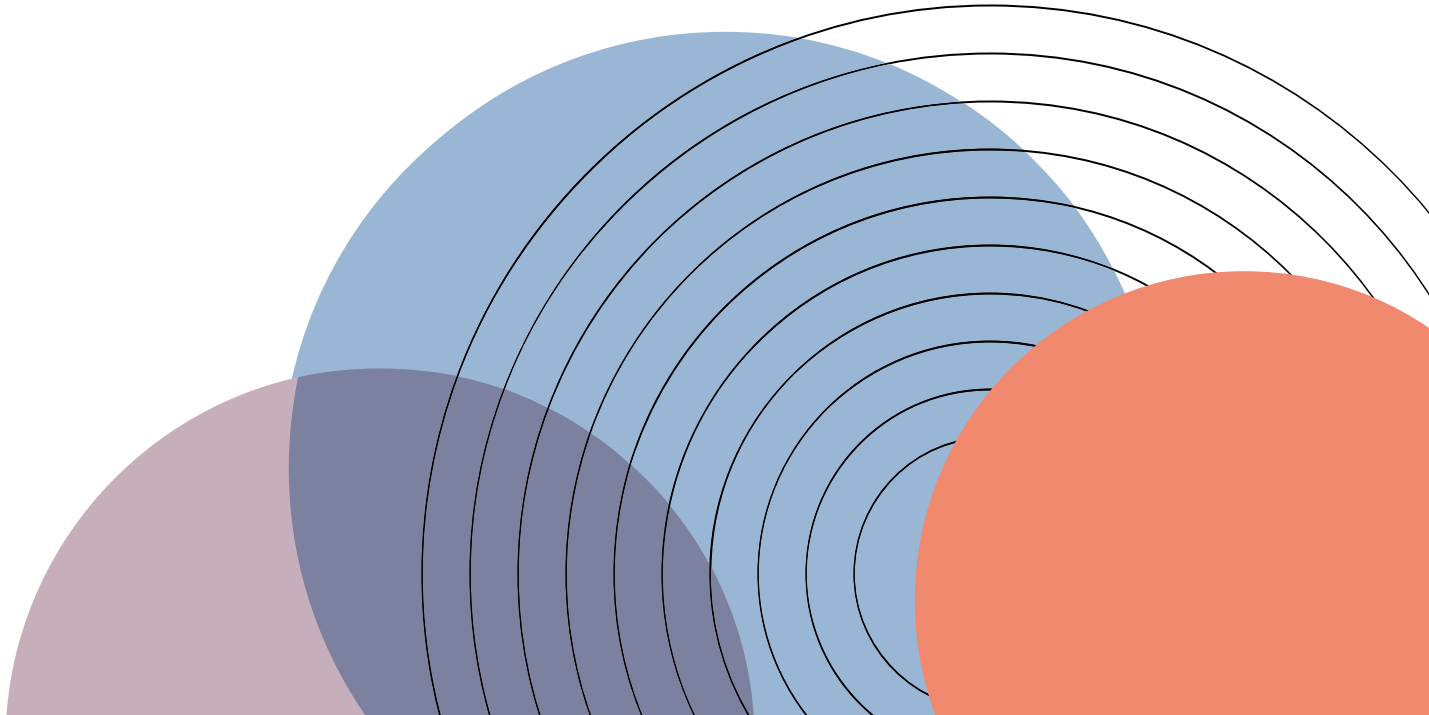
08 Juillet 2022

afnic
Internet
made in France

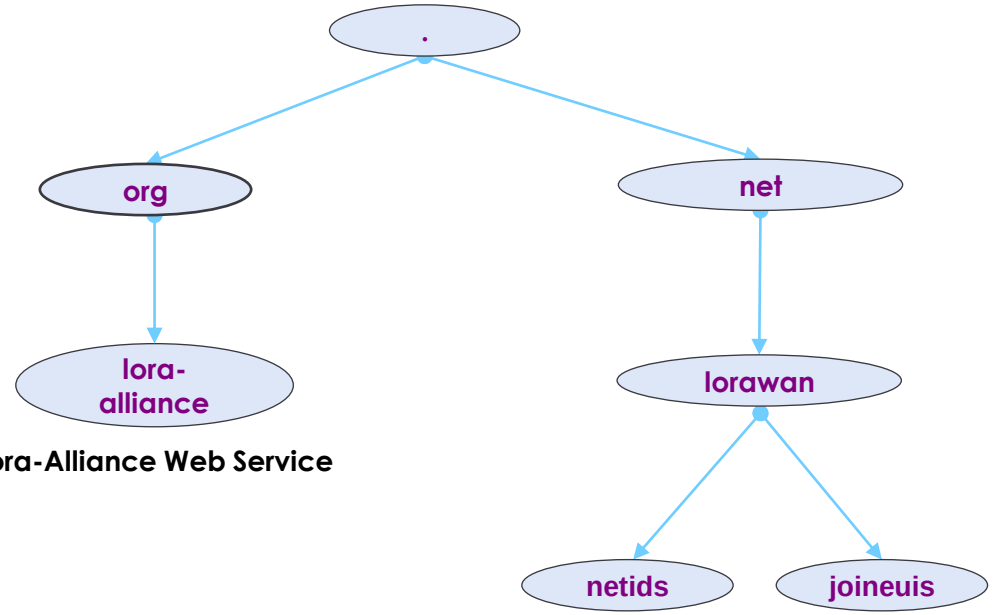
Role for DNS in LoRaWAN



DNS Usages in LoRaWAN as per the Specifications

- IoT device bootstrapping (OTAA)
- Roaming
- Portability

LoRa DNS Tree



"lora-alliance.org" ➔ Lora-Alliance Web Service

"netids.lorawan.net" ➔ Lora-Alliance Roaming Service

"joineuis.lorawan.net" ➔ Lora-Alliance OTAA Service

Ref: Section 20 of the LoRaWAN Backend Interfaces specification

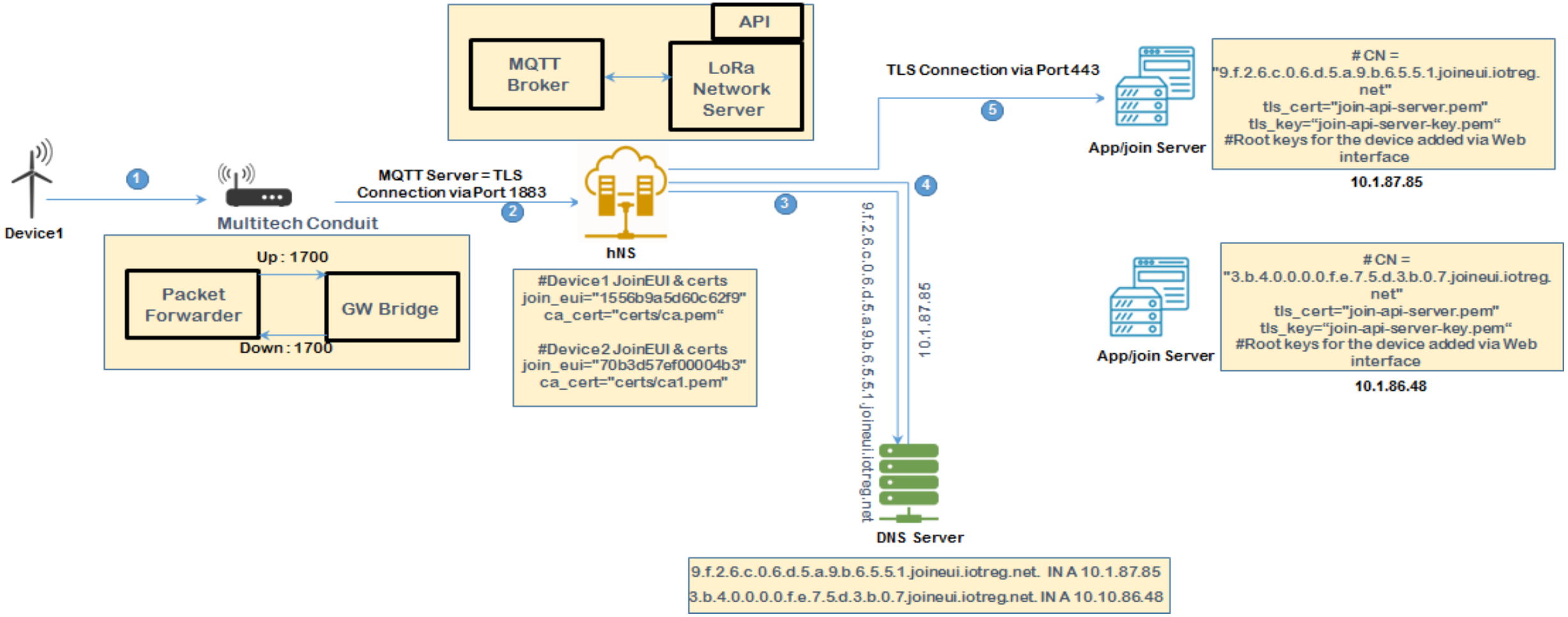
Pre-provisioning needed before OTAA

Device contains the DevEUI, NwkKey, AppKey, JoinEUI

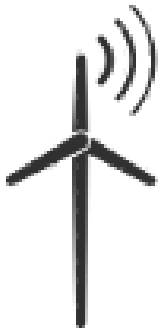
Network server contains the DevEUI, NwkKey

Appserver contains the DevEUI, AppKey

OTAA via DNS

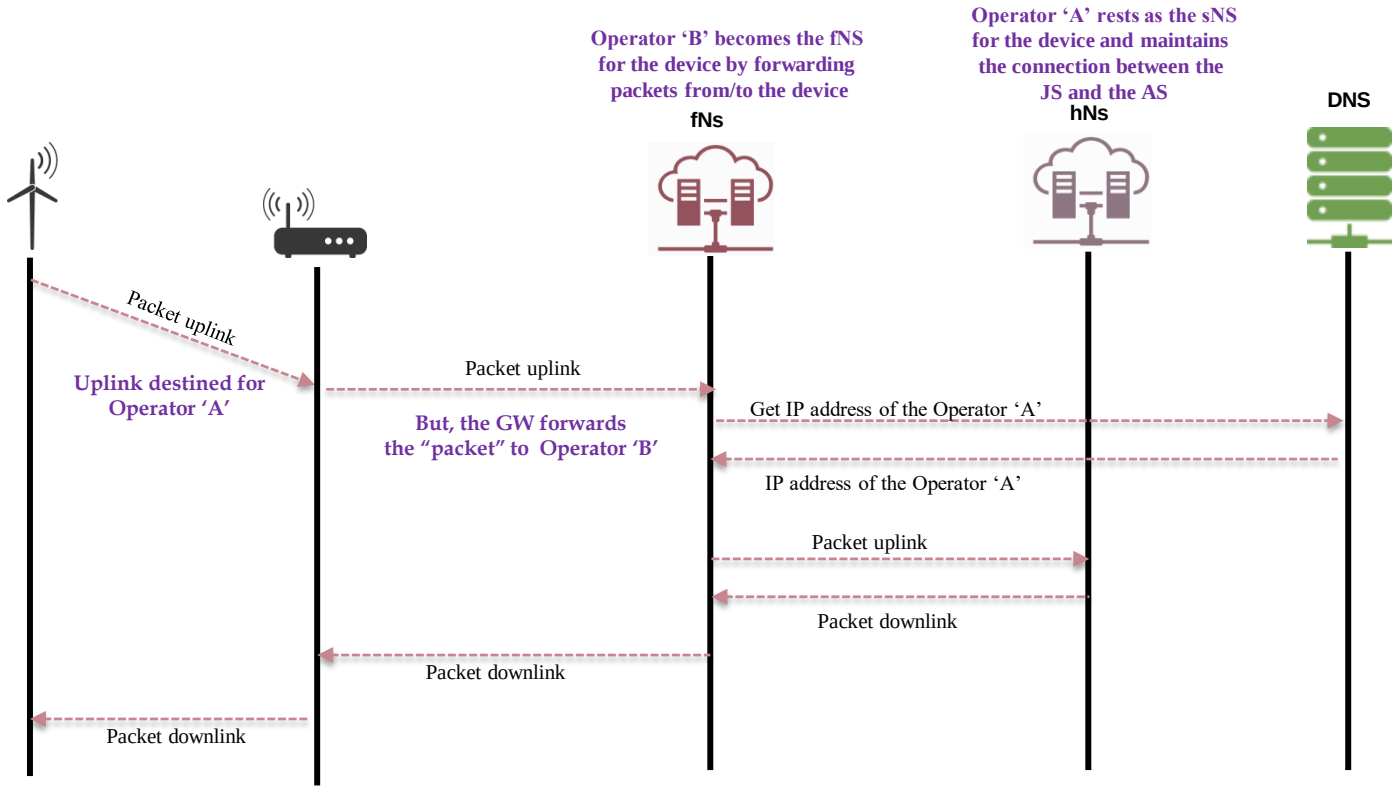

API
MQTT Broker
LoRa Network Server
TLS Connection via Port443
5
App/join Server
CN = "9.f.2.6.c.0.6.d.5.a.9.b.6.5.5.1.joineui.iotreg.net" tls_cert="join-api-server.pem" tls_key="join-api-server-key.pem" #Root keys for the device added via Web interface
10.1.87.85
Device1
1
Multitech Conduit
MQTT Server = TLS Connection via Port 1883
2
hNS
3
4
9.f.2.6.c.0.6.d.5.a.9.b.6.5.5.1.joineui.iotreg.net
10.1.87.85
Up : 1700
Packet Forwarder
GW Bridge
Down : 1700
#Device1 JoinEUI & certs join_eui="1556b9a5d60c62f9" ca_cert="certs/ca.pem"
#Device2 JoinEUI & certs join_eui="70b3d57ef00004b3" ca_cert="certs/ca1.pem"
App/join Server
CN = "3.b.4.0.0.0.0.f.e.7.5.d.3.b.0.7.joineui.iotreg.net" tls_cert="join-api-server.pem" tls_key="join-api-server-key.pem" #Root keys for the device added via Web interface
10.1.86.48
DNS Server
9.f.2.6.c.0.6.d.5.a.9.b.6.5.5.1.joineui.iotreg.net. IN A 10.1.87.85
3.b.4.0.0.0.0.f.e.7.5.d.3.b.0.7.joineui.iotreg.net. IN A 10.10.86.48

Information in the device after OTAA

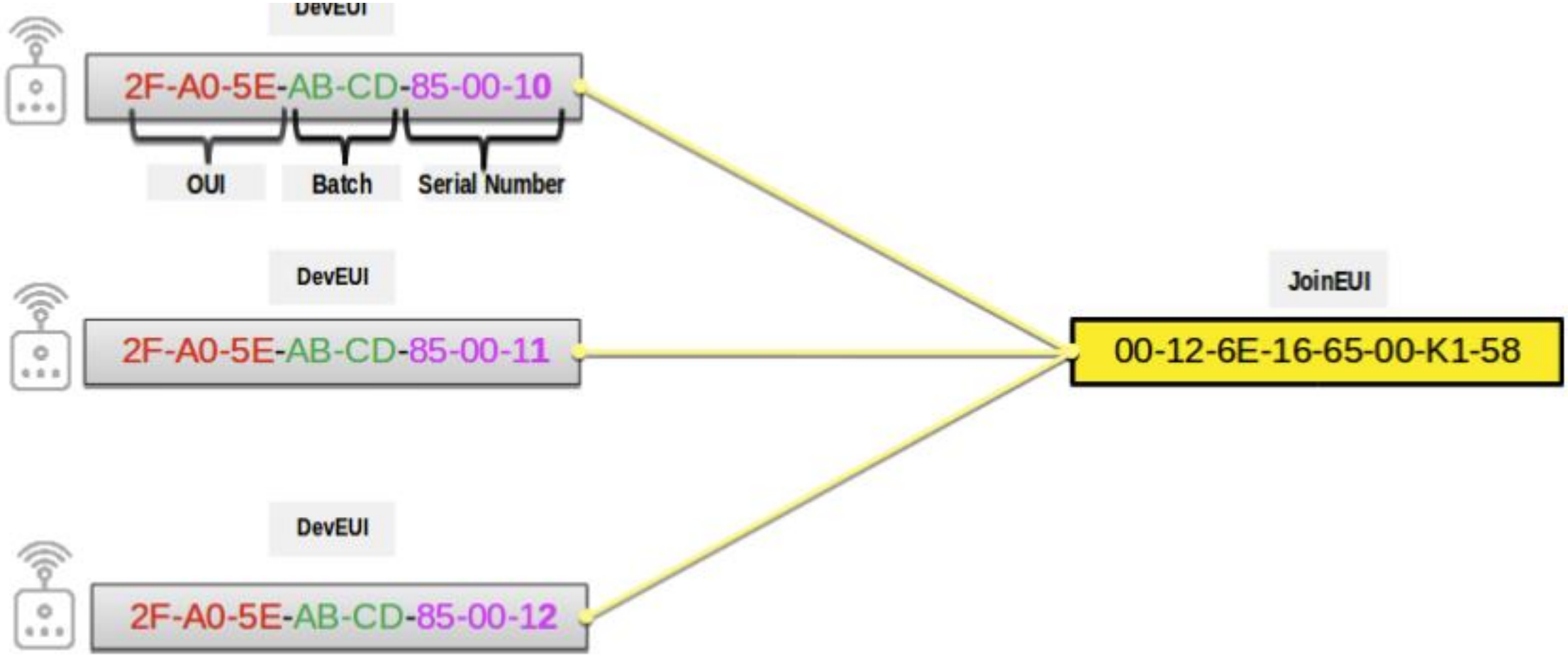


Device contains the
DevEUI, NwkKey, AppKey,
JoinEUI, JoinNonce, NetID,
DevAddr , NwkSIntKeyUp,
NwkSIntKeyDwn, NwkSEncKey,
AppSKey

Passive roaming using DNS



Number portability using DNS – 1/2



Number portability using DNS – 2/2

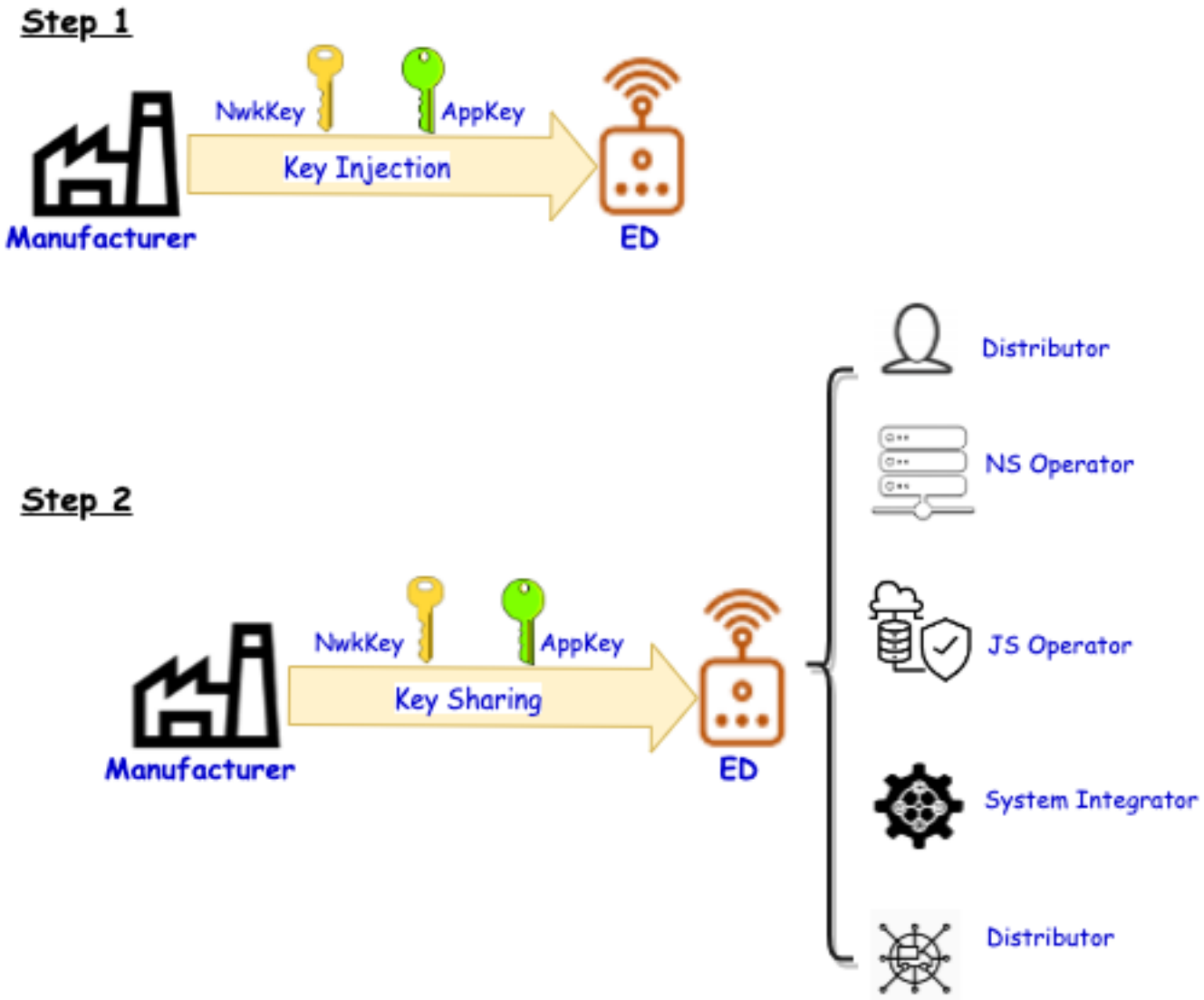
*.D.C.B.A.E.5.0.A.F.2.8.5.1.K.0.0.5.6.6.1.E.6.2.1.0.0.joineui.lora-alliance.org. IN A 1.2.3.4

Breaking the JoinEUI dependancy of the JS:

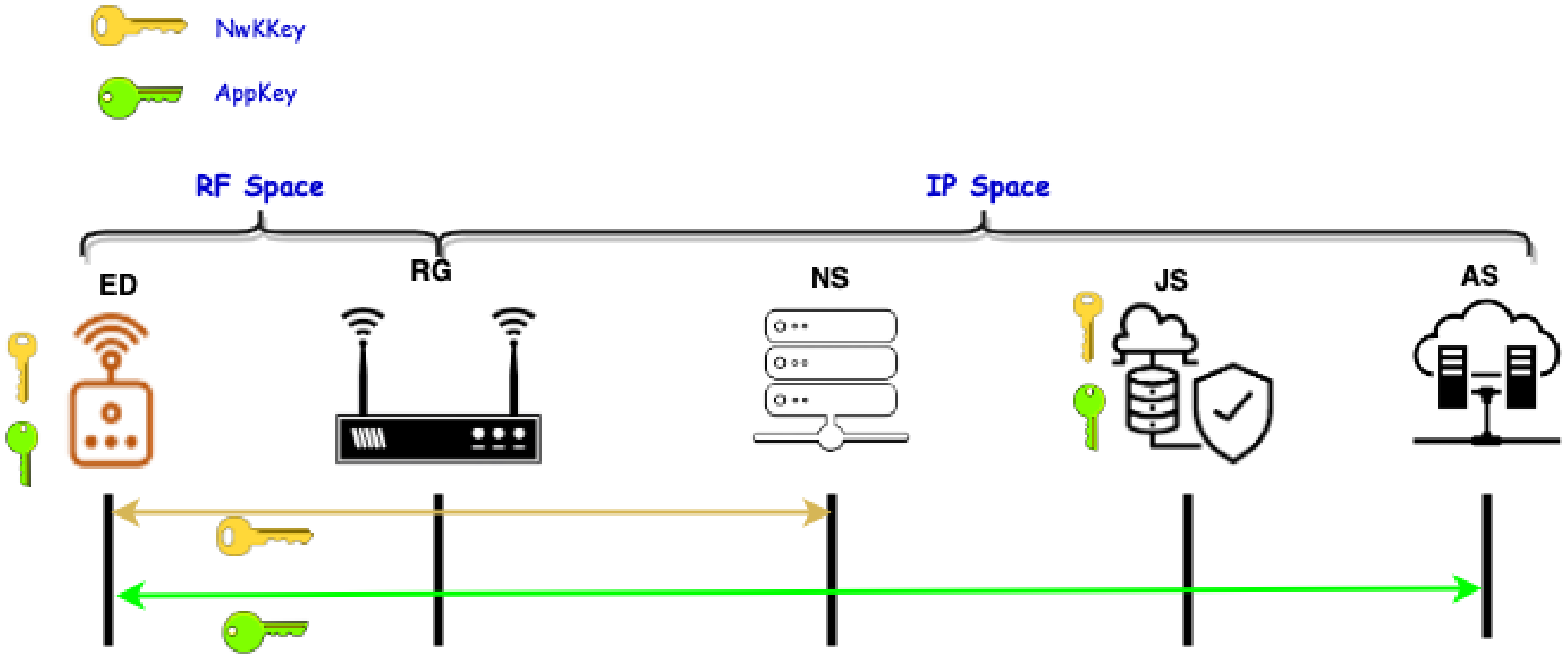
*.4.5.D.C.B.A.E.5.0.A.F.2.8.5.1.K.0.0.5.6.6.1.E.6.2.1.0.0.joineui.lora-alliance.org. IN A 1.1.1.1

Another role: DNS as the PKI

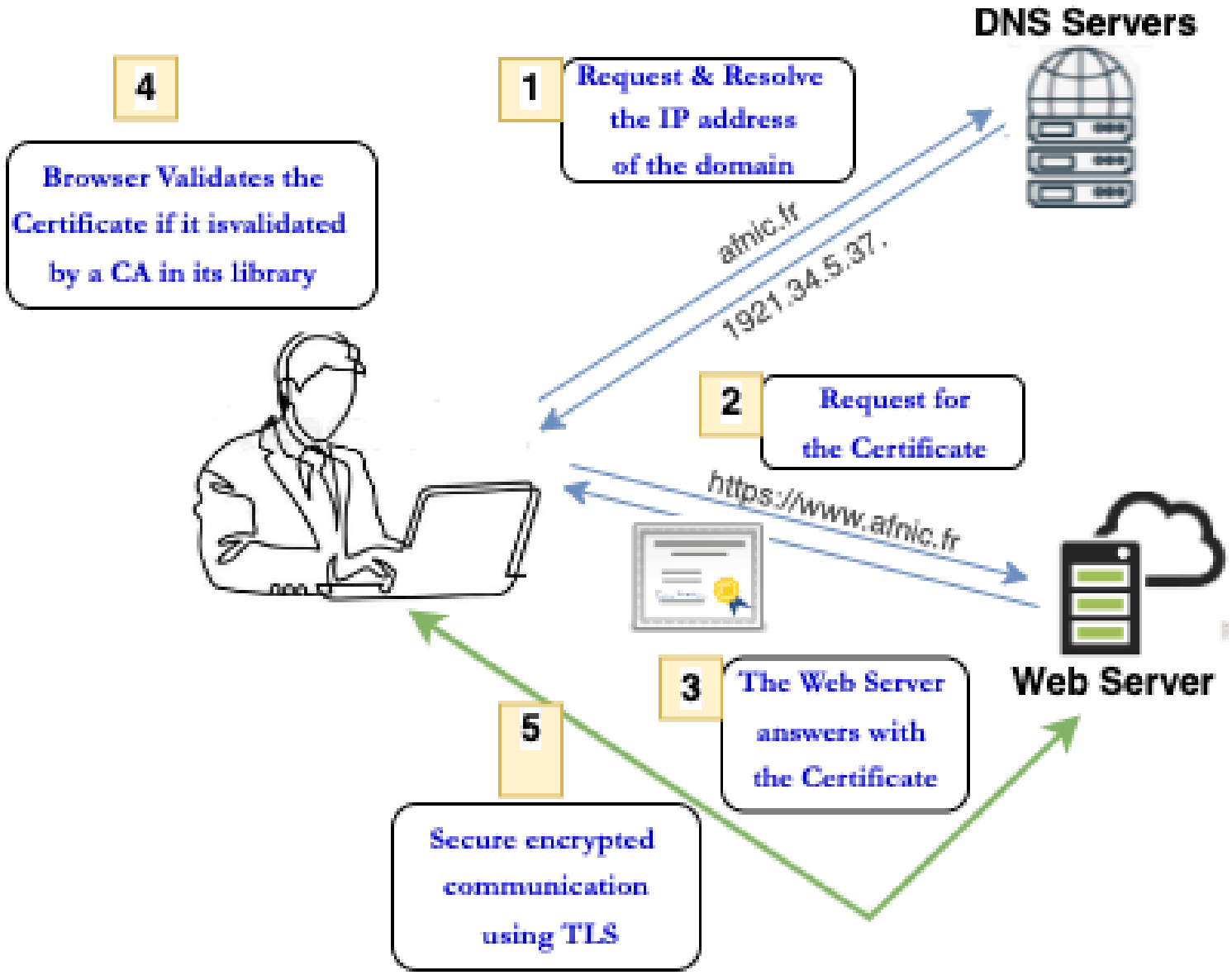
Key Sharing Challenge



LoRaWAN Key Distribution

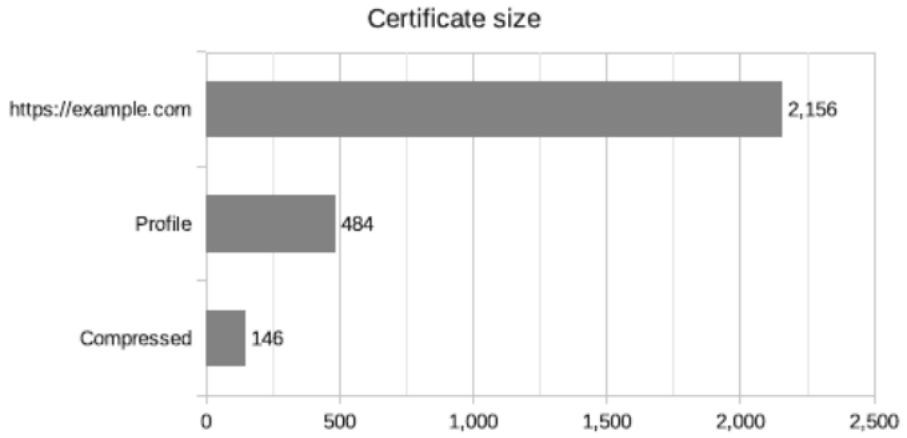


Web PKI using Public & Private Key



X.509 Certificates cannot be employed in the LoRa RF space

F. Forsby et al.



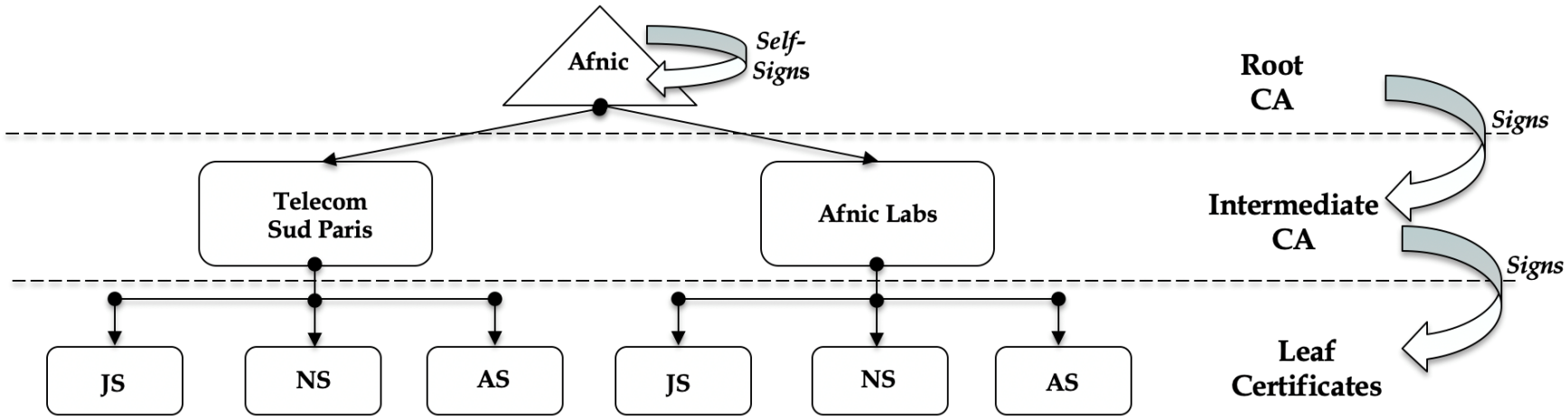
Data Rate (DR)	Spreading Factor (SF)	Channel Frequency	Uplink or Downlink	Bitrate (Bits/Sec)	Maximum User Payload Size (Bytes)
0	SF10	125 kHz	Uplink	980	11
1	SF9	125 kHz	Uplink	1,760	53
2	SF8	125 kHz	Uplink	3,125	125
3	SF7	125 kHz	Uplink	5,470	242
4	SF8	500 kHz	Uplink	12,500	242
5 – 7					
8	SF12	500 kHz	Downlink	980	53
9	SF11	500 kHz	Downlink	1,760	129
10	SF10	500 kHz	Downlink	3,125	242
11	SF9	500 kHz	Downlink	5,470	242
12	SF8	500 kHz	Downlink	12,500	242
13	SF8	500 kHz	Downlink	21,900	242

Step 1: Focus on the IP Space

Issues with the Web PKI

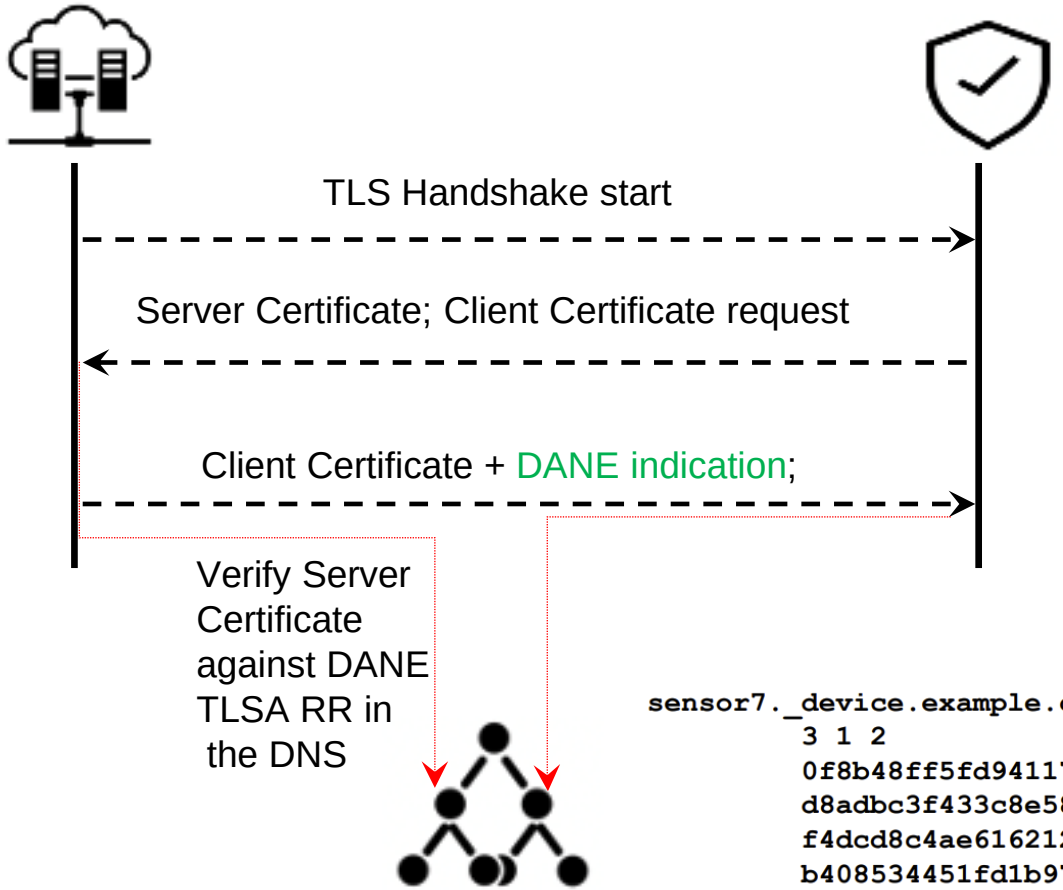
- CA bundle not available in most cases
- Web PKI CA adds Cost –> Possible Solution: *Self-Signed*
- Private PKI – Since the trust is based on a single Root CA

Currently – Trust is Siloed

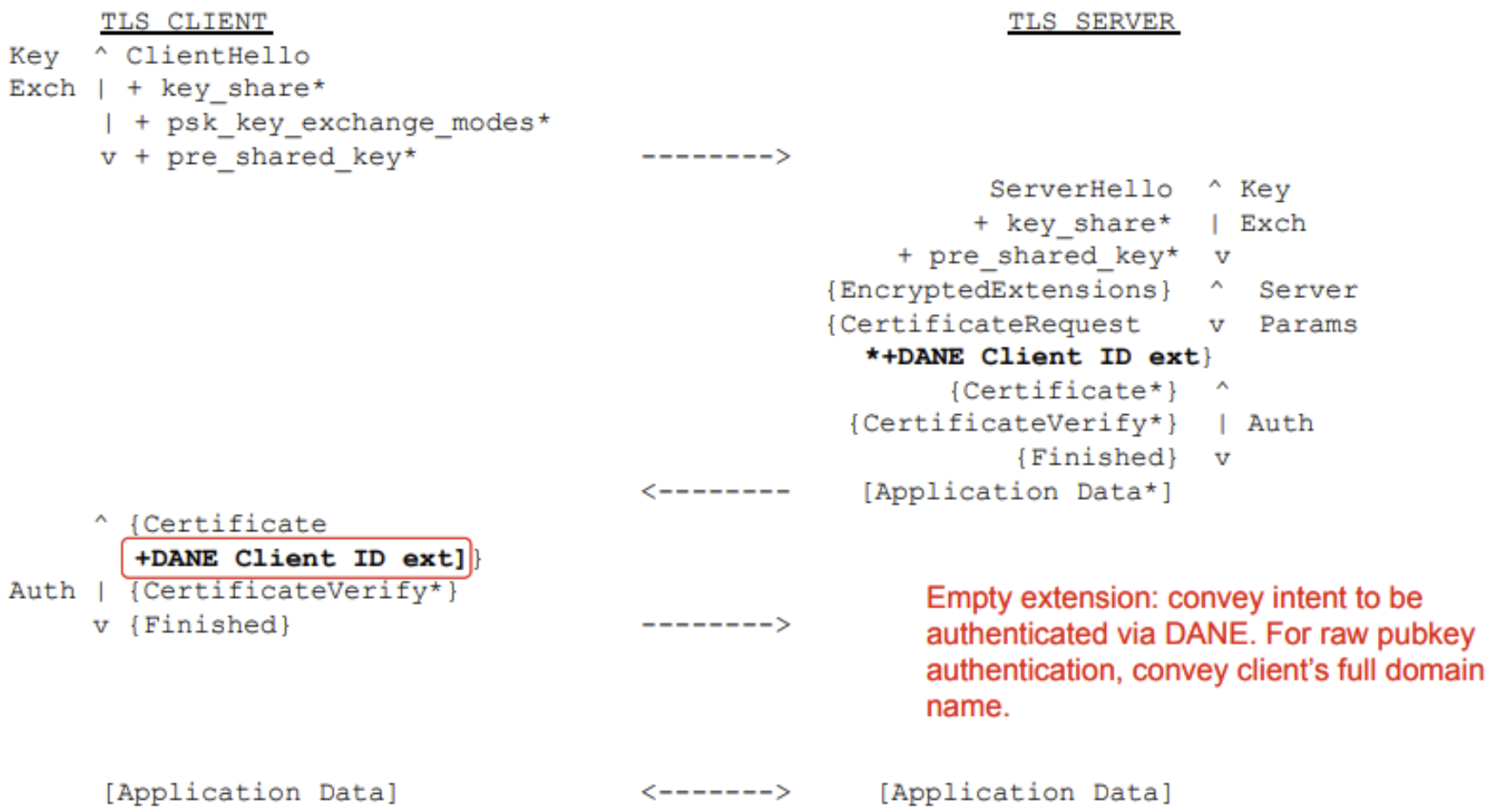


DANE Client authentication with TLS 1.2 & TLS 1.3

- *DANE Client ID has made it possible to mutually authenticate between different private PKI's*



DANE Client authentication with TLS



Empty extension: convey intent to be authenticated via DANE. For raw pubkey authentication, convey client's full domain name.

Drafts that we worked on

- draft-huque-tls-dane-clientid-06

- draft-huque-dane-client-cert-08

Dane-client-cert draft

- Existing Implementation
  - go library for DANE TLSA authentication (Author: Shumon Huque)

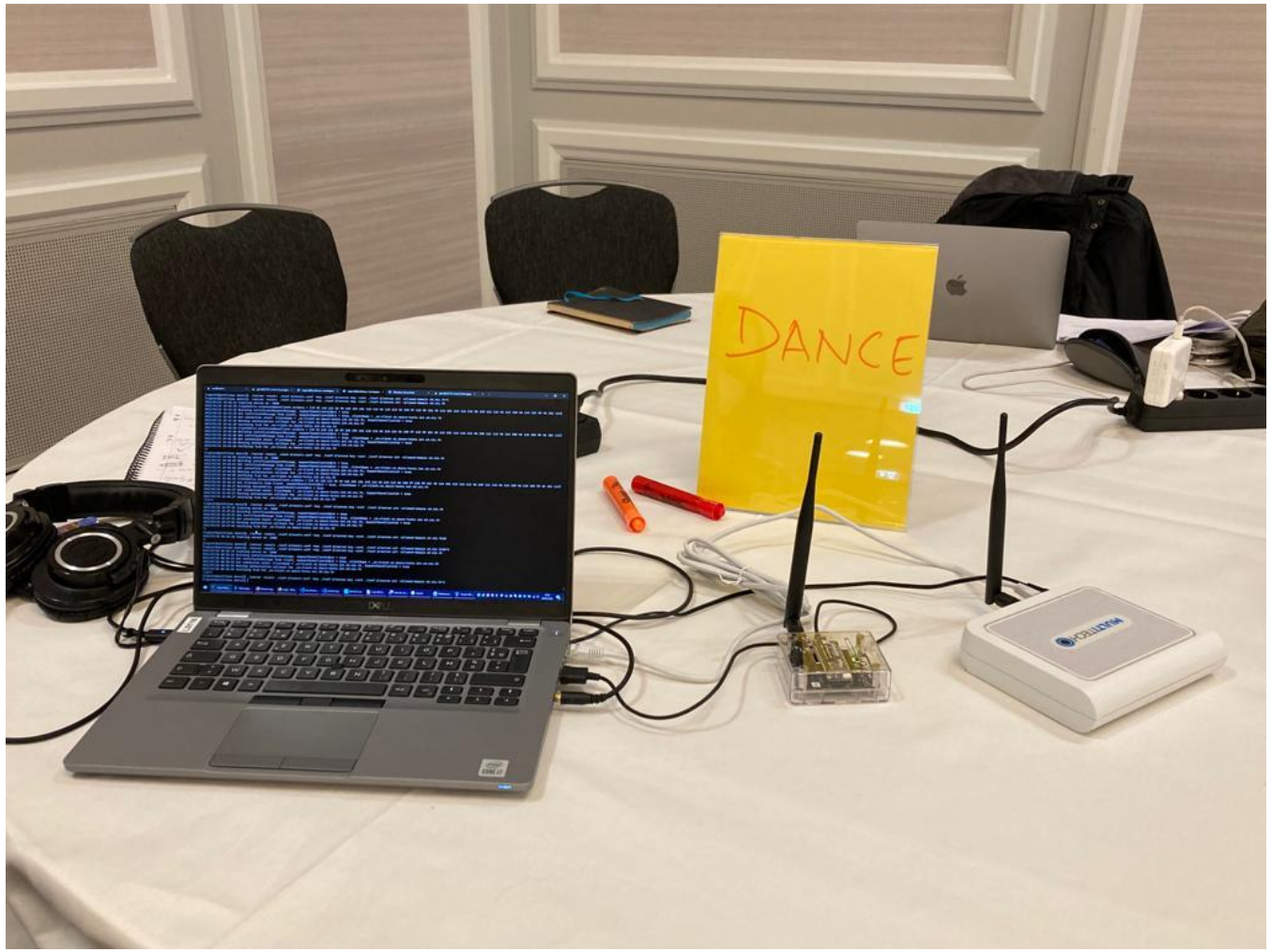
- What has been done during the IETF 113 Hackathon?
  - Environment for testing TLS Client/Server authentication
  - Authentication based on dane_clientid (Both for TLS 1.2 & TLS 1.3)
  - Fallback to authentication using SAN when dane_clientid is not sent
  - Possibility of whitelisting & authorization rules for which dane_clientid to accept

dane_clientid draft

- Extending TLS 1.2 & TLS 1.3 library to use the new value dane_clientid extension

- Adding the dane_clientid support for TLS 1.2 & TLS 1.3 handshake

Deploying the Updates in an IoT use-case - LoRaWAN



Step 2: Focus on extending asymmetric keys to the RF Space

Methods in discussion

- Further compression of Keys using SCHC
- Fragmentation of Keys
- Authenticated using a Certificate (Provided by reference)

Application

IoTRoam

- https://github.com/AFNIC/IoTRoam-Tutorial/blob/master/QuickStart.md

Pub for the Academia WG

Free for Institutional members

LoRa ALLIANCE® MEMBERSHIP LEVELS	ADOPTER $0K ($1K STARTUP)	CONTRIBUTOR $20K	SPONSOR $50K	INSTITUTIONAL FREE
LEADERSHIP				
Right to be nomintated for a Board Seat			✓	
Vote for Board of Director Seats			✓	
Chair of Committees, Working Groups, and Task Forces		✓	✓	
Represent the LoRa Alliance as a LoRaWAN Ambassador during events, webinars and interviews		✓	✓	
TECHNICAL				
Net ID allocation		✓	✓	
License additional Type 7 NetIDs	✓	✓	✓	
LoRaWAN Certification Test Tool	✓	✓	✓	✓
One LoRaWAN end-device certification	✓	✓	✓	✓
Regulatory support by region	✓	✓	✓	✓
MEMBER EXCLUSIVES				
Access to Member Portal for shared ecosystem information	✓	✓	✓	✓
Access to LoRa Alliance RFP & Tender Connect: project requests	✓	✓	✓	✓
System Integrator Education Spotlight	✓	✓	✓	✓
Training and deployment advice & assistance	✓	✓	✓	✓
COLLABORATION				
Attend & vote at Committee meetings		✓	✓	
Create new Working Groups or Task Forces		✓	✓	
Create user groups: commercial, operational, technical	✓	✓	✓	✓
Attend Working Group or Task Force meetings (in-person)		✓	✓	✓
Attend Working Group or Task Force meetings (teleconference)	✓	✓	✓	✓
Attend one Committee meeting as an observer	✓			
Participate in seminars and webinars	✓	✓	✓	✓
Attend member meeting networking events	✓	✓	✓	✓
Contribute to draft deliverables	✓	✓	✓	✓
MARKETING & PROMOTION				
Products featured in the LoRaWAN Showcase (online catalog) with link to member	✓	✓	✓	✓
Online public Member Directory	✓	✓	✓	✓
Digital promotion of member content and news	✓	✓	✓	✓
Exclusive use of "LoRa Alliance Member" and "LoRaWAN" logos and wordmarks	✓	✓	✓	✓
LoRa Alliance marketing & educational resources including leadership quotes for member PRs	✓	✓	✓	✓

Sandoche.balakrichenan@afnic.fr