Journées lp-wan
7-8 Juillet 2022
Toulouse

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Federated roaming for IoT using private DNS Resolutions

Arnol LEMOGUE
Ivan MARTINEZ
Laurent TOUTAIN
Ahmed BOUABDALLAH

LoRa Alliance® Member

AGENDA

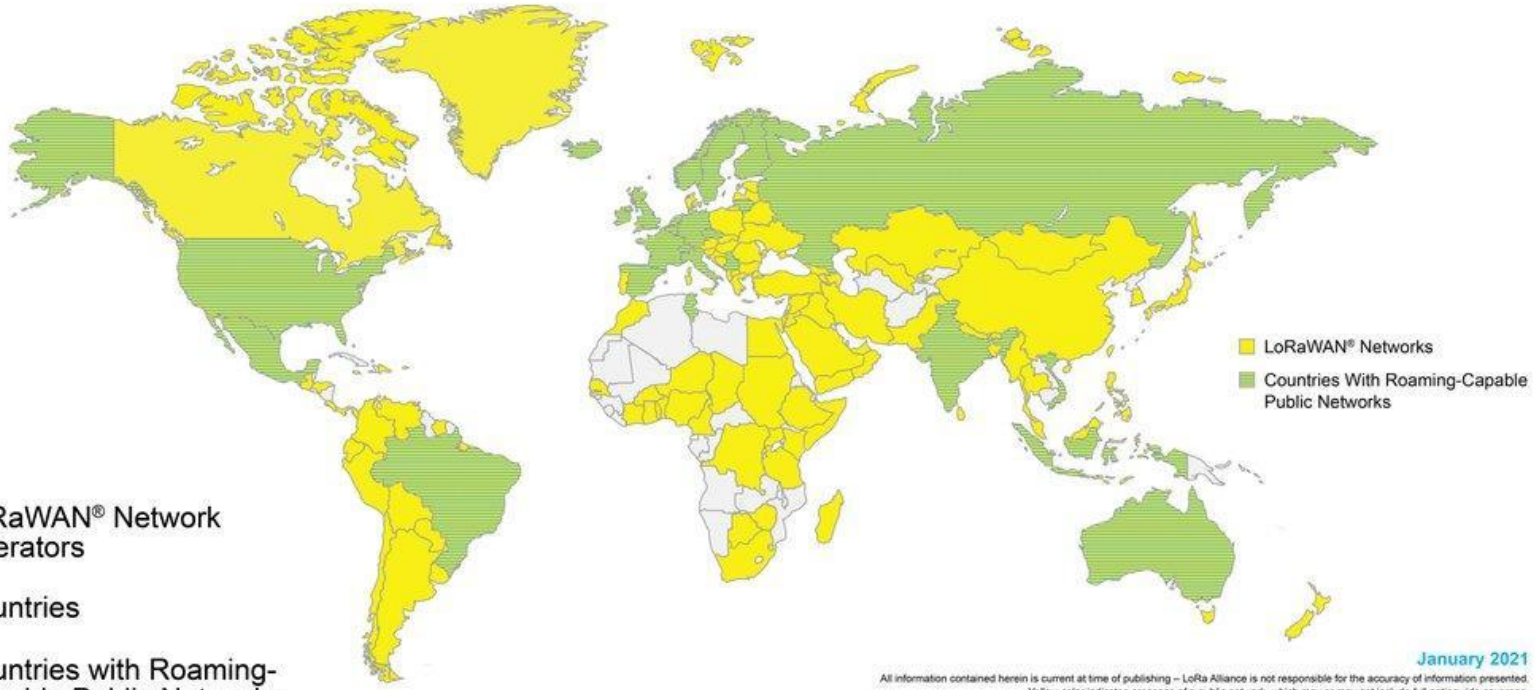
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

INTRODUCTION

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Availability of LoRaWAN® Networks and Roaming Capability

LoRa Alliance®



150 LoRaWAN® Network Operators

163 Countries

27 Countries with Roaming-Capable Public Networks

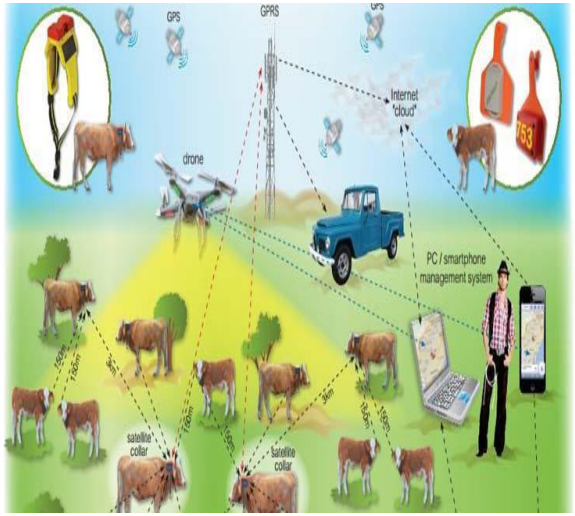
January 2021

All information contained herein is current at time of publishing – LoRa Alliance is not responsible for the accuracy of information presented.
Yellow color indicates presence of a public network, which may or may not include full nationwide coverage.
Blue lines indicate presence of a roaming-capable public network, does not indicate which networks it currently has roaming agreements with.

I. Roaming use cases [1,2,3]

Some use cases :

- On parcels: Tracking a parcel or valuable item in motion
- On transport: tracking the position of vehicles (boats, cars, bikes, trucks, planes, ...)
- On the animals: determine the position and health of the animals that change environment according to the season.



[1] https://www.groupestarservice.com/blog/comment-liot-optimise-la-logistique-du-dernier-kilometre/, To be consulted on 26 March 2022
[2] http://univida fup.edu.co/bienestar/la-ganaderia-se-apunta-al-internet-de-las-cosas/, To be consulted on 26 March 2022
[3] https://www.thomasnet.com/insights/how-the-iot-is-improving-the-logistics-sector/; To be consulted on 26 March 2022

EXISTING ROAMING ARCHITECTURES

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

II. EXISTING ROAMING ARCHITECTURE : IoTRoam

1.1 Brief description of IoTRoam [5]

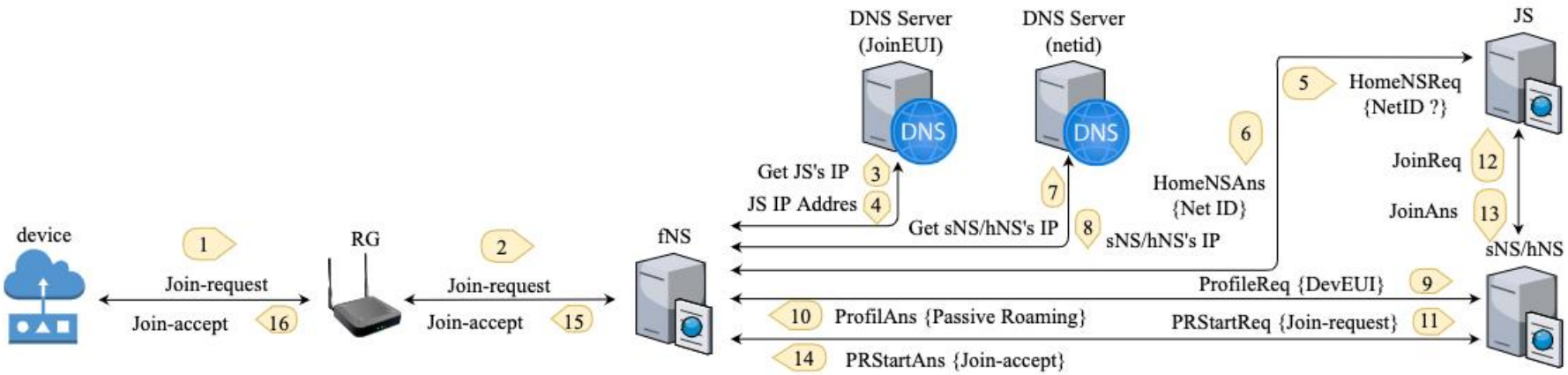
Main objectives:

- Federated IoT Roaming solution.
- DNS Resolutions to identify hNS.
- Offer portability between NO
- No ED modifications

Solution key points:

- Passive roaming activation.
- JoinEUI DNS resolution.
  - NetID.netids.iotreg.net
- NetID DNS Resolution
  - Nibbles(JoinEUI).joineuis.iotreg.net

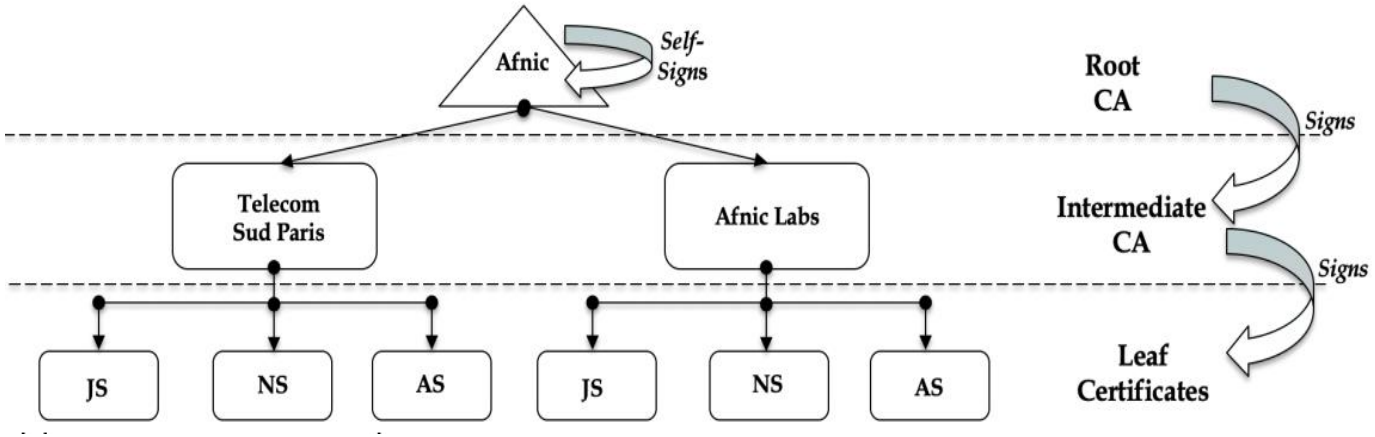
Roaming Architecture:



[5] IoTRoam – Design and Implementation of a Federated IoT Roaming Infrastructure using LoRaWAN, *Sandoche Balakrichenan, Antoine Bernard, Michel Marot*, Benoit Ampeau, 6 Jan 2021

Certificate provisioning:

- Centralized deployment:
  - LoRa Alliance delivers Intermediate CA
  - Operators generate JS, NS and AS leaf certificates to secure exachanges using TLS



[5] IoTRoam – Design and Implementation of a Federated IoT Roaming Infrastructure using LoRaWAN, *Sandoche Balakrichenan, Antoine Bernard, Michel Marot*, Benoit Ampeau, 6 Jan 2021

II . EXISTING ROAMING ARCHITECTURE : IoTRoam

1.3 Limitations associated with this architecture [5]

IoT Roam effectively provides a roaming solution but …

- Device Owner (DO) needs to provision IEEE EUI 64-bit identifier (JoinEUI)
  - It is costly
  - IEEE EUI-64 is not intended for this purpose
  - It has to be changed when a device is purchased/sold to another customer.
  - Lock-in situation with a unique NO.
- It exposes the Join Server to external networks (Security risk)
- The LoRa Alliance manages JoinEUI allocations to ensure its uniqueness
- Only LoRa Alliance controls the DNS zone and DNS updates that ensures the correspondence between JoinEUI and JS or NetID and NS.
- Centralized provision of certificates.

[5] IoTRoam – Design and Implementation of a Federated IoT Roaming Infrastructure using LoRaWAN, *Sandoche Balakrichenan, Antoine Bernard, Michel Marot*, Benoit Ampeau, 6 Jan 2021

PROPOSED ROAMING ARCHITECTURE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

III. PROPOSED ARCHITECTURE

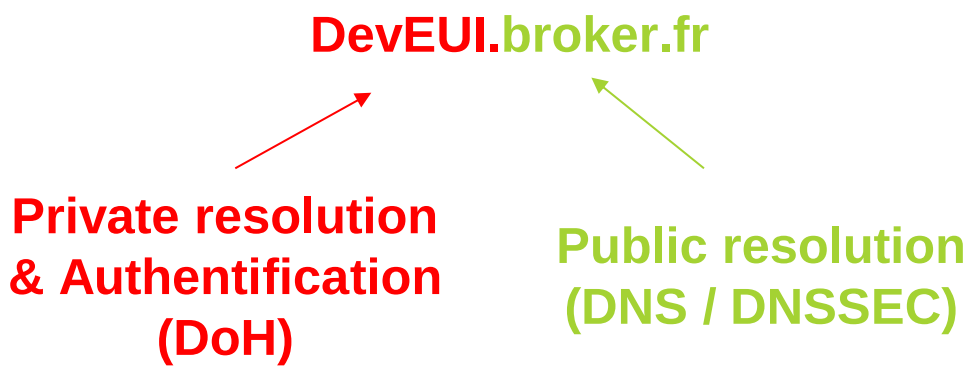
2.1 Brief description

Main objectives:

- Federated IoT Roaming solution.
- DNS Resolutions to identify hNS.
- Offer portability between operators (No ED modifications)
- Decentralized provision of Certificates.
- Decentralized Roaming architecture with DNS Brokers

Proposed solution:

- Passive roaming activation.
  - No Join Server exposition
- DNS Resolution :
  - DevEUI resolutions with DNS Brokers
  - DoH with mutual authentication
- Reduce signalling.
  - Combine DNS resolution and device authentication.

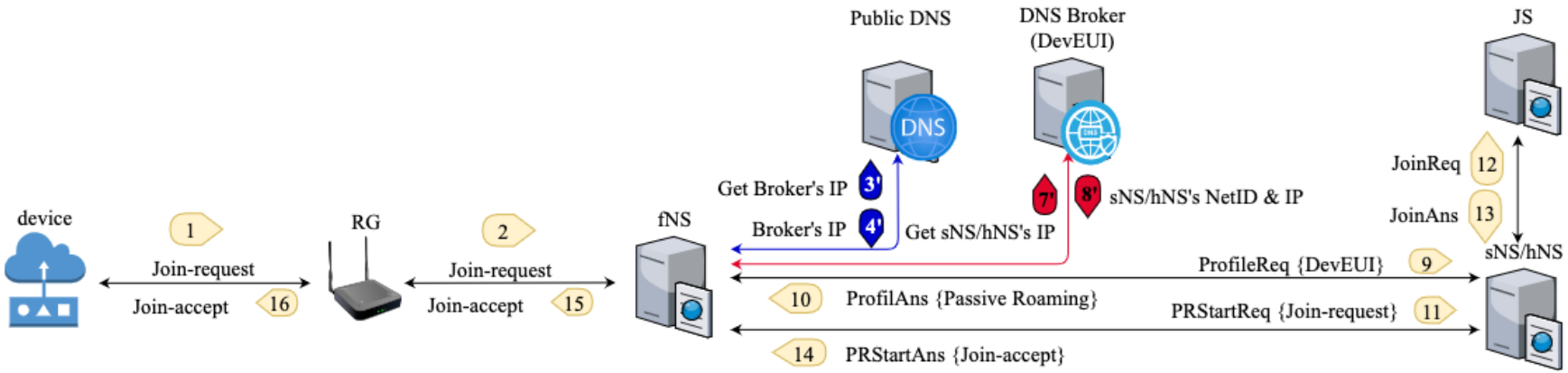


IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Paper accepted :https://manage-iot.future-iot.org/2022-agenda-overview/

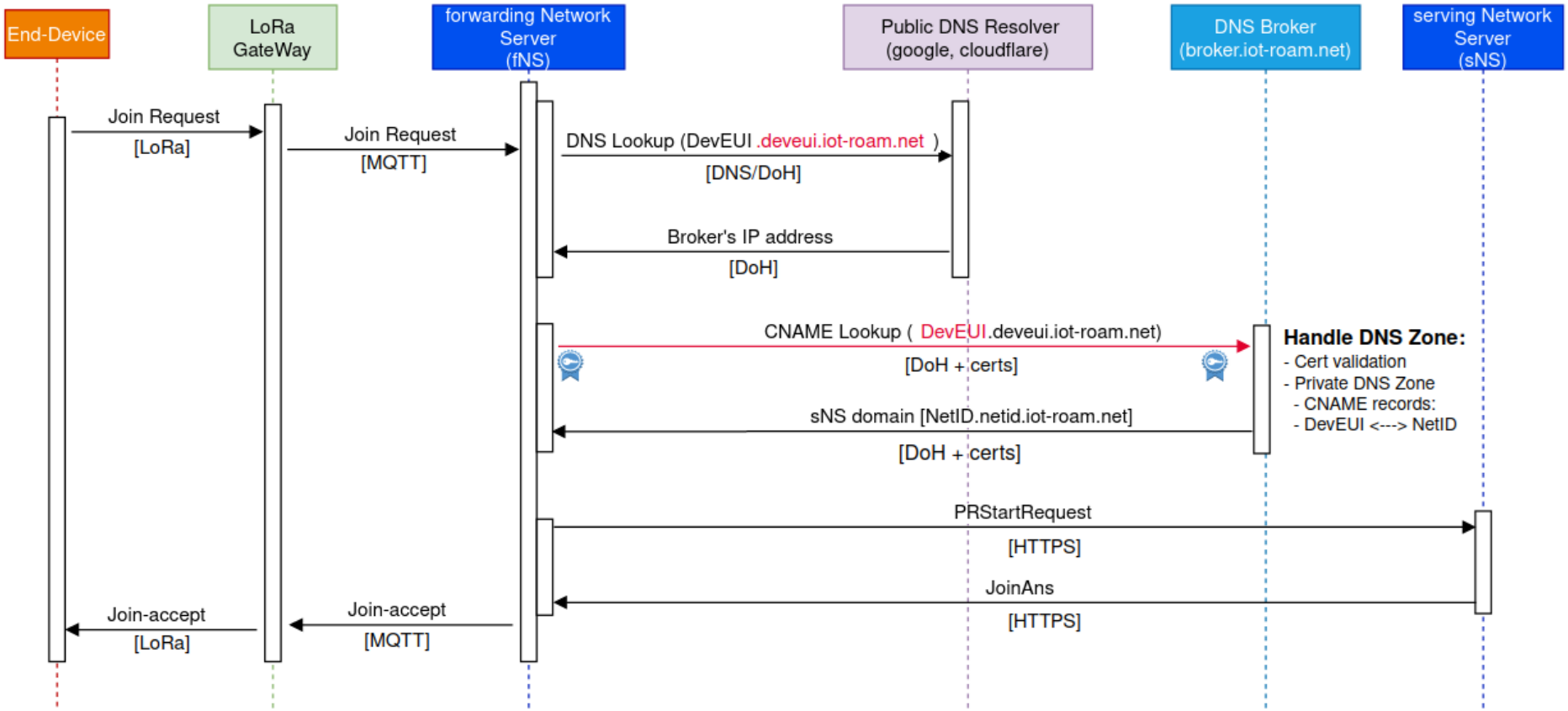
II. PROPOSED ARCHITECTURE

2.2 Block diagram



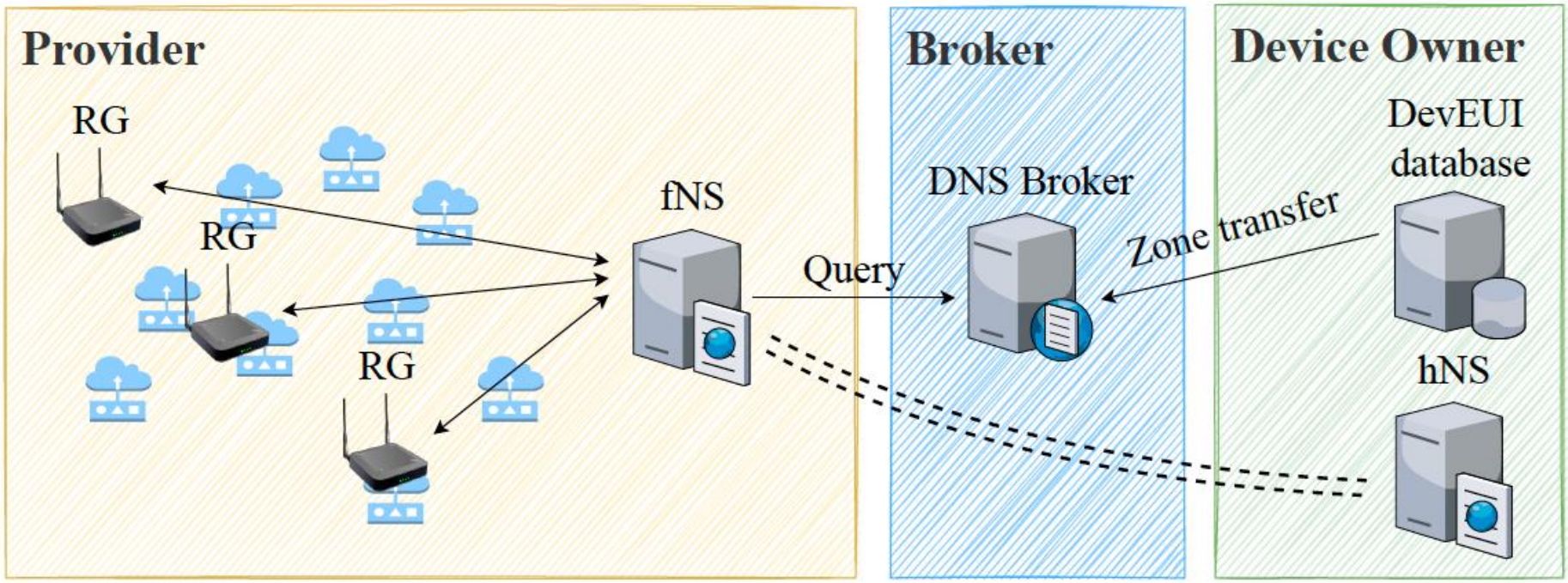
III. PROPOSED ARCHITECTURE

2.3 Flowchart for join procedure



II. PROPOSED ARCHITECTURE

2.2 DNS Broker architecture

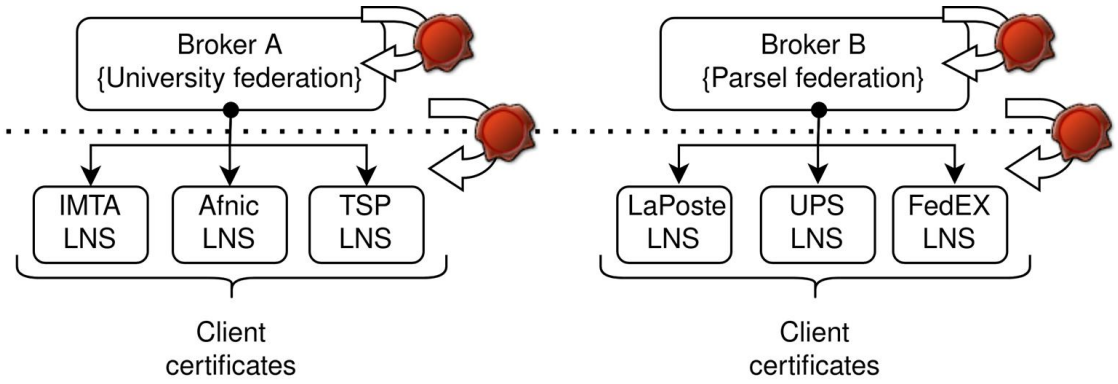


With the DNS Broker we divide the resolution into two parts:

- ***Public*** part where the IP of a DNS broker is resolved.
- ***Private*** part where the DevEUI is resolved to a NetID/IP address with CNAME.

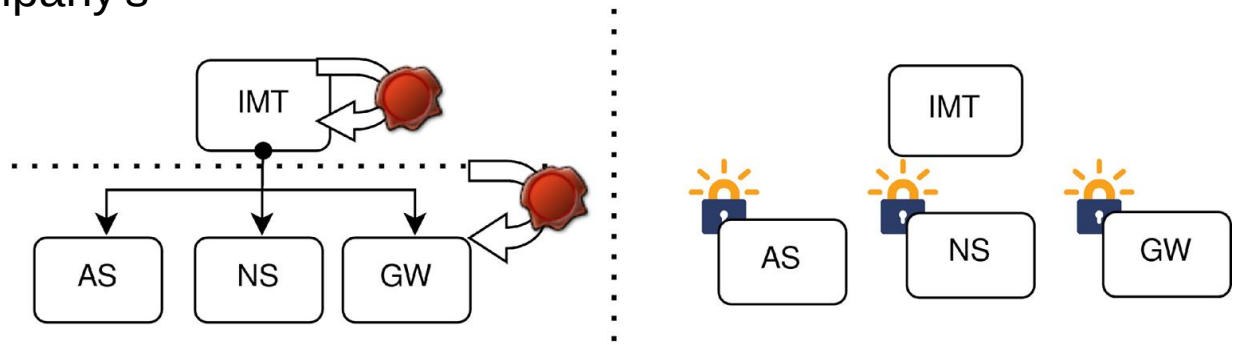
Roaming Certificates:

- Decentralized provision of client Certificates.
- One broker per federation:
  - Client cert. provisioning.
  - DevEUI DNS Zones.
    - -- {DevEUI <--> NetID <--> LNS IP}
  - A company may be part of multiple federations



LNS Certificates:

- In accordance with company's policy:
  - Let's Encrypt
  - Self-signed
- Certs for :
  - NS, AS, GW



Traffic volume at the fNS when Joining [# RTTs and # Packets].

Types	Parameter	IoTRoam JR ($n=1$) #	IoTRoam JR ($n=1$) Len. [B]	IoTRoam JR ($n>1$) #	IoTRoam JR ($n>1$) Len. [B]	Proposed architecture JR ($n=1$) #	Proposed architecture JR ($n=1$) Len. [B]	Proposed architecture JR ($n>1$) #	Proposed architecture JR ($n>1$) Len. [B]
DNS	IP	8	160	0	0	4	80	0	0
	UDP	8	56	0	0	4	32	0	0
	DNS	8	606	0	0	4	332	0	0
HTTPS	TCP Sig'	21	1140	3	156	27	1452	3	152
	TLS	15	18167	6	2811	24	25788	6	2793
TLS Gran.	IP	15	300	6	120	24	480	6	120
	TCP	15	480	6	192	24	768	6	192
	C. Hello	3	858	0	0	3	870	0	0
	S. Hello	3	8198	0	0	5	10862	0	0
	C. Cipher	3	5775	0	0	3	6166	0	0
	App. Data	6	2556	6	2499	13	6642	6	2481
# of packets		44		9		55		9	
RTTs		21		6		24		6	

'(SYN – SYN/ACK – ACK)

First Join Request

- DNS traffic: Decrease in the number of exchanges [8 to 4]
- HTTPS: Sligthly increase [15 to 24] due to DoH with mutual authentication.

Second Join Request

- No DNS exchanges in both
- HTTPS, TLS load is almost identical for the same RTTs.

CONCLUSION & PROSPECTS

Work done:

- Implementation of existing proposal
  - NO with modified version of Chirpstack LNS
  - DevEUI DNS Zone creation and transfer.
  - Implementation of first DNS Broker
- Implementation of PoC:
  - Architecture design
  - Chirpstack code source modification
  - Broker at dnsbroker.fr
  - Online tutorial for NO/DO and Broker: https://github.com/MarinoMtz/LoRaWAN-Roaming-Tutorial

To be done:

- Complete PoC with other partners:
  - DevEUI transfer Zone
  - Certificate delivering
- Testing campaign of the PoC.
  - Testing with others NO/DO
    - **Academic Federation ?**
  - Performance evaluation
  - Scalability assessment

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom