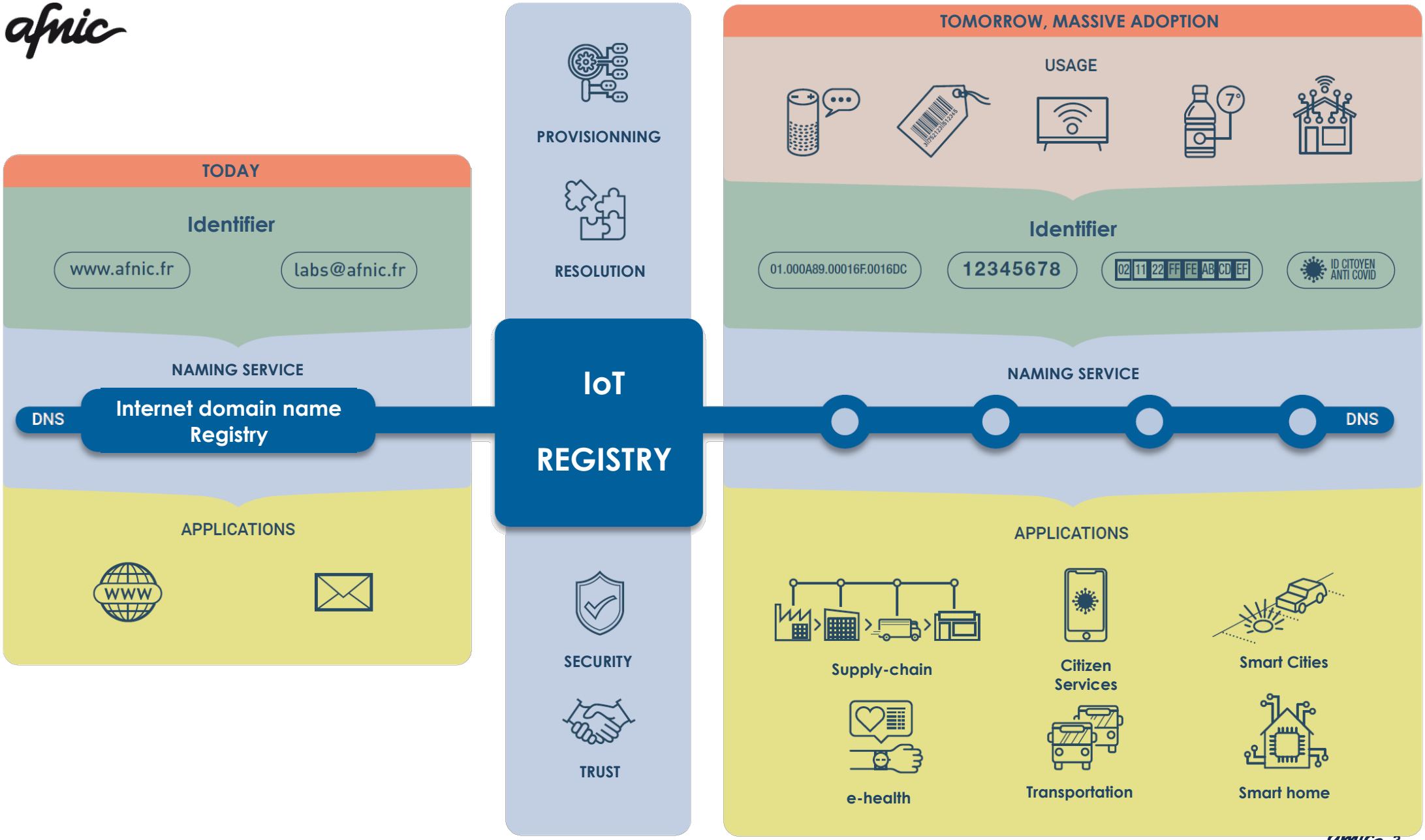
May 11th 2021

Extending DNS and its ecosystem for IoT

Sandoche BALAKRICHENAN



image: Freepik.com


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 Objective: IoT Registry

DONE

WINGS

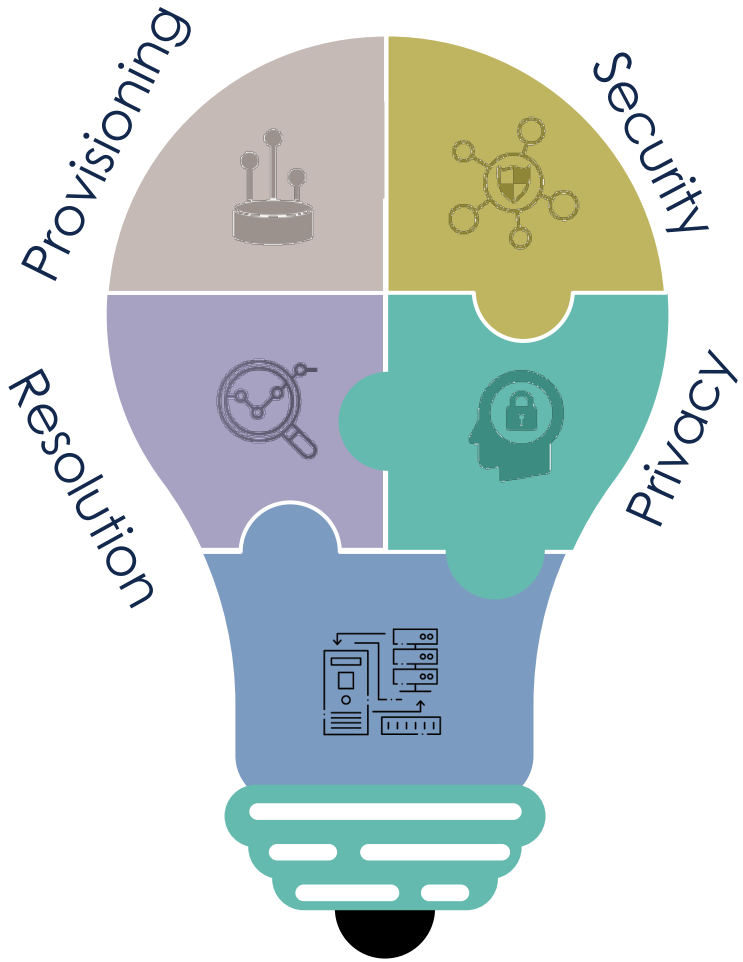
Widening interoperability for networking Global supply Chains

GS1 France · afnic · Inria · UPMC · GREYC · orange

PoC

LoRa Alliance®

DNS Service



ONGOING

DINS*

DNS Naming and Services for Secure Seamless IoT

Grenoble INP | UGA · Objenious · afnic · IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom · acklio

ONGOING

PIVOT*

Privacy-Integrated design and Validation in the constrained IoT

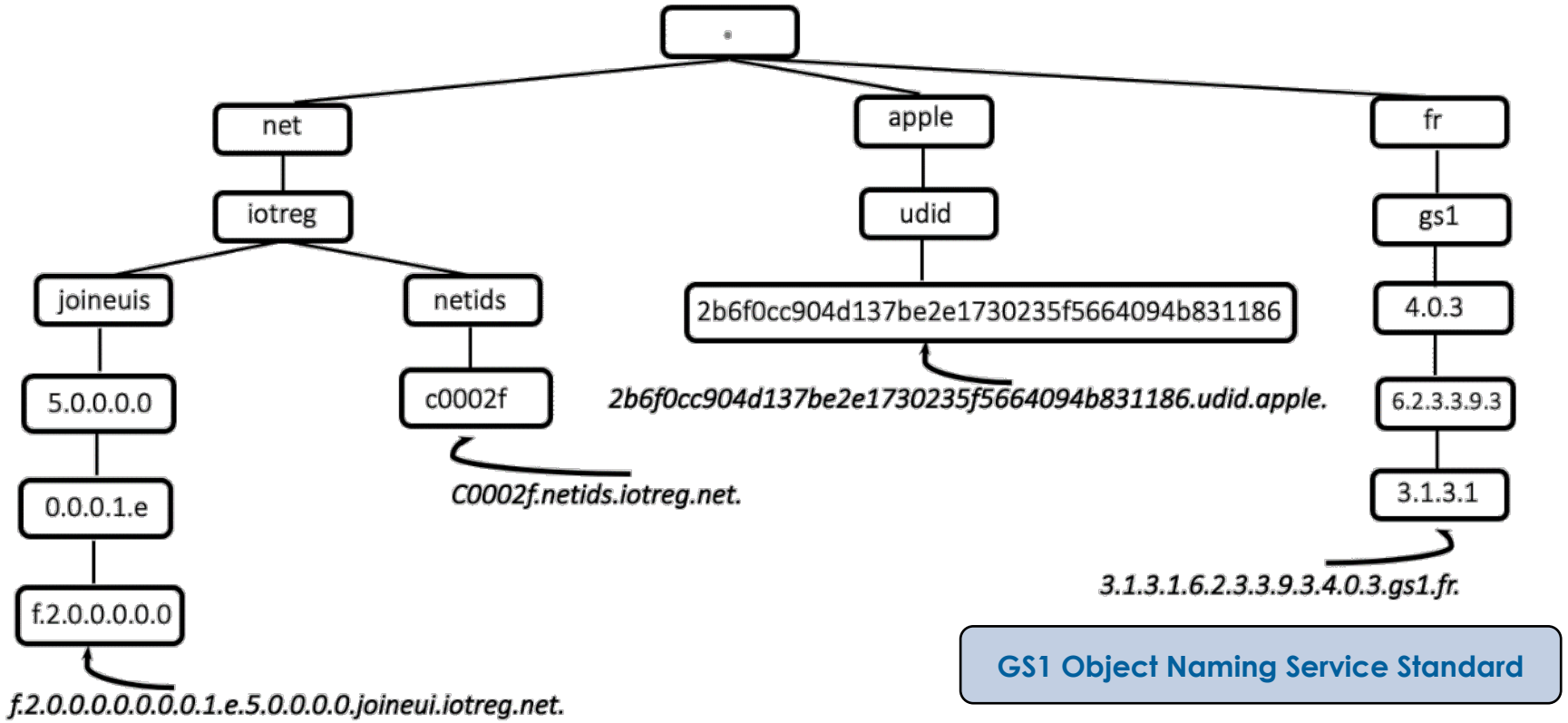
Freie Universität Berlin · Hochschule für Angewandte Wissenschaften Hamburg · Lobaro Industrial IoT Solutions · INSA Institut National des Sciences Appliquées Lyon · Inria · afnic

IoT Provisioning in the DNS



Frame photo created by jannoon028 - ww.freepik.com

It's about converting IoT naming conventions into DNS RR's



LoRaWAN Backend Interfaces specification

GS1 Object Naming Service Standard

We all 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
```

DNS Camel



Example of standards using DNS for IoT Provisioning & Resolution

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

Labs contributions

DNS for leveraging IoT protocols and infrastructures

- ONS : Standard
- LoRaWAN : Protocol
- IoTRoam : Open architecture
- Research Papers / PhD



Designed by katemangostar / Freepik

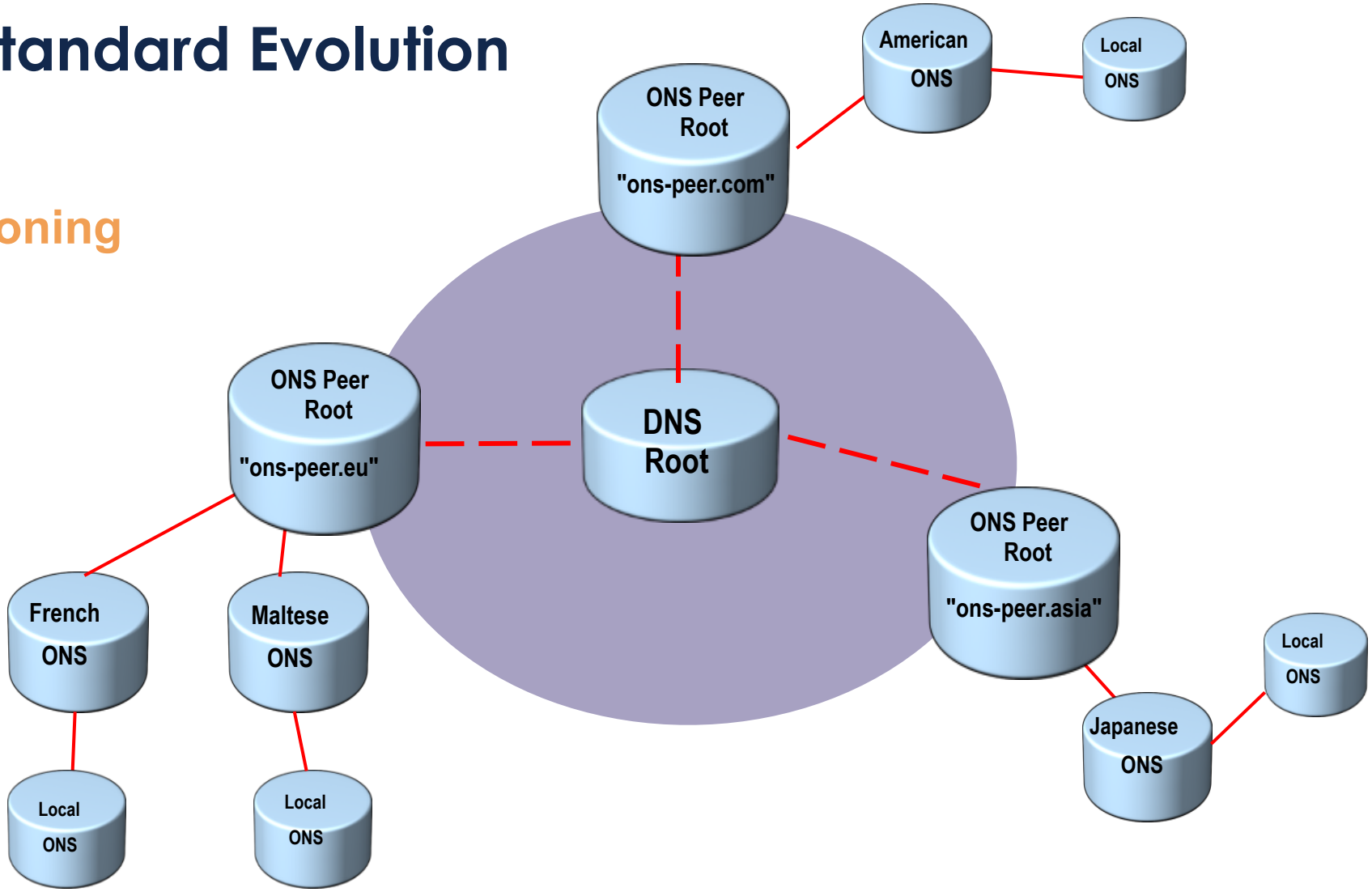
ONS

Contribution



ONS Standard Evolution

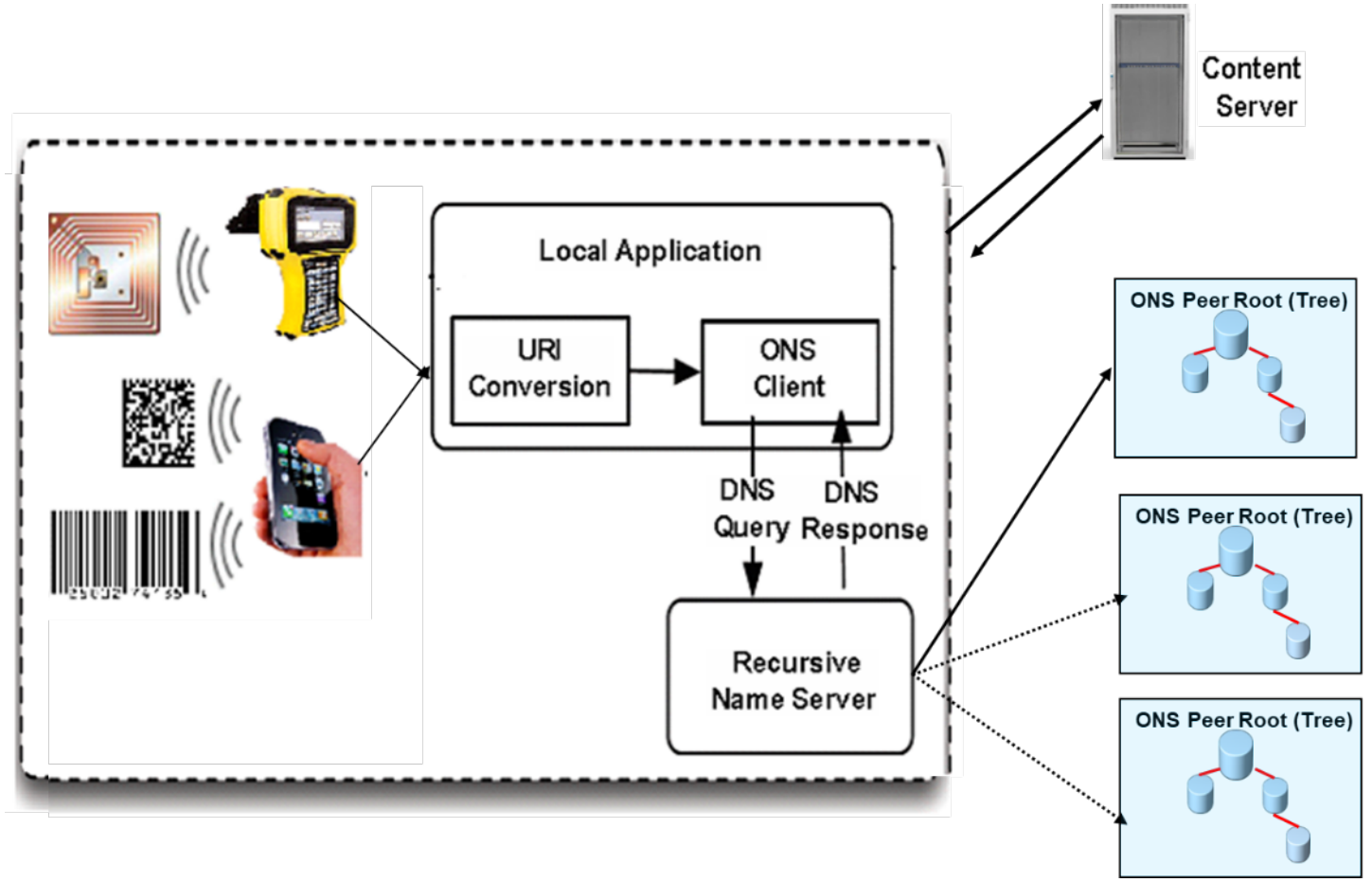
Provisioning



ONS Standard Evolution

Resolution





LoRaWAN

Low Power, Wide Area (LPWA) networking protocol

Non-IP IoT Technology

We were/are not Radio experts

We were/are not Electronics/IoT devices experts

We know (a bit) about software

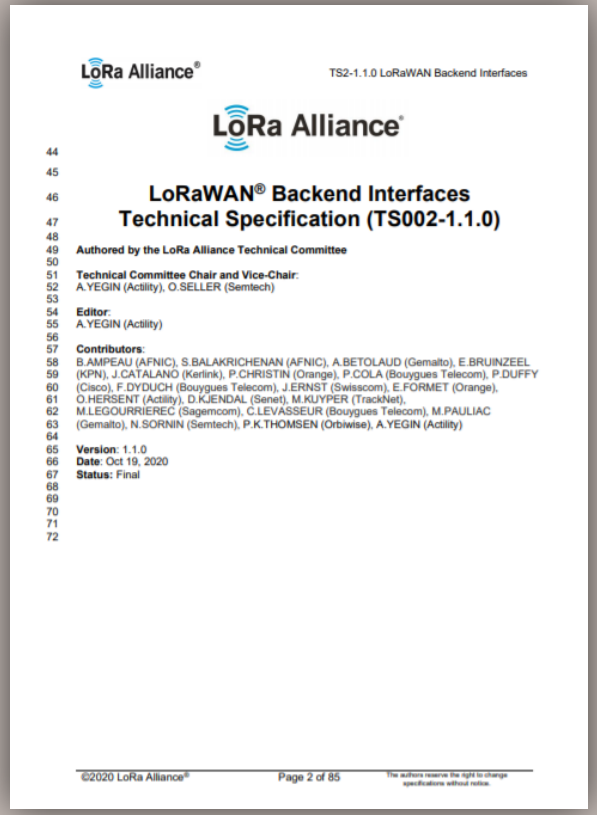
We know about security

We know about provisioning

We know about trust

We know about Interoperability…cause we know Internet

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)

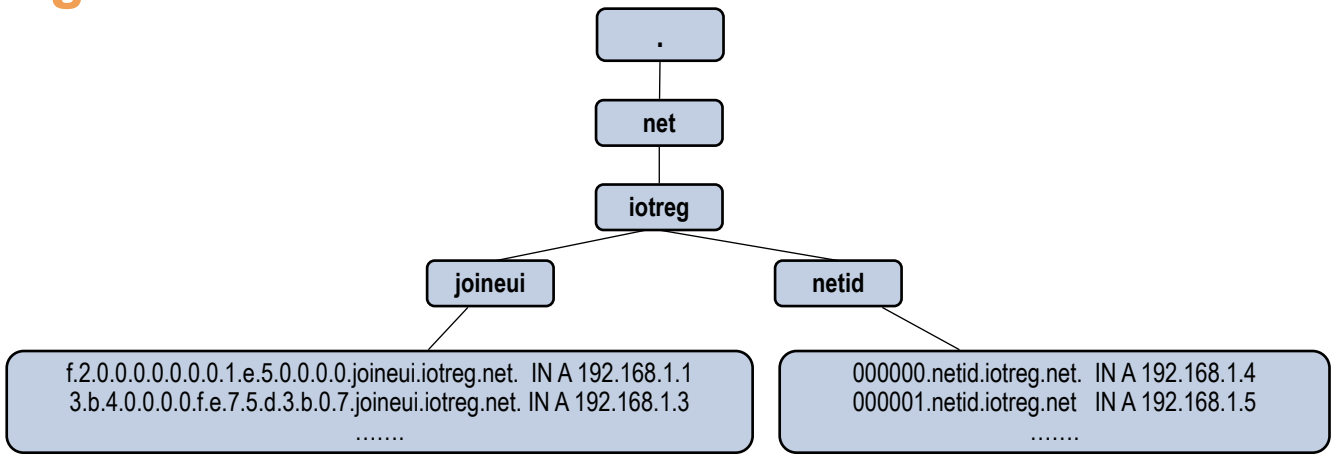
Contributors:
B.AMPEAU (AFNIC), S.BALAKRICHENAN (AFNIC), A.BETOLAUD (Gemalto), E.BRUINZEEL (KPN), J.CATALANO (Kerlink), P.CHRISTIN (Orange), P.COLA (Bouygues Telecom), P.DUFFY (Cisco), F.DYDUCH (Bouygues Telecom), J.ERNST (Swisscom), E.FORMET (Orange), O.HERSENT (Actility), D.KJENDAL (Senet), M.KUYPER (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

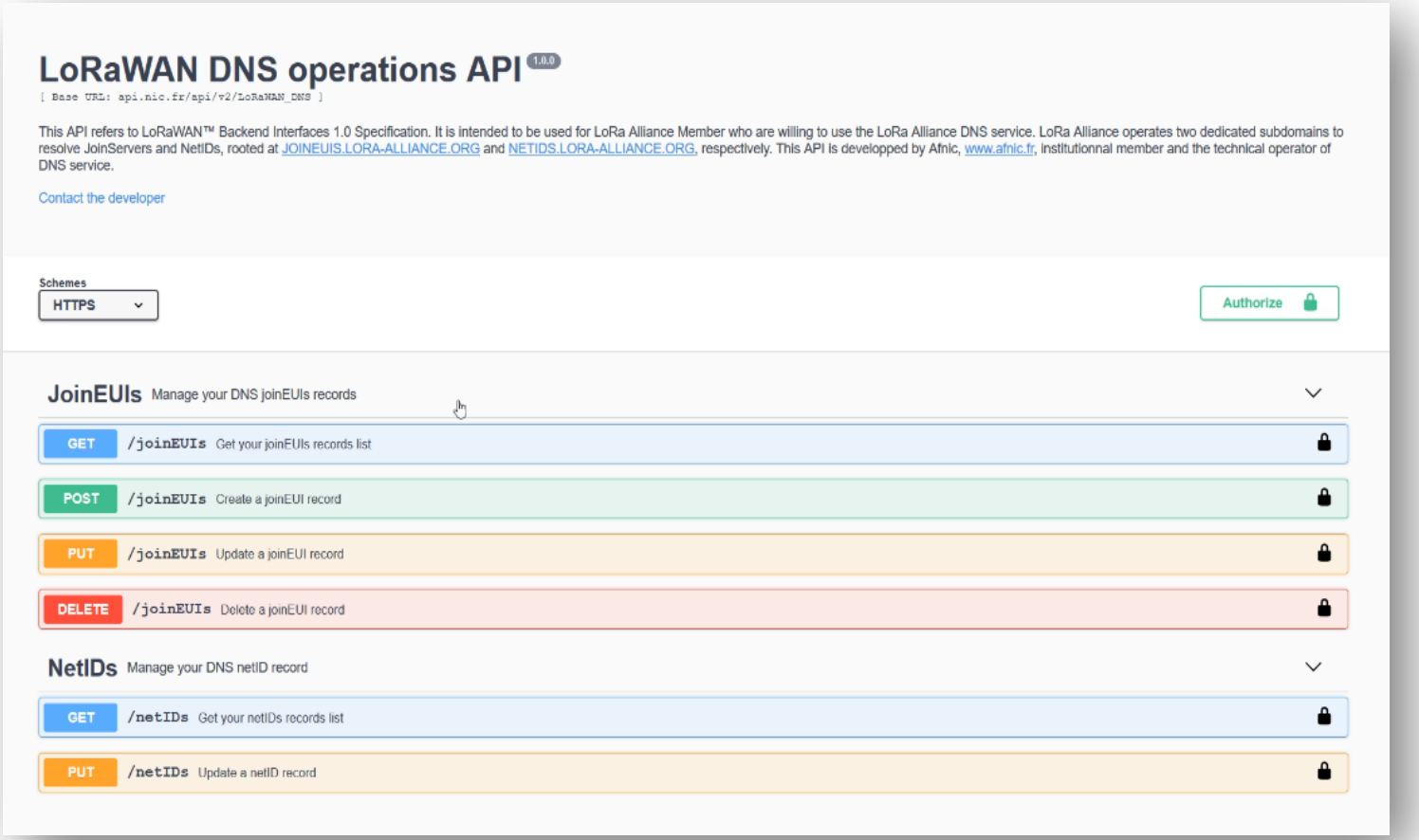
©2020 LoRa Alliance® Page 2 of 85 The authors reserve the right to change specifications without notice.

LoRaWAN Backend Specifications

Provisioning

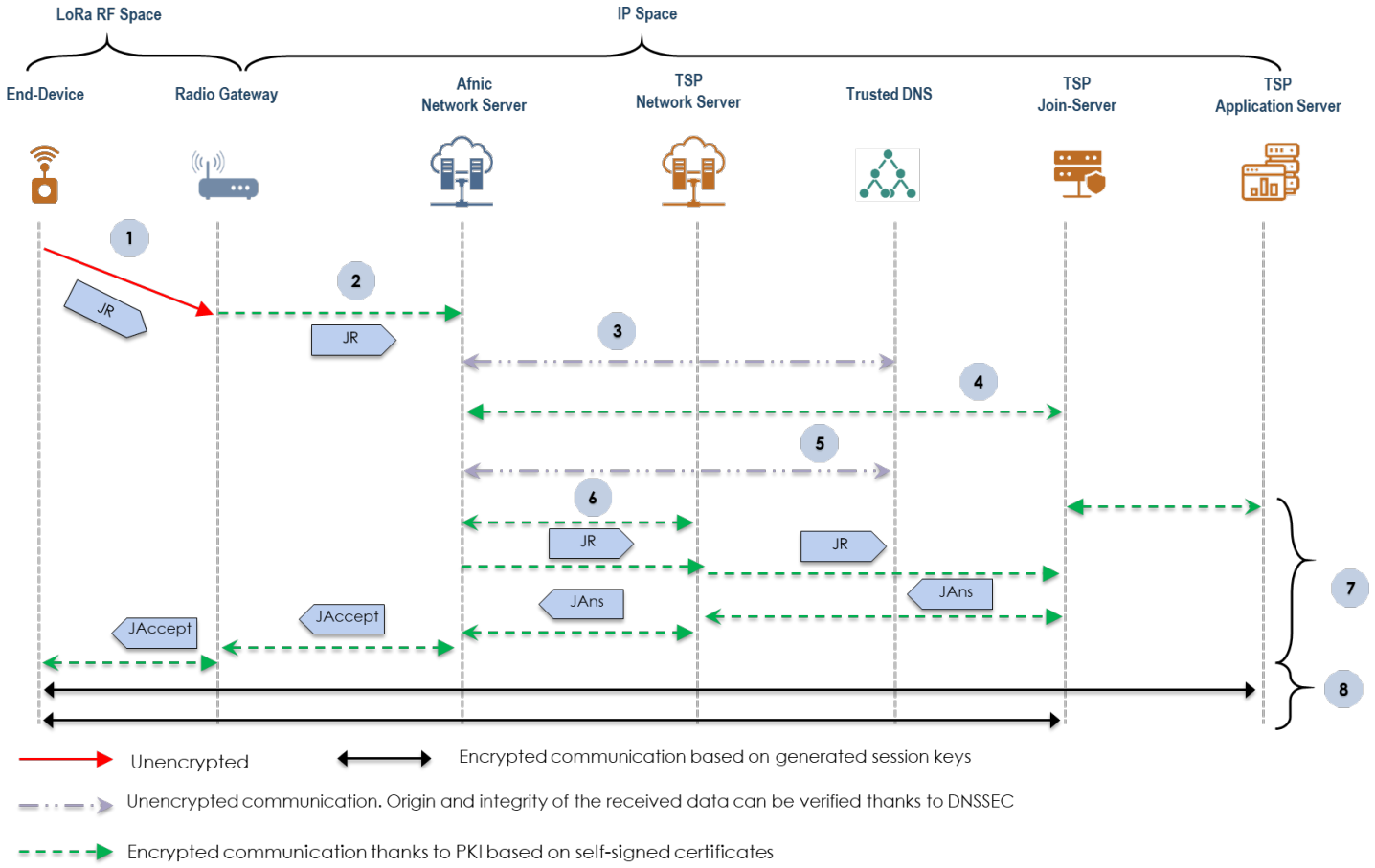


Dedicated LoRaWAN DNS Service



LoRaWAN Backend Specifications

Resolution

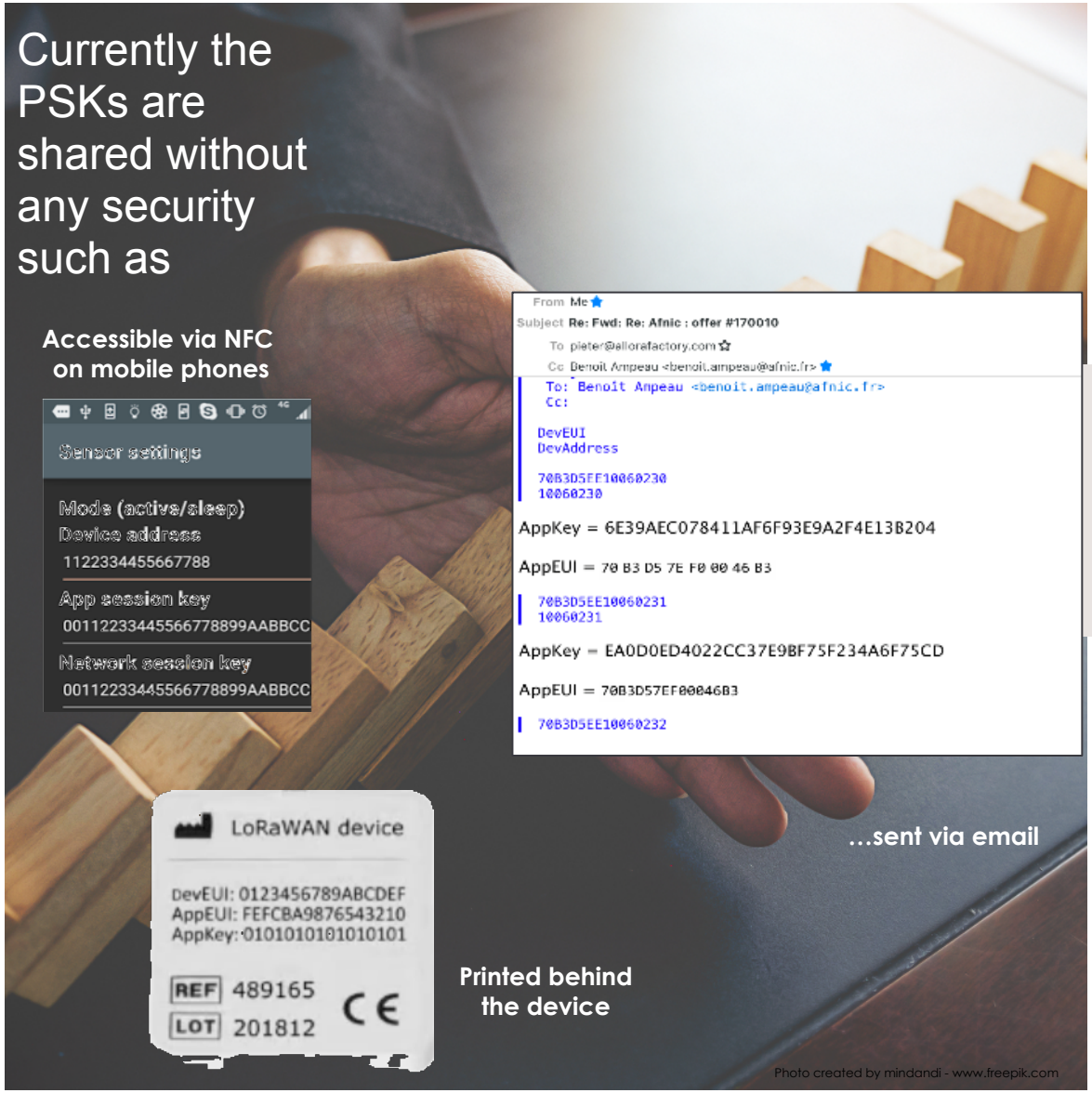


Problem statement

Adding Security using DNS infrastructure for Key Sharing

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

Sharing the PSKs is an operational nightmare



Adding Security using DNS infrastructure

- Using Internet Style CA based solutions
- Issues in using CA certificates – Cost/Size
- For Cost – Self Signed Certificates
- For Size – ECDH, New IETF Standards (e.g: LAKE)

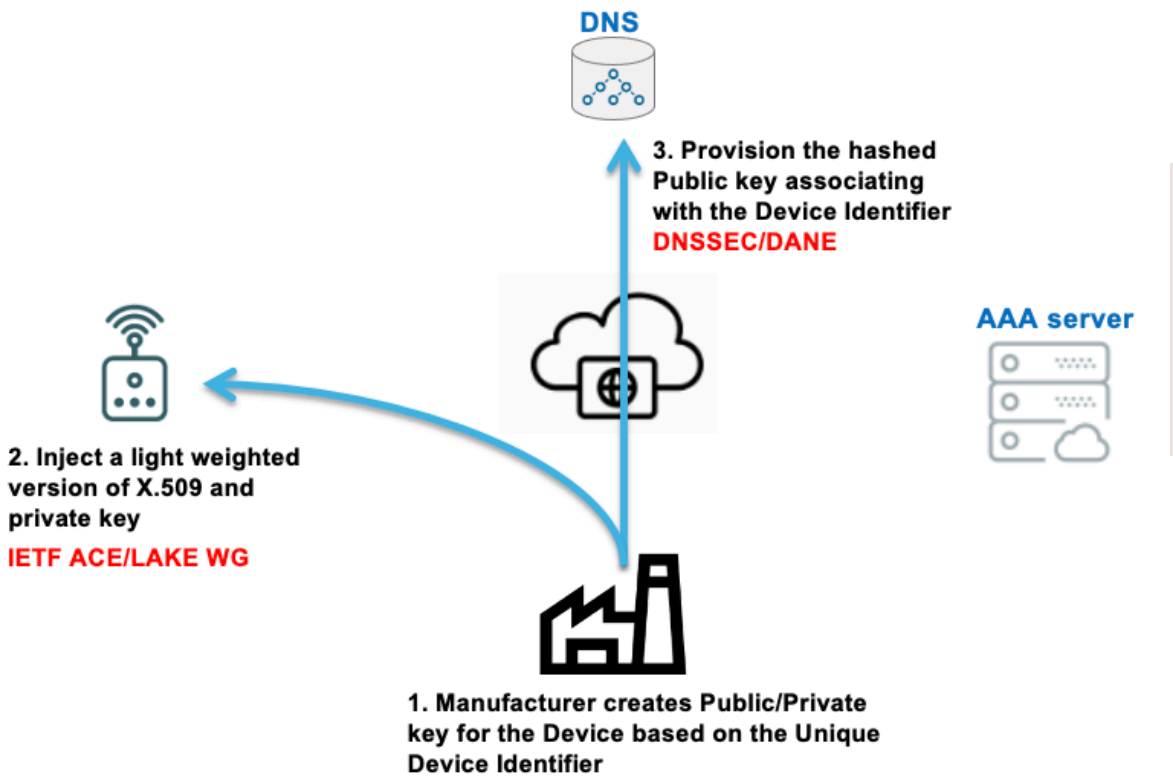


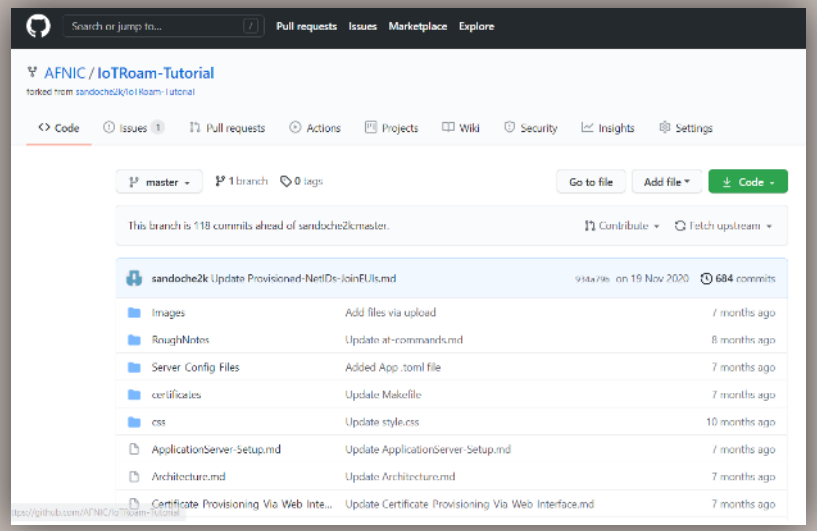
Adding Security using DNS infrastructure

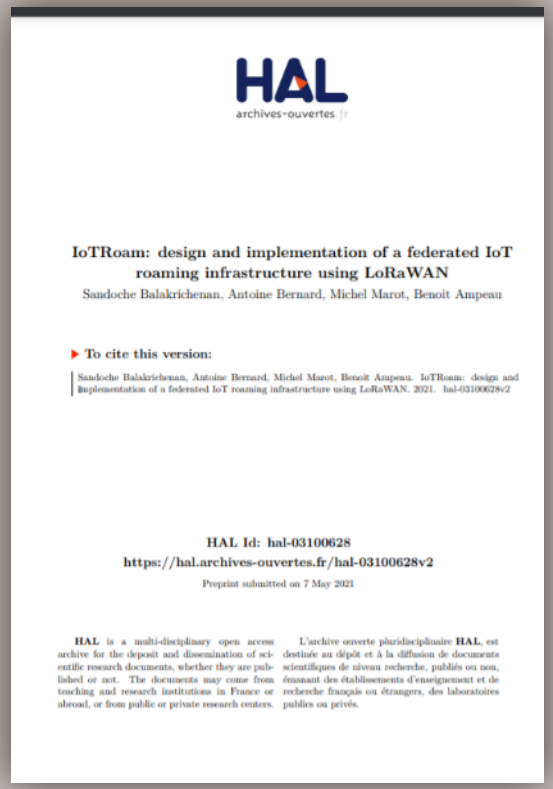
Solution

DNSSEC

DANE (yes we have a new use-case for DANE !)







HAL
archives-ouvertes.fr

IoTRoam: design and implementation of a federated IoT roaming infrastructure using LoRaWAN

Sandoche Balakrichenan, Antoine Bernard, Michel Marot, Benoit Ampeau

To cite this version:

Sandoche Balakrichenan, Antoine Bernard, Michel Marot, Benoit Ampeau. IoTRoam: design and implementation of a federated IoT roaming infrastructure using LoRaWAN. 2021. hal-03100628v2

HAL Id: hal-03100628
https://hal.archives-ouvertes.fr/hal-03100628v2

Preprint submitted on 7 May 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

IoTRoam

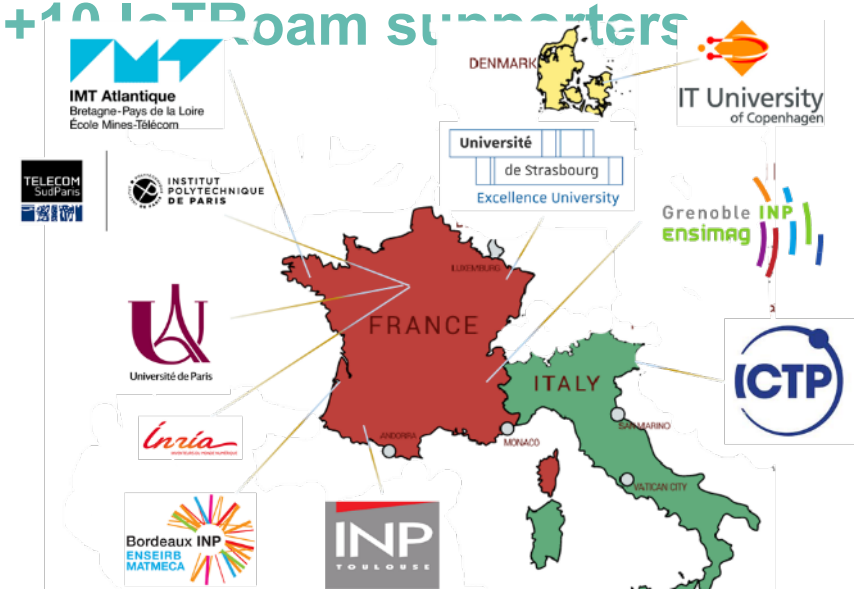
A Federated IoT roaming infrastructure using LoRaWAN

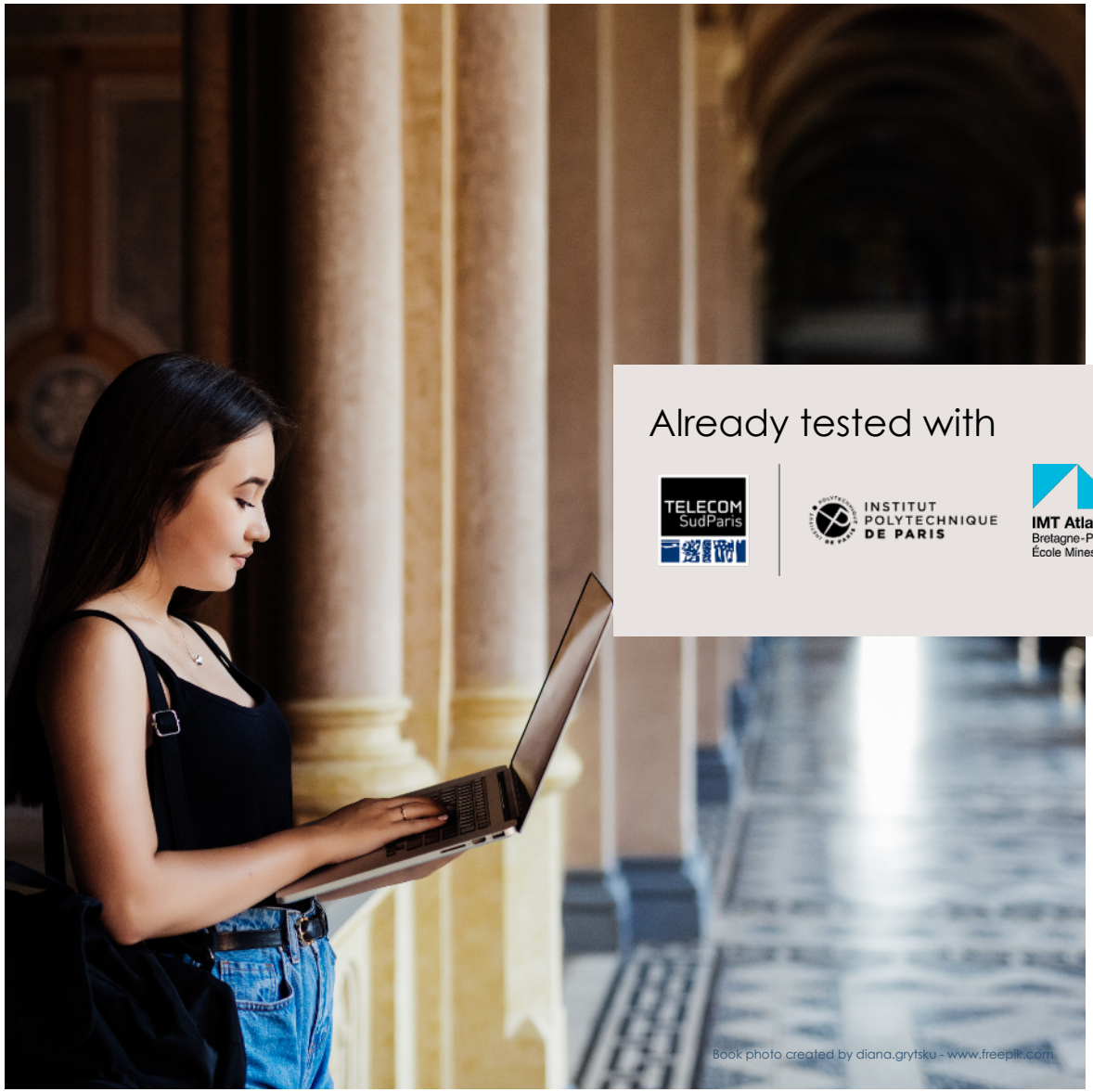
IoTRoam

A Federated IoT roaming infrastructure using LoRaWAN

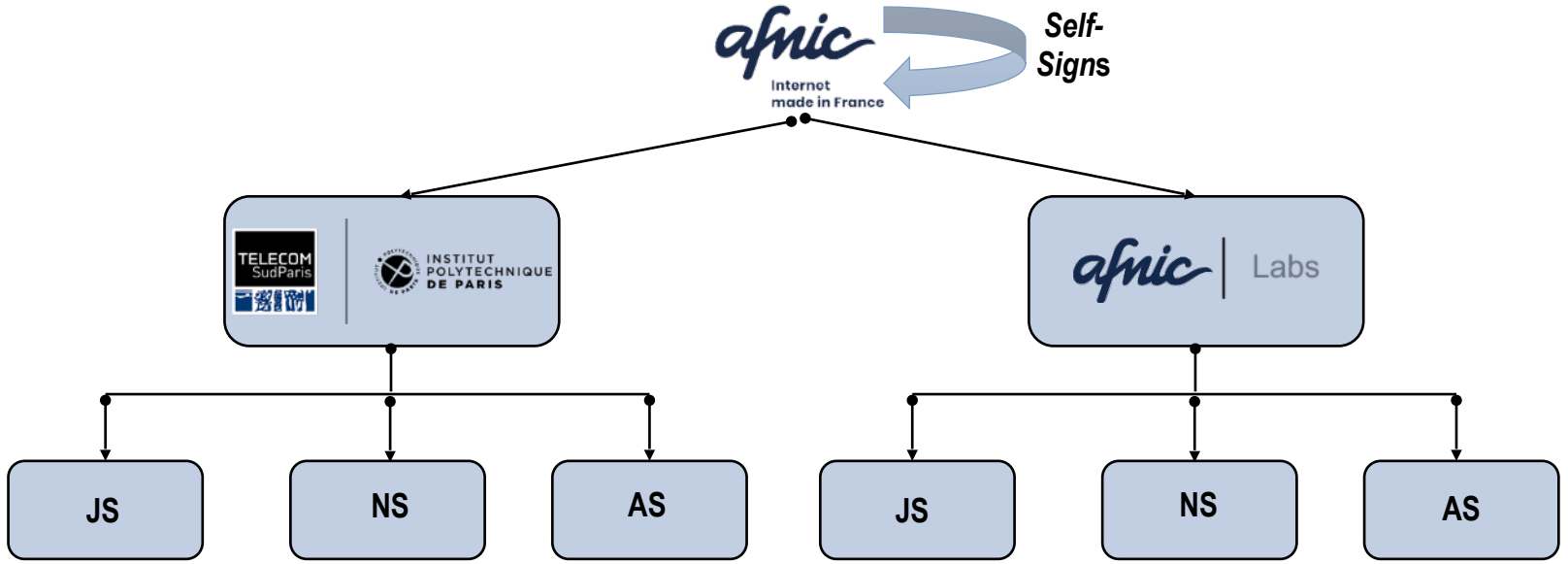
USE-CASE eduroam

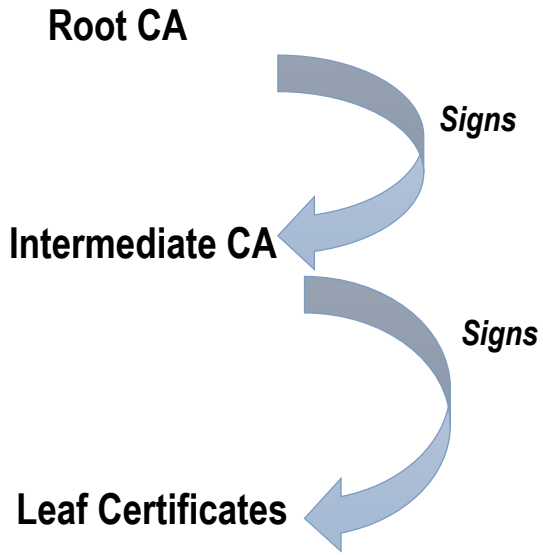
+10 IoTRoam supporters



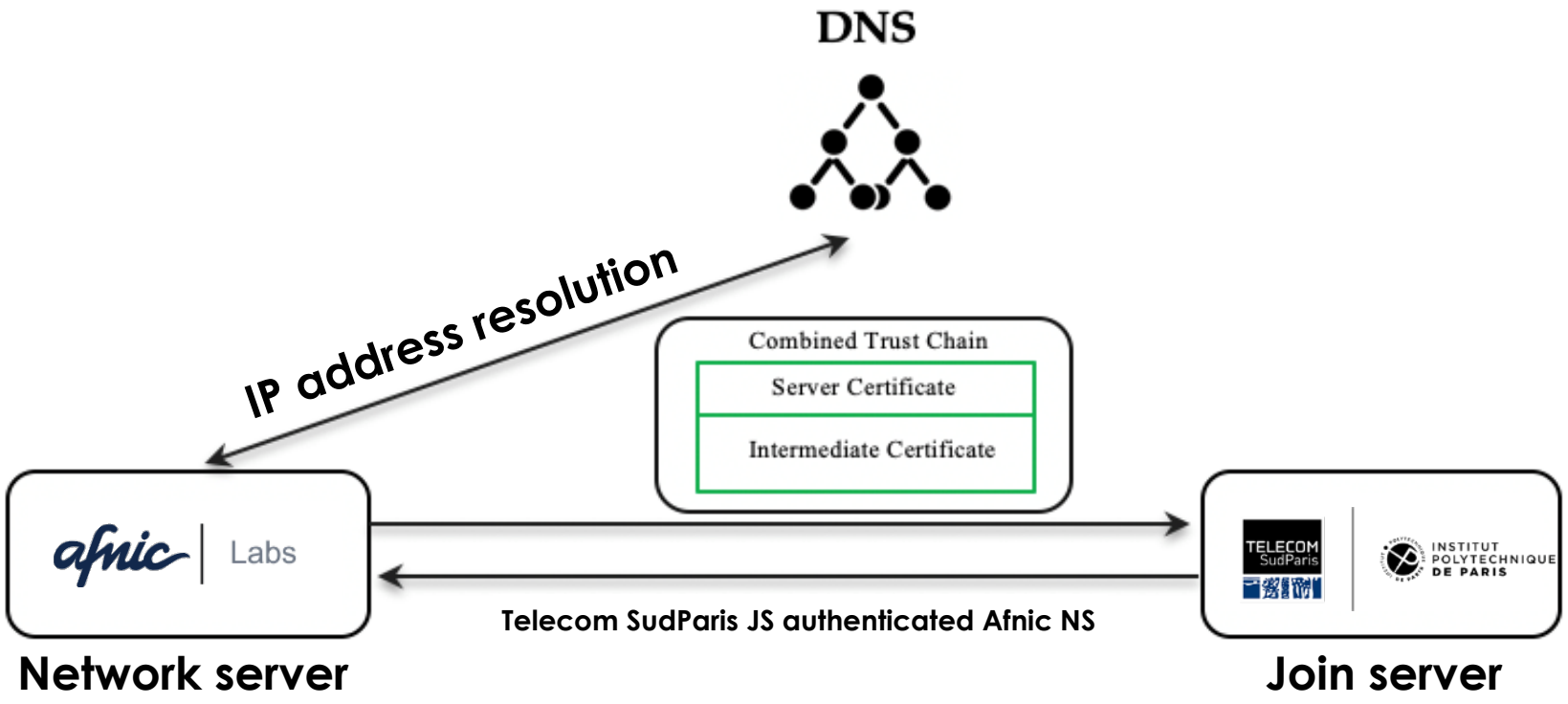


IoTRoam – Certificate Provisioning



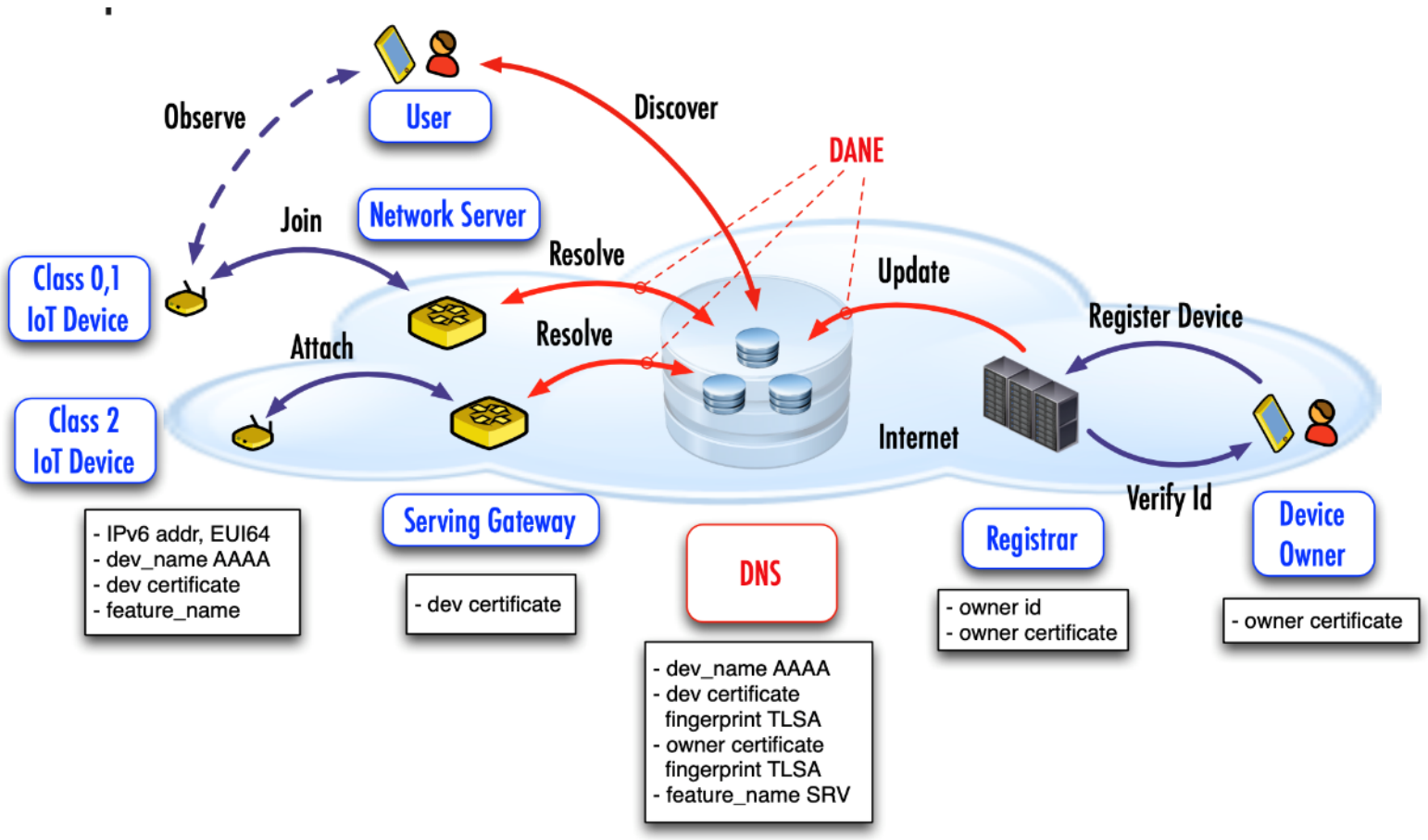


IoTRoam – Certificate Validation



Collaborative research projects

DiNS Project



PIVOT – French German collaboration

- Privacy by design – Object Security

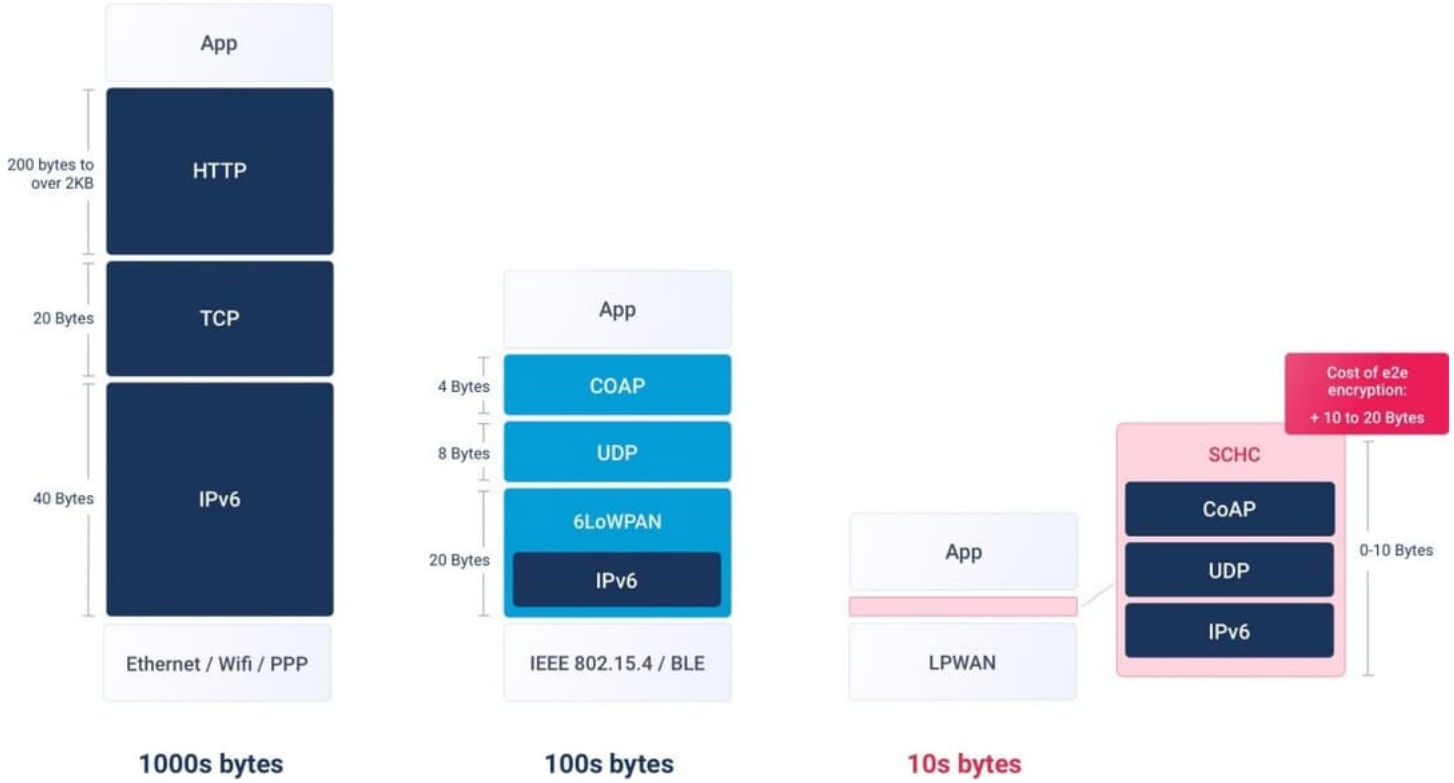
- Multi-stakeholder name management that preserves privacy requirements and generates, allocates, and resolves IoT names globally—regardless of the IoT applications or networks.

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

Papers and related works in progress

Using DNS for ‘Rules’ provisioning in extending IPv6 to IoT

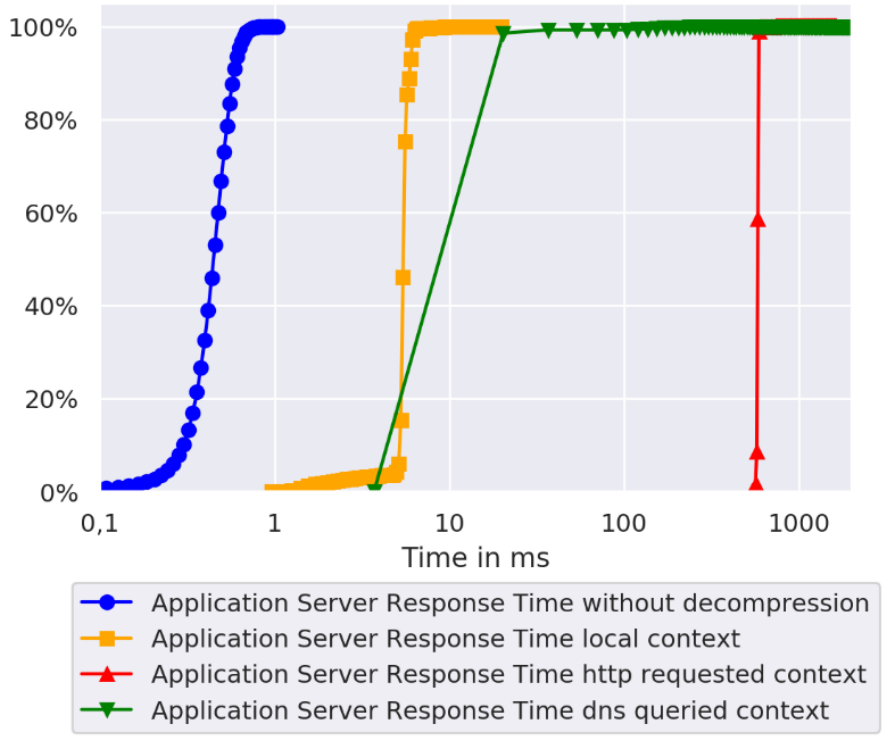
SCHC (RFC 8724)



Source: https://www.ackl.io/technology/schc

Using DNS for Rule resolution – SCHC

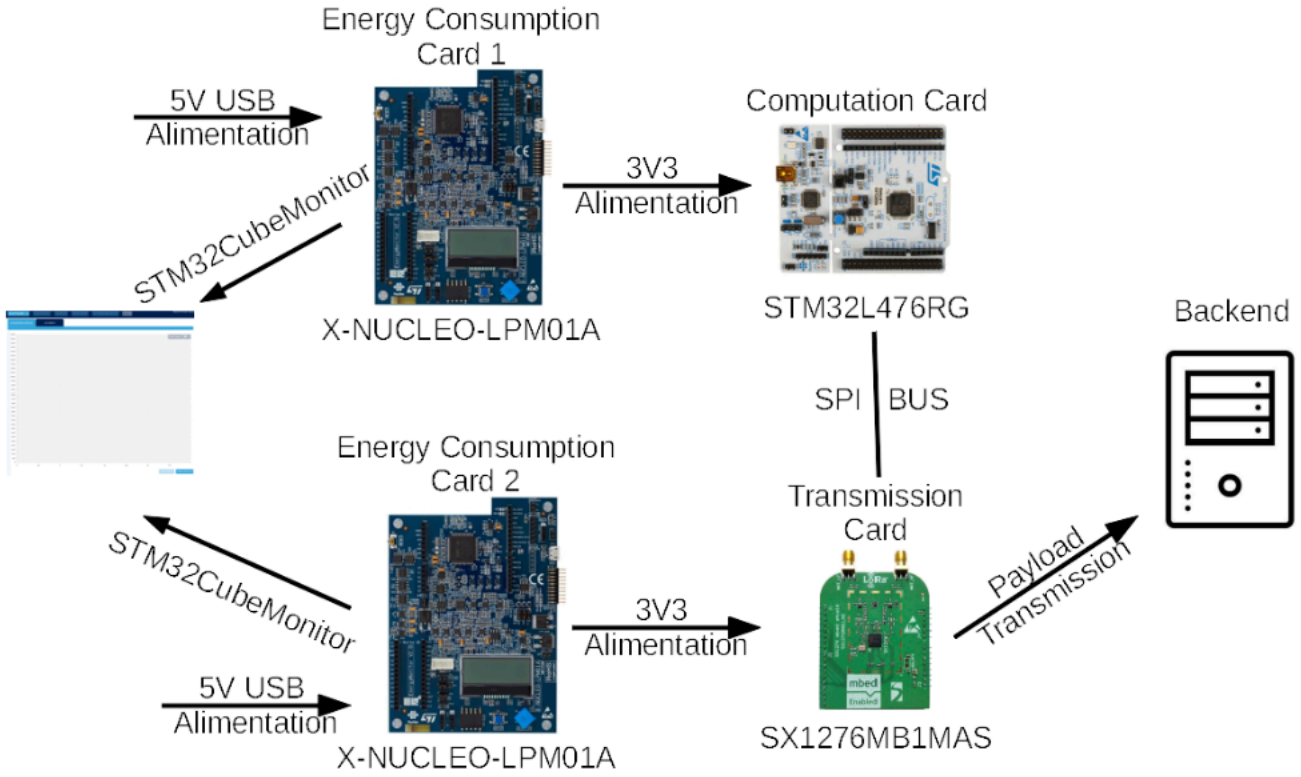
DNS-based dynamic context resolution for SCHC
ICC 2020 - 2020 IEEE International Conference on Communications (ICC)
https://doi.org/10.1109/ICC40277.2020.9148910



- **Adding SCHC increase packet processing time up to 8ms**
- **Using DNS to query the context would take up to 20ms**
- **HTTP requests are much slower (around 750ms)**

Provisioning LSTM Models in DNS

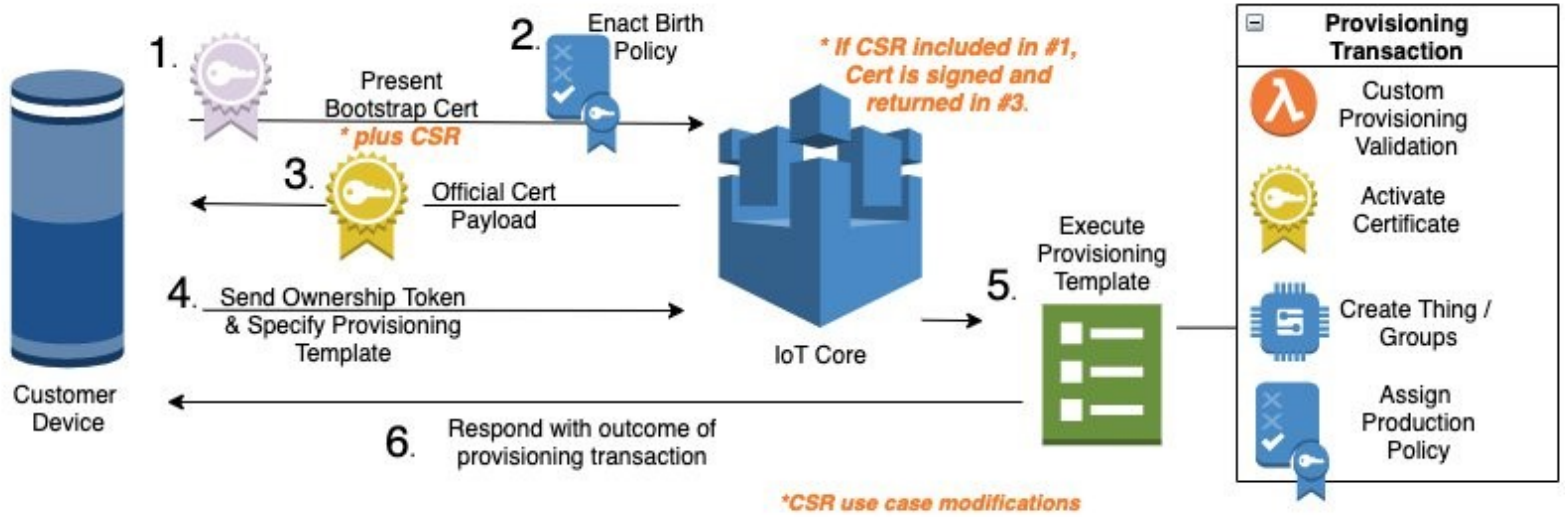
***Embedding ML Algorithms onto LPWAN Sensors for Compressed Communications* – Submitted to PIMRC 2021**



- **DNS experimentation in progress**

IoT Onboarding to AWS IoT Core

A centralization example

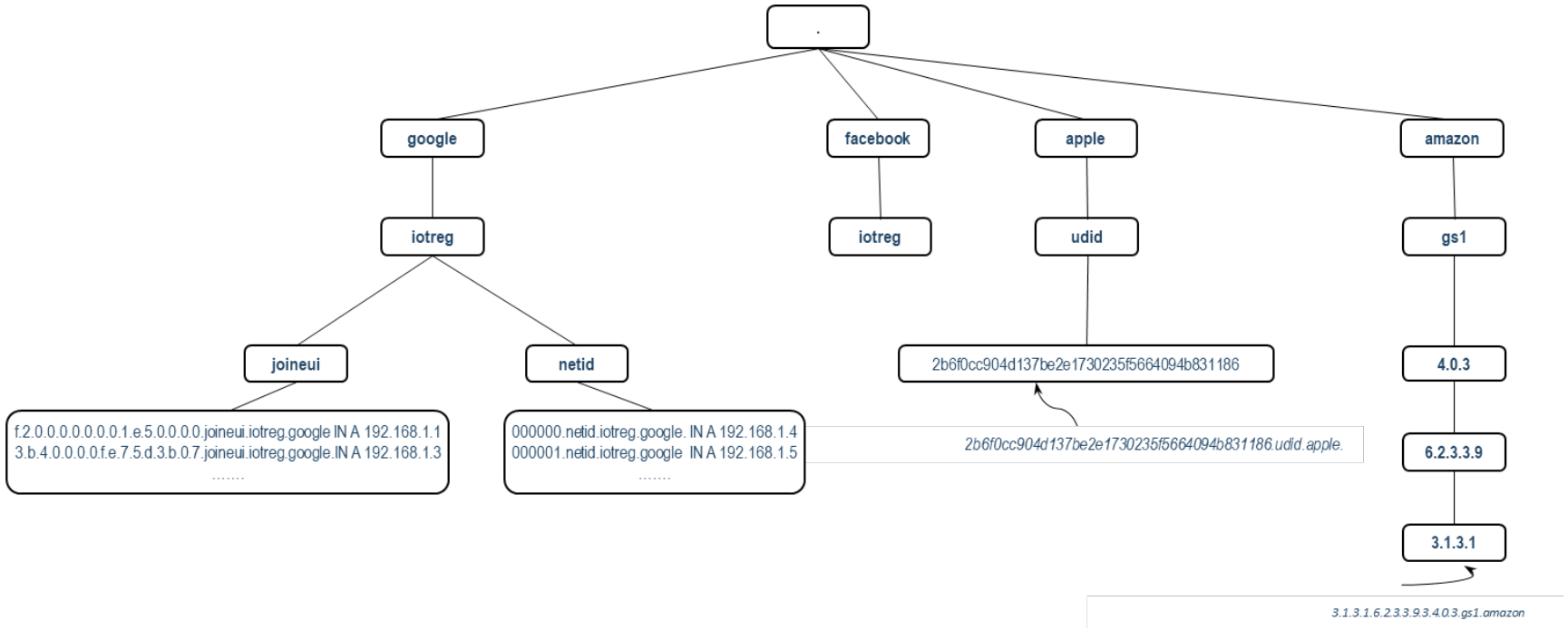


Source: Amazon

It's already packaged by big players

☹

The Future Scenario ?



Massive IoT is here

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

Conclusion

Could we do something as a group?



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

Merci !

Contact us !

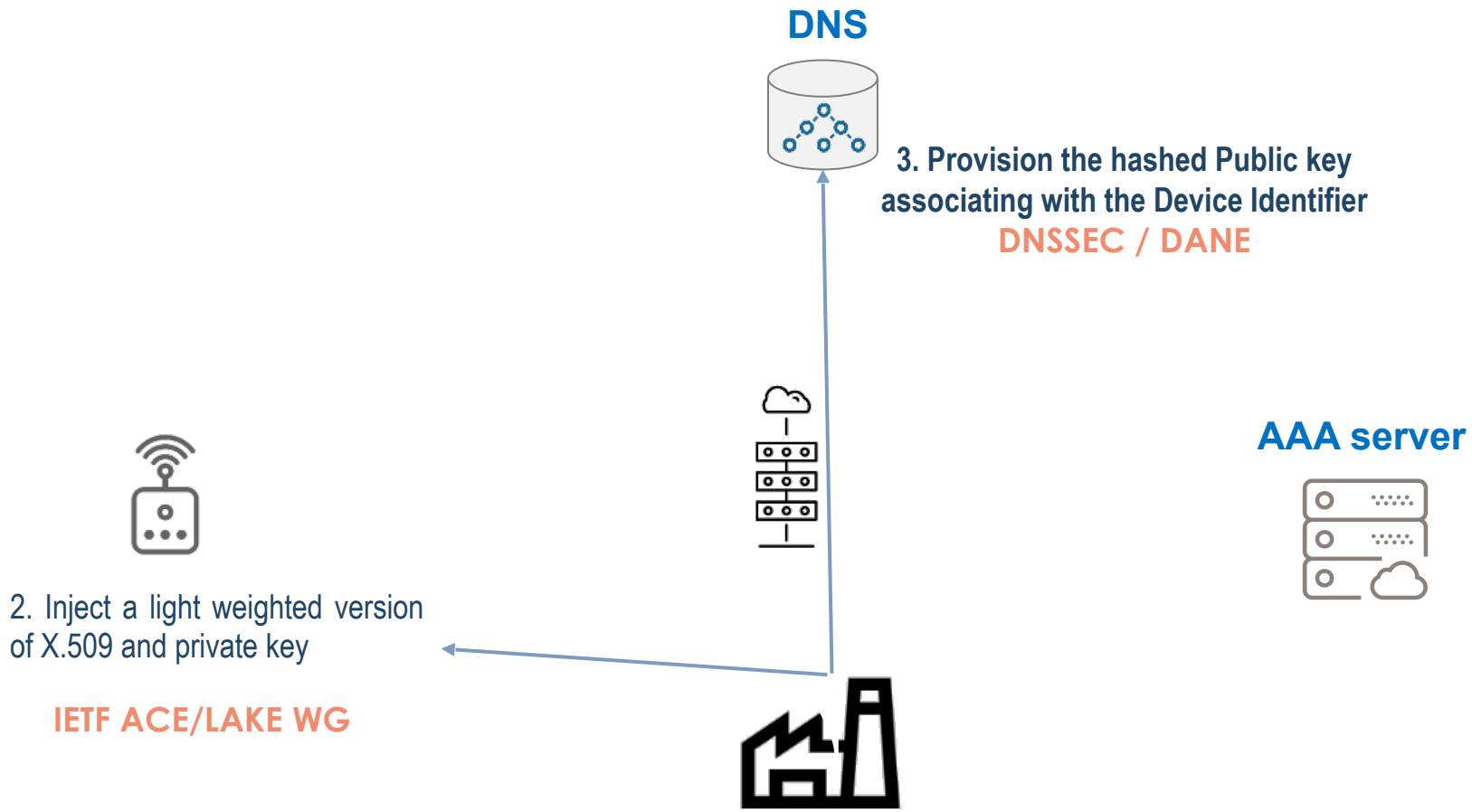
sandoche.balakrichenan@afnic.fr
benoit.ampeau@afnic.fr

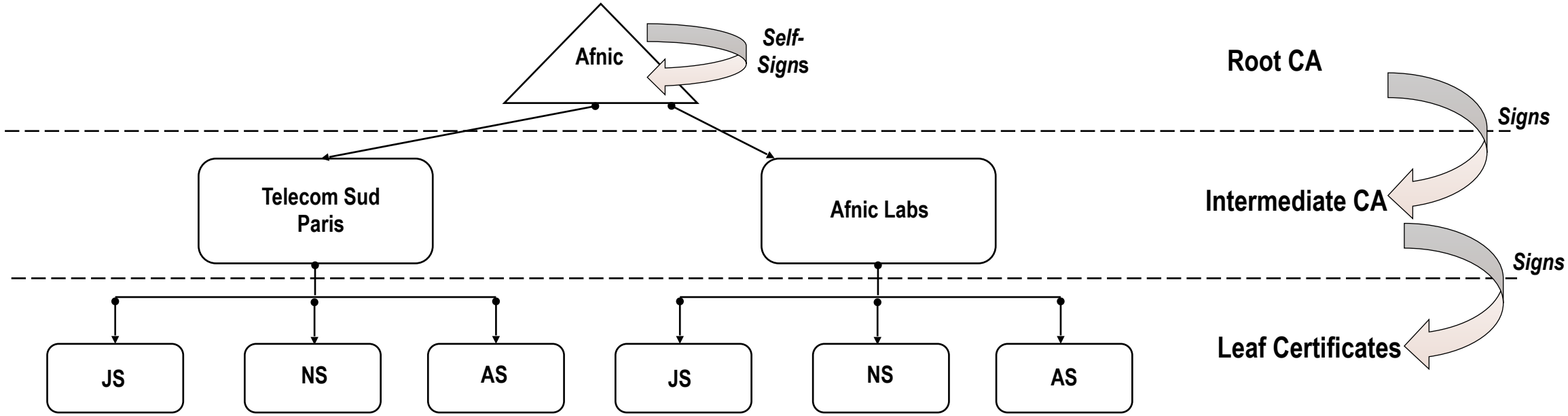
Internet made in France

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

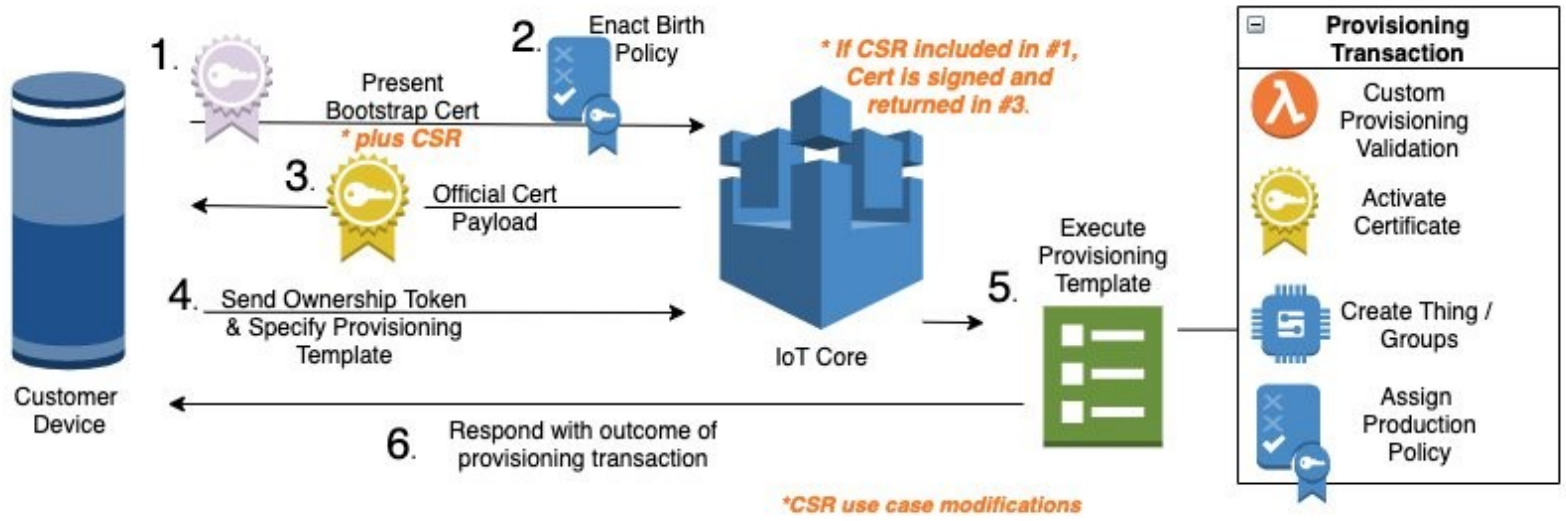
Backup / sources

Vision – Using DNS infrastructure as the PKI for IoT




Afnic
Self-
Signs
Root CA
Signs
Telecom Sud
Paris
Afnic Labs
Intermediate CA
Signs
JS
NS
AS
JS
NS
AS
Leaf Certificates

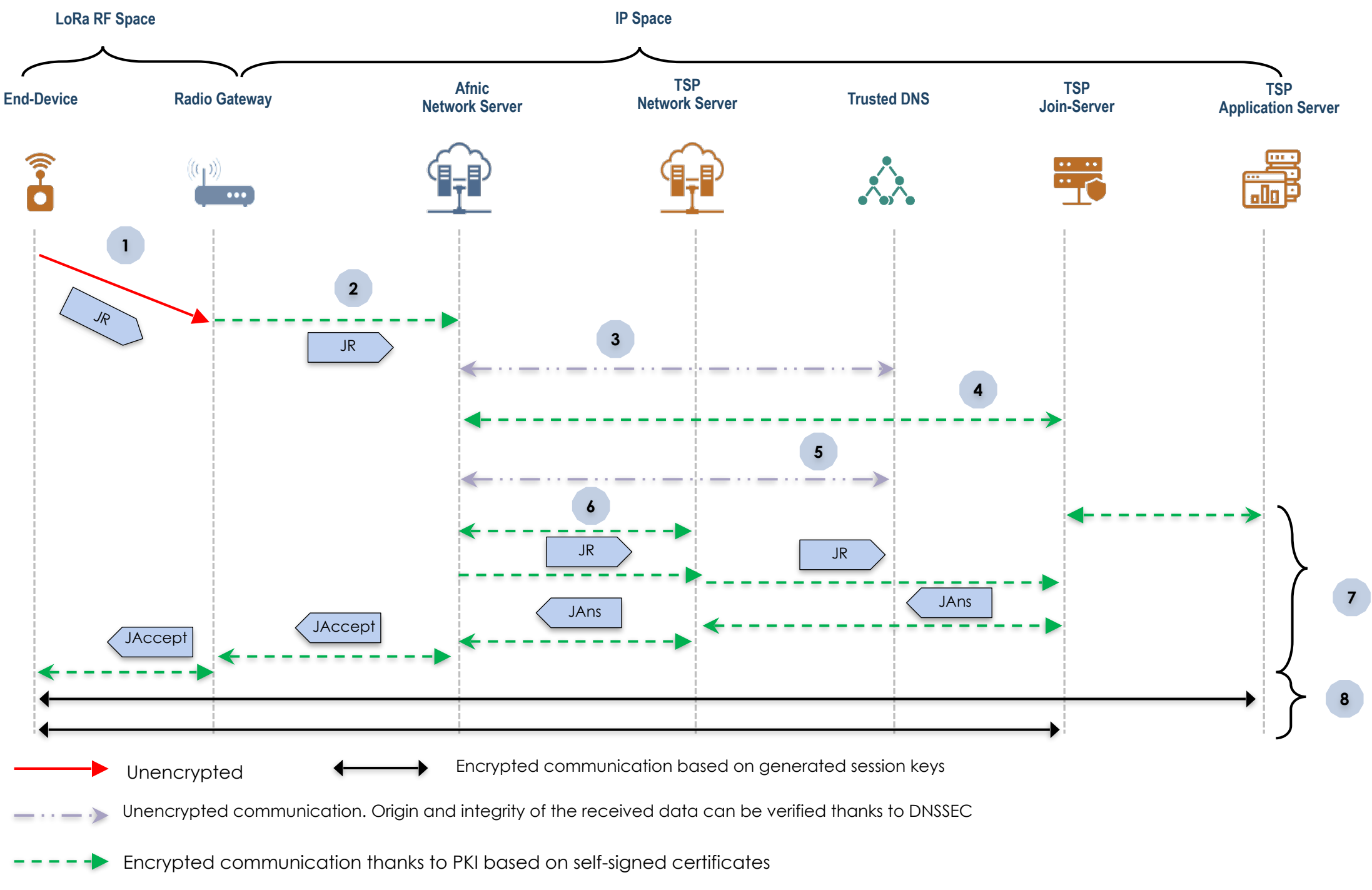
IoT Onboarding to AWS IoT Core



Source: Amazon

DNS Camel




LoRa RF Space
IP Space
End-Device
Radio Gateway
Afnic
Network Server
TSP
Network Server
Trusted DNS
TSP
Join-Server
TSP
Application Server
1
2
3
4
5
6
7
8
JR
JR
JR
JR
JAns
JAns
JAccept
JAccept
Unencrypted
Encrypted communication based on generated session keys
Unencrypted communication. Origin and integrity of the received data can be verified thanks to DNSSEC
Encrypted communication thanks to PKI based on self-signed certificates

A Future Scenario

