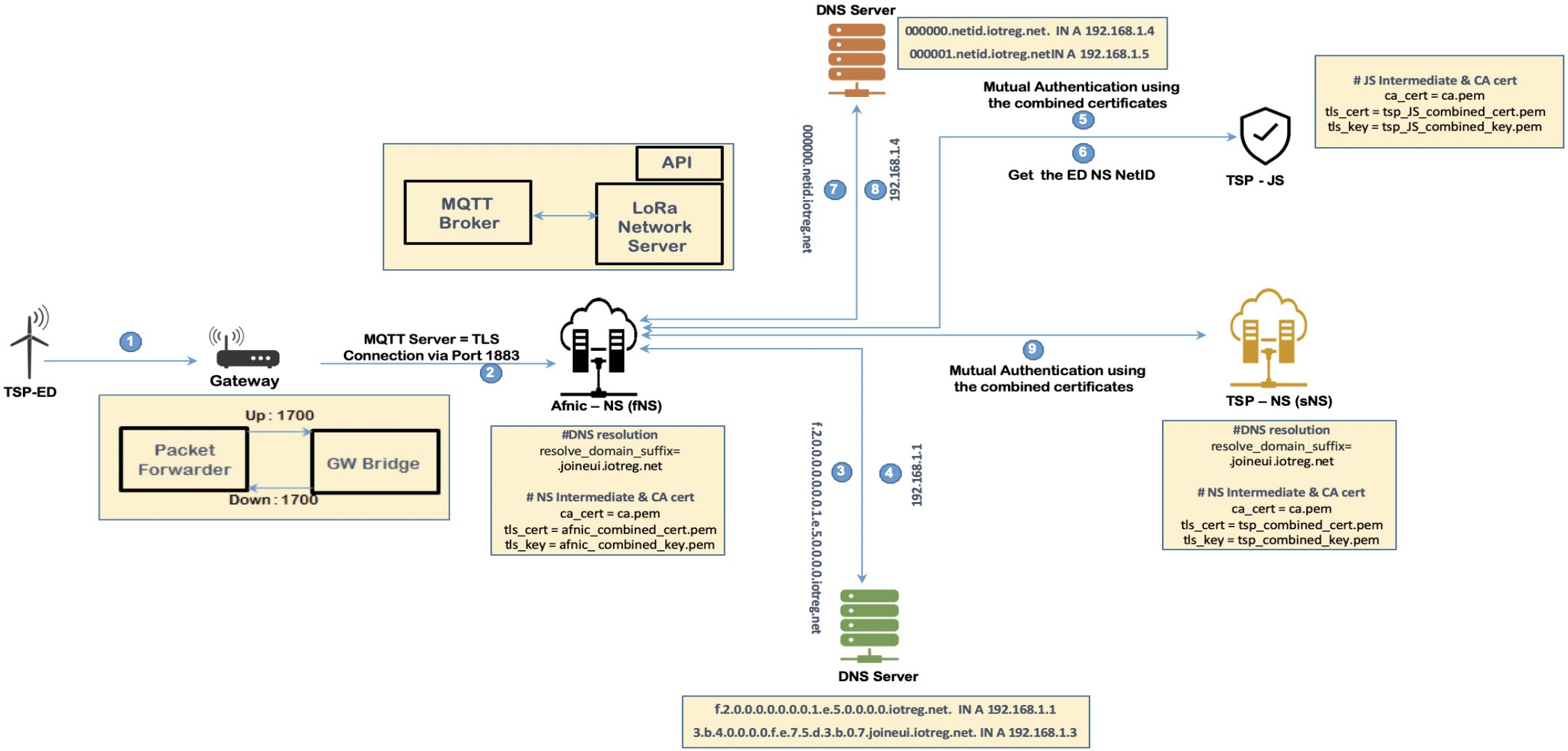



Call for collaboration - https://github.com/AFNIC/IoTRoam-Tutorial

# Adding Security – Certificate Validation

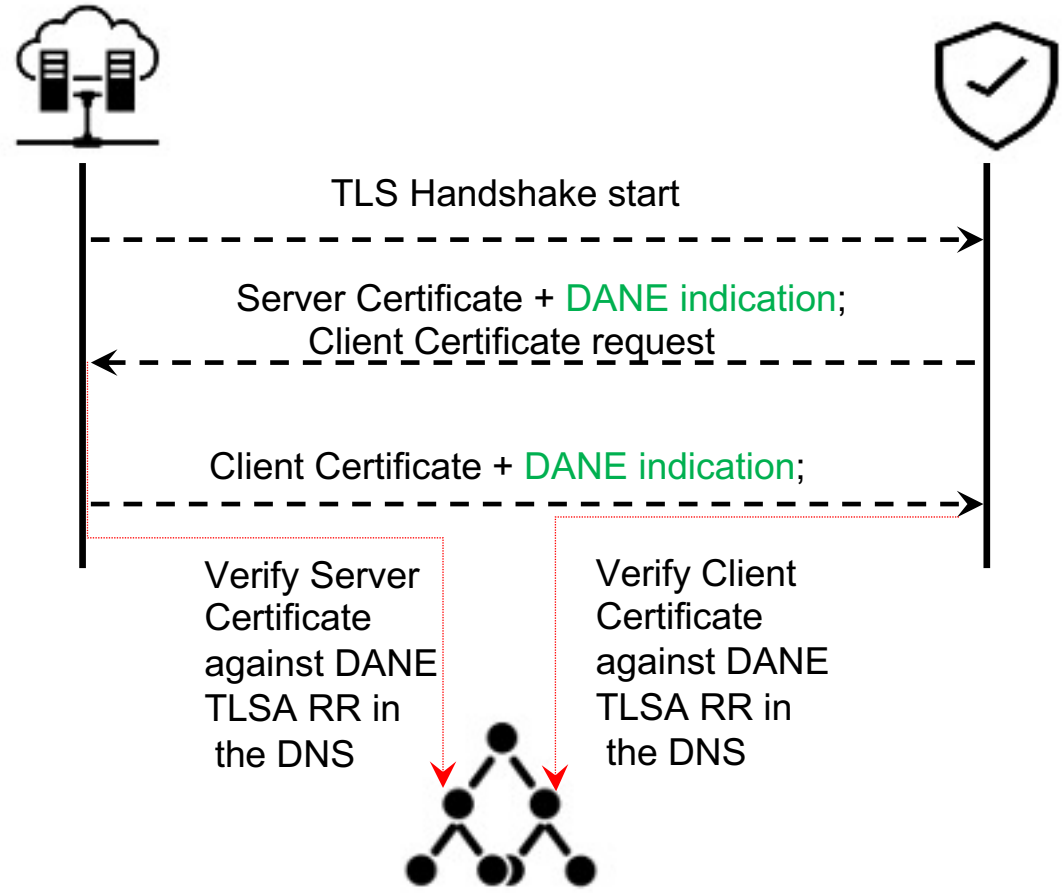


# IoTRoam Platform

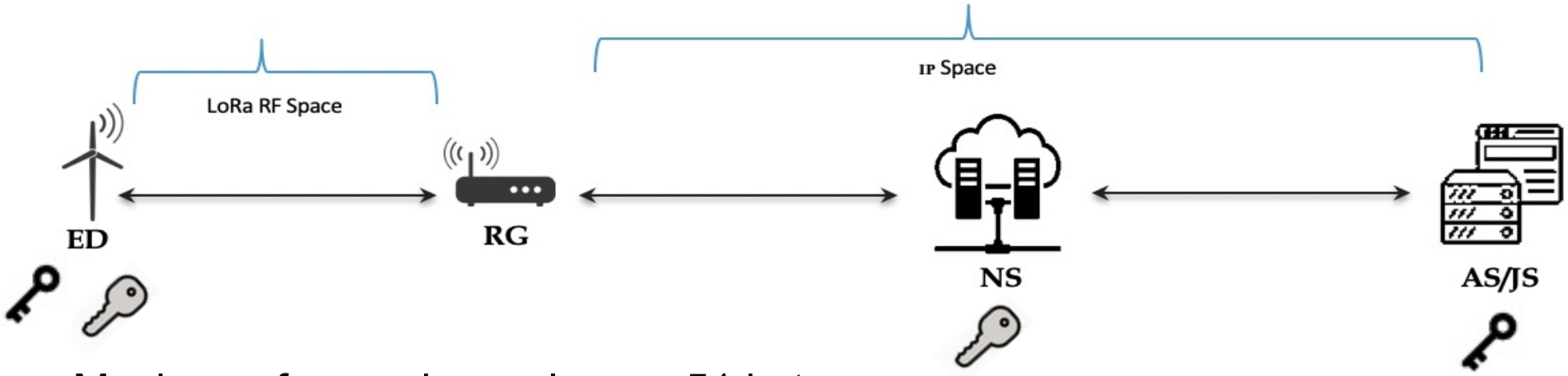


# Using DANE Client Authentication (Ongoing work)

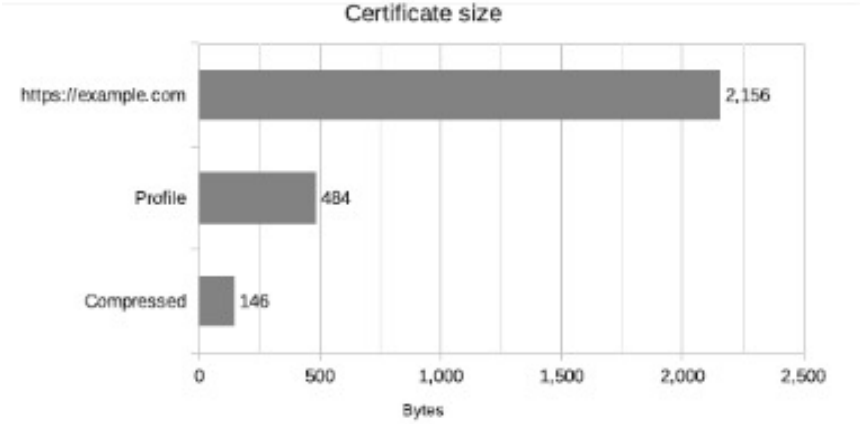
## Enables using self-signed certificate with multiple Root CA's



# Compressing X.509 certificates for constrained LoRaWAN use-case (Ongoing work)




- Maximum frame size as low as 51 bytes
- LoRaWAN uses 128-bit AES pre-shared symmetric keys




Source: F. Frosby et al.

- LAKE IETF WG, LPWAN IETF WG

# Privacy Challenges & Solutions envisioned

- Protecting the IoT device identity – *Ephemeral & Application Identifiers*
- Protecting the metadata – *Content Object Security* (Content disclosure attributed to designated receivers)
- How to handle Object Security in decentralized manner? – *DNS based PKI*
- Standardised crypto library framework – *Deployment on RIOT OS*
- Architecture validation - *IoTRoam*

sandoche.balakrichenan@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