Towards connecting everything safely & securely using DNS

Sandoche BALAKRICHENAN

Nov. 02 2022

afnic
Internet
made in France

Presented at IEEE-CAMAD @Paris(2022)

afnic | Labs

Agenda

- About Afnic
- Importance of Identifiers and the DNS role in the Internet
- DNS as glue between the Internet and IoT
- Using DNS for safe & secure connection in a real IoT use case
- Extending DNS for privacy in the Internet

afnic | Labs

About Afnic

afnic | Labs

About Afnic



TLDs Operated by Afnic

As Registry



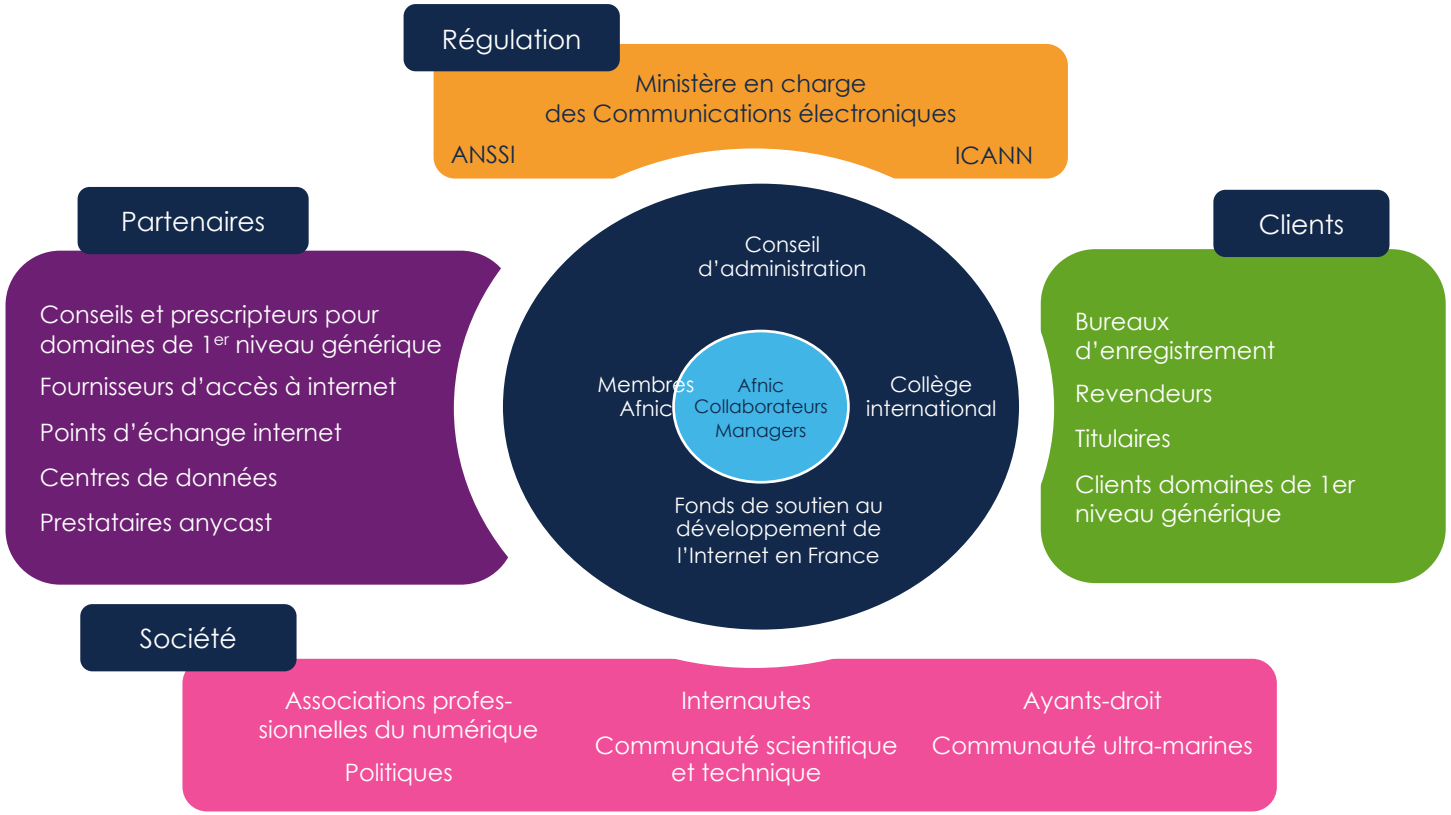
As Technical Operator



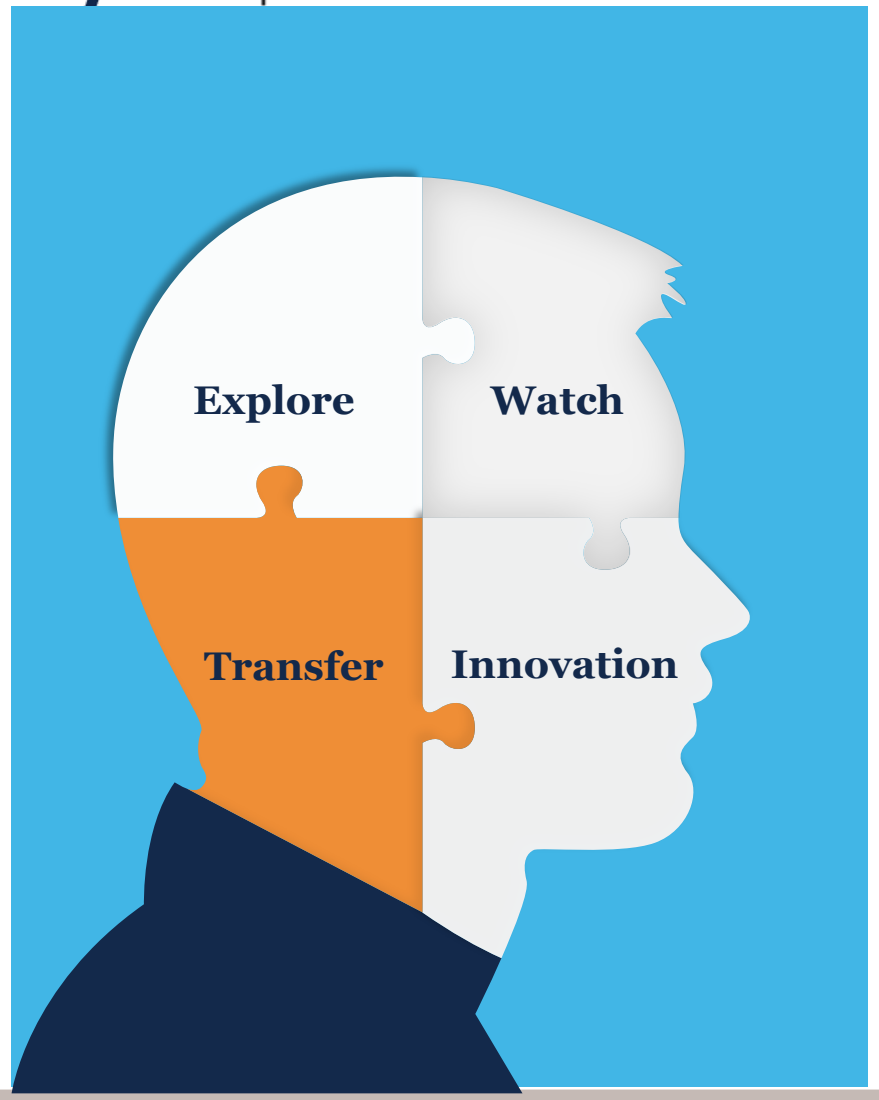
As Technical Operator for Closed TLDs



Stakeholder mapping



About Afnic Labs



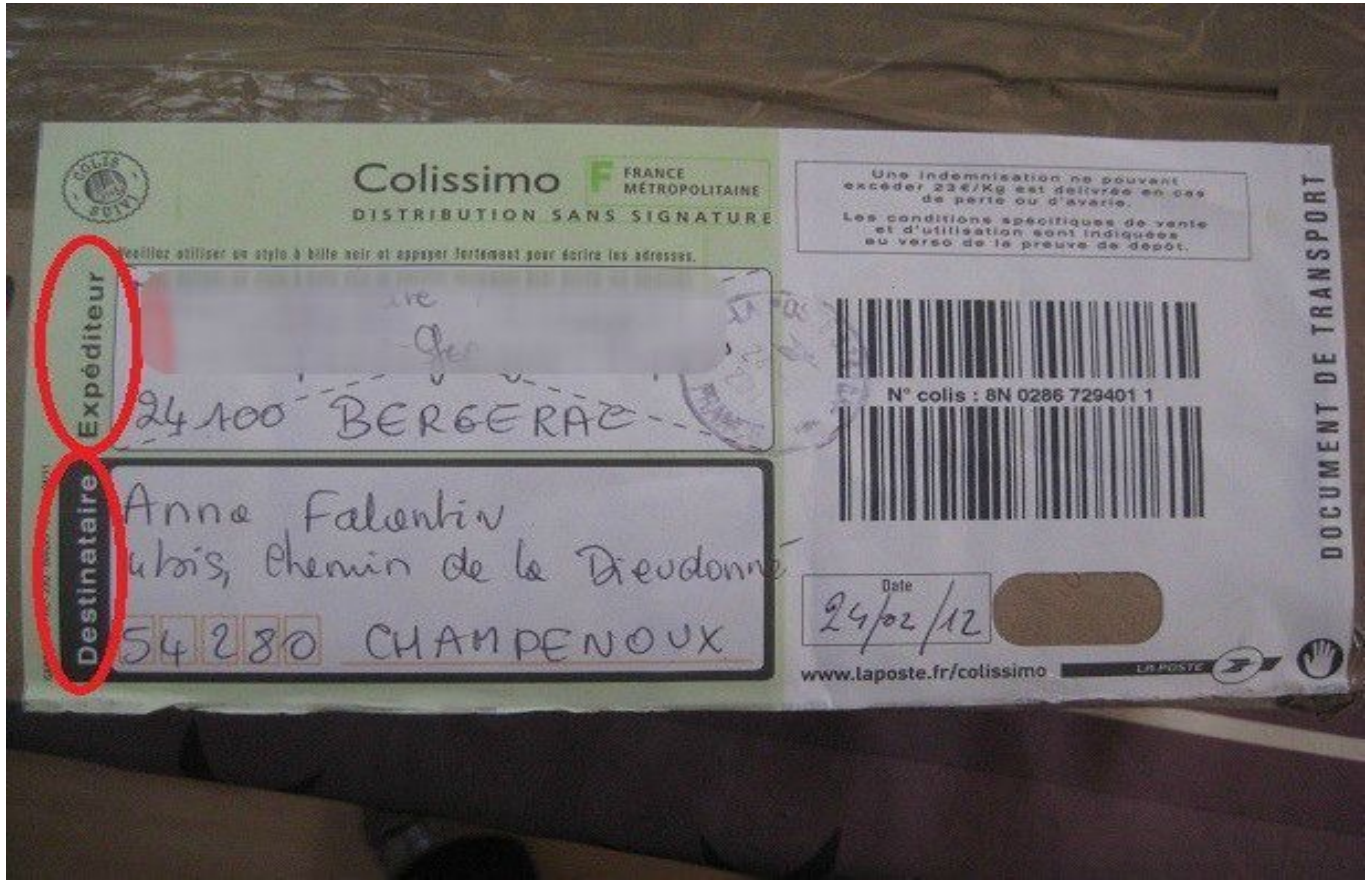
- Work on Experimental projects
- Ensure technology watch and contribute to standardization activities
- Knowledge and know-how transfer
- Prototype new products and services

afnic | Labs

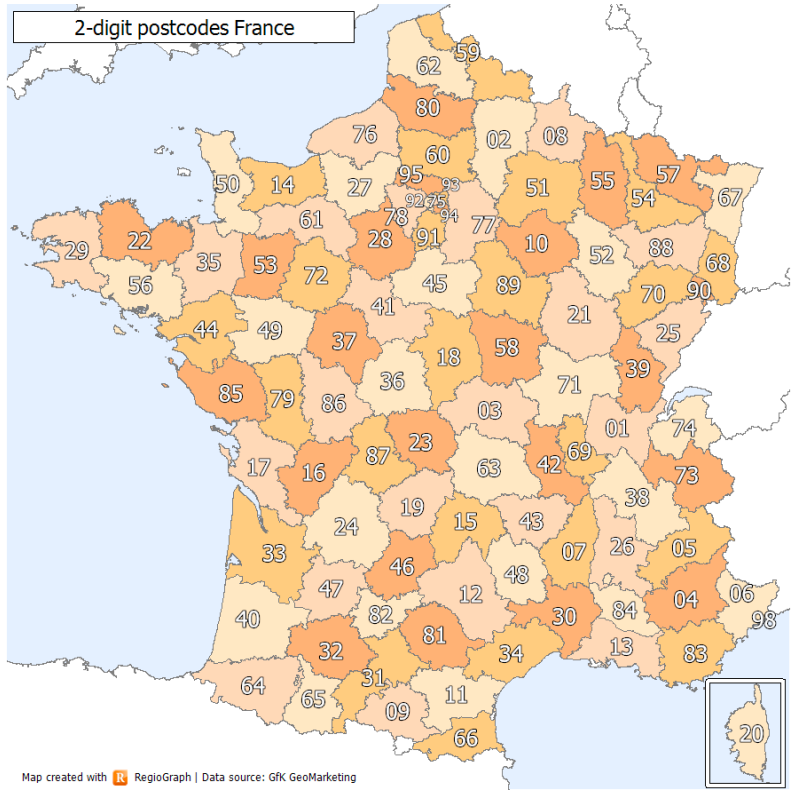
Importance of Identifiers and DNS role in the Internet

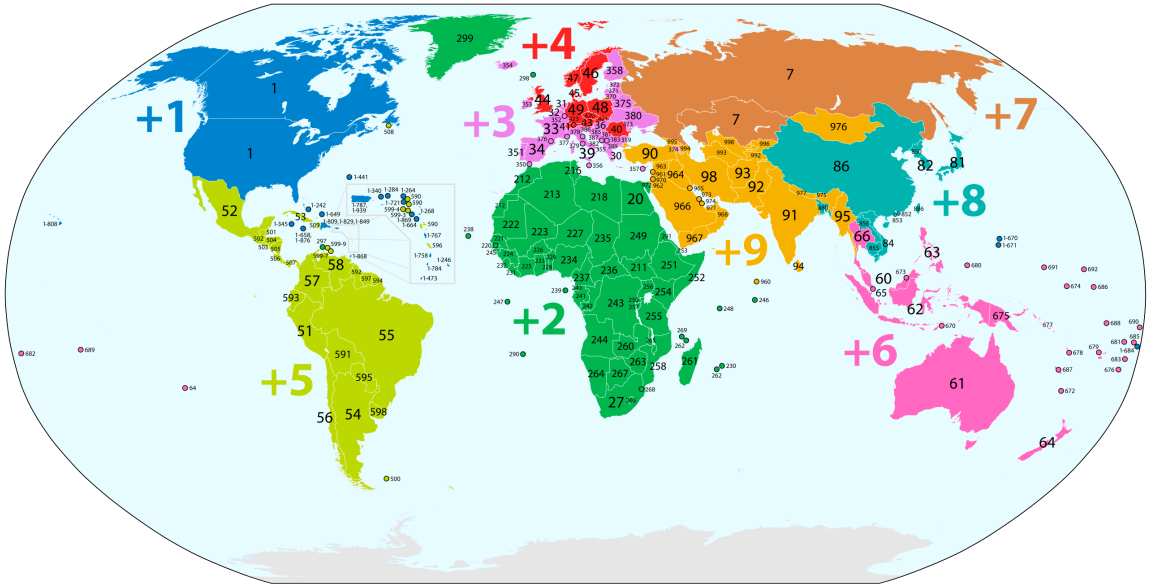
afnic | Labs

Identity – Core for communication



Identifiers - Hierarchical



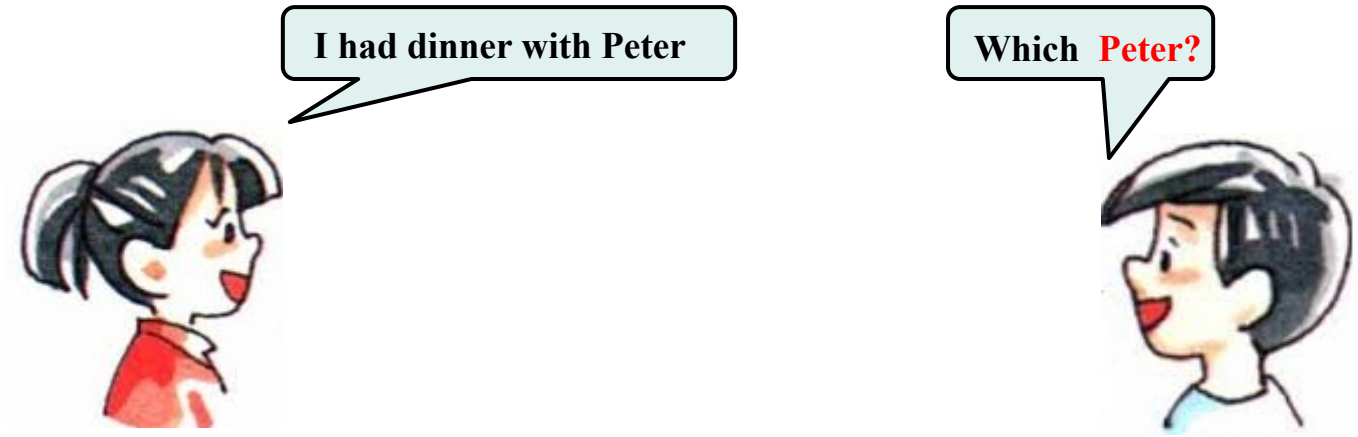




Why do we need DNS for Internet Identity management? (1/5)



Why do we need DNS for Internet Identity management? (2/5)



Why do we need DNS for Internet Identity management? (3/5)

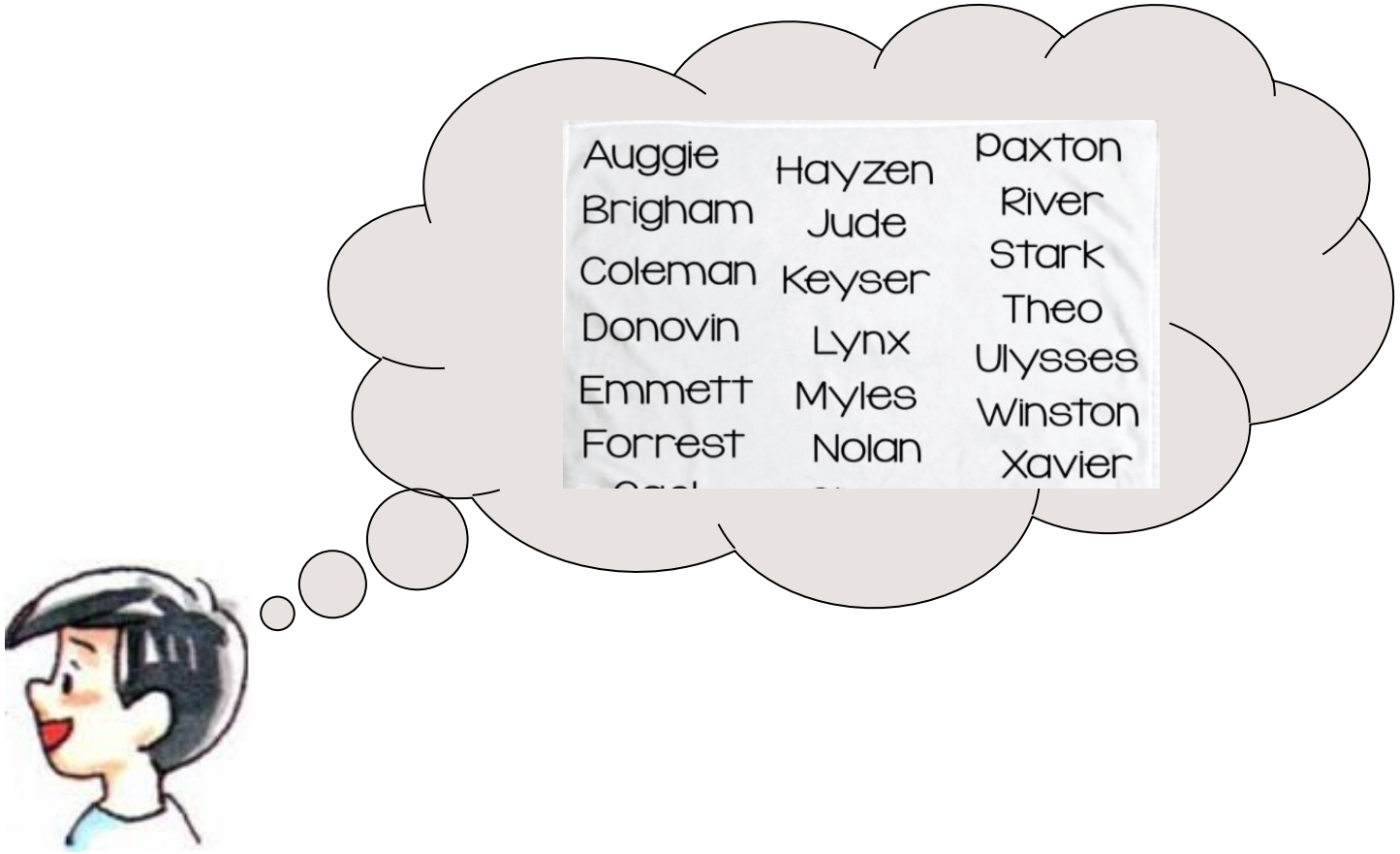


Why do we need DNS for Internet Identity management? (4/5)

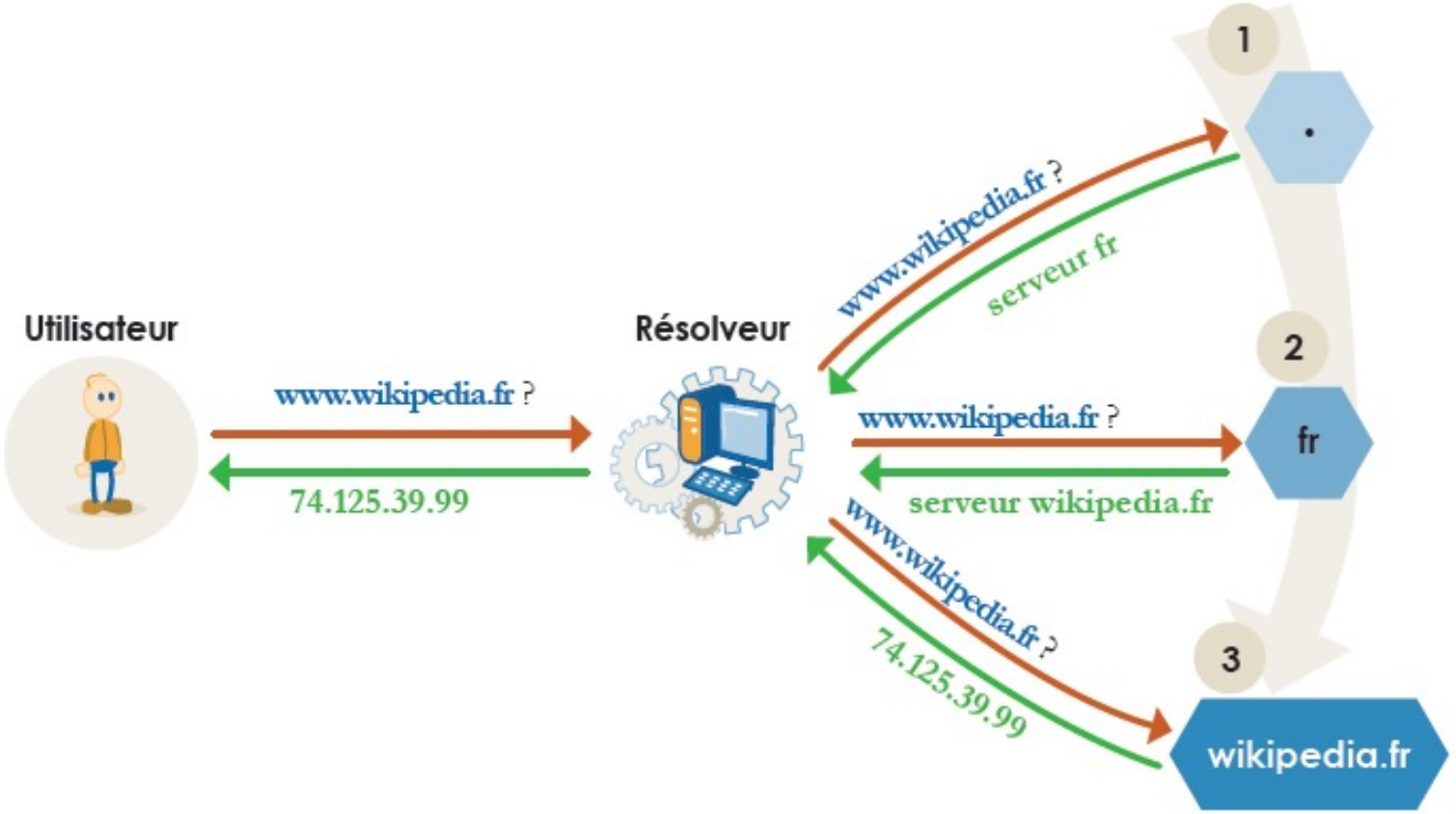
- balakrichenan.fr, .இந்தியா

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

Why do we need DNS for Internet Identity management? (5/5)



Domain Naming System (DNS)



Three steps to resolve an Identifier in the Internet

1. Naming Conventions

IETF is the SDO

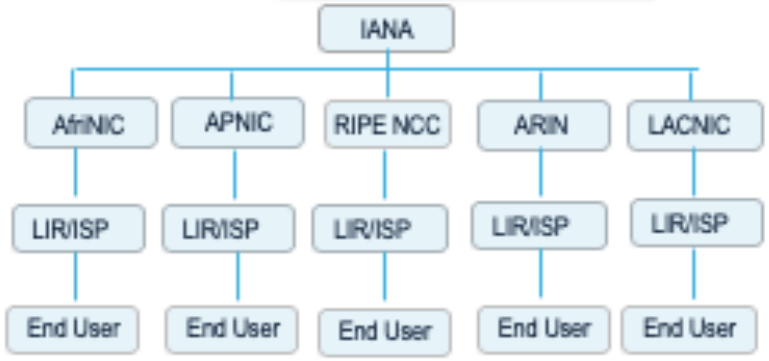
- Domain names, URI
- IP Addresses (IPv4/IPv6)

2. Provisioning

2.1. Domain registry



2.2 Internet number registry



3. Resolution



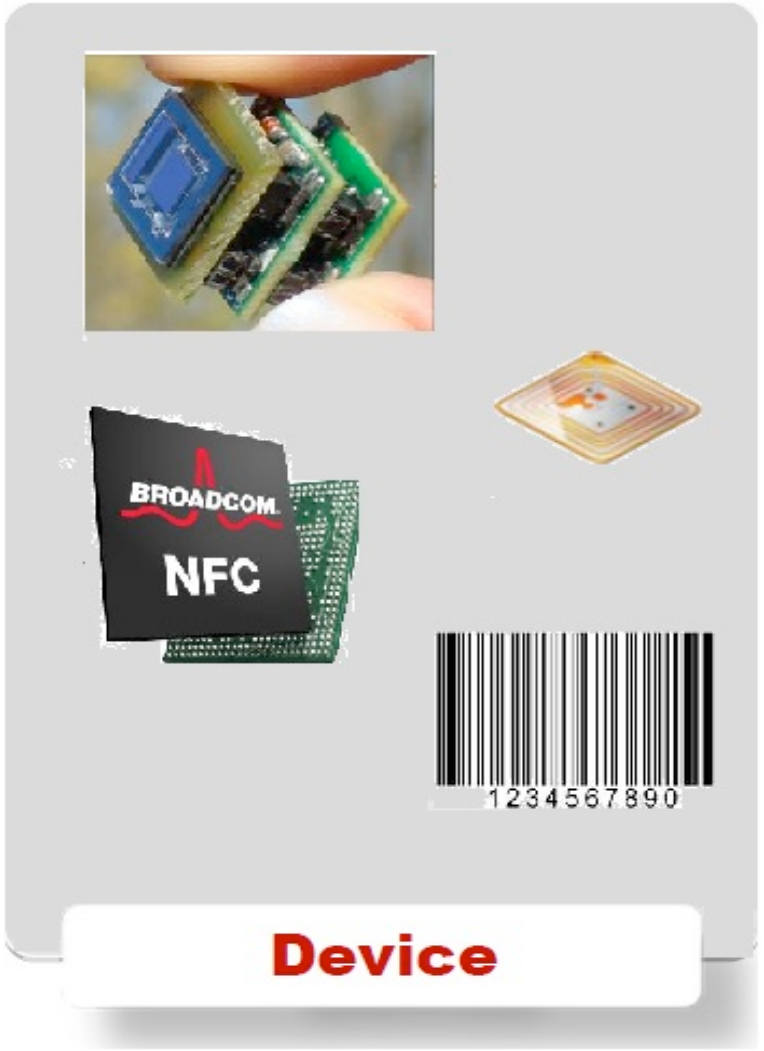
afnic | Labs

How DNS could act as a glue between the Internet and the IoT?

afnic | Labs

Towards Connecting everything

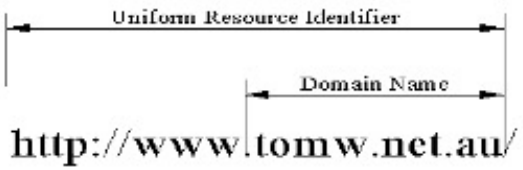




afnic | Labs

Identifiers in IoT

IETF



ISO/IEC 15459



GS1



ISO 2108



Resolving an IoT identifier in an Intranet of Things

Use-Case



1. Naming Conventions

- No SDO, No naming conventions required

2. Provisioning



3. Resolution



Resolving an IoT identifier in an Intranet of Things

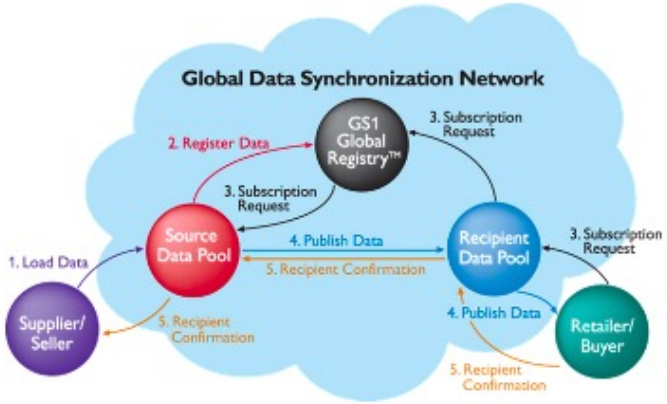
Use-Case



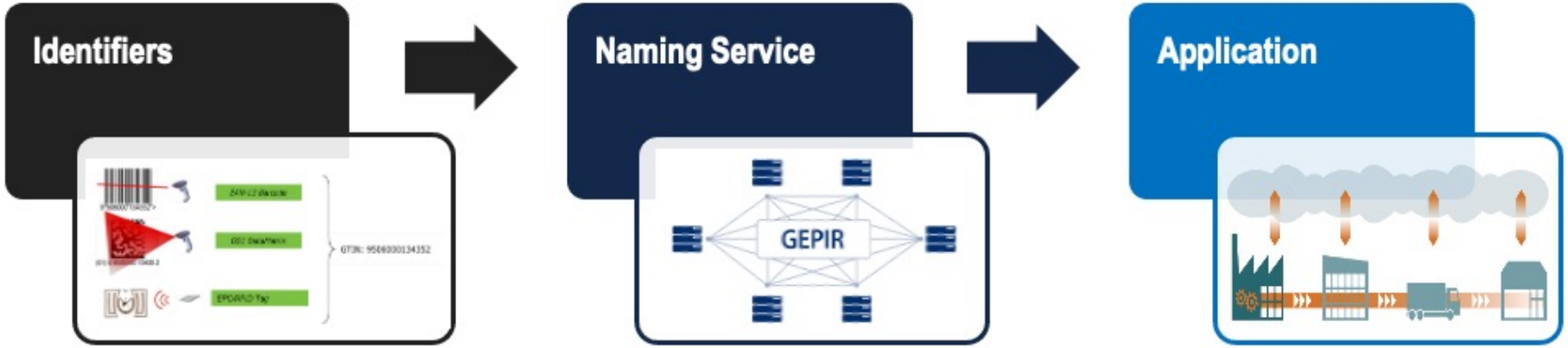
1. Naming Conventions

- GTIN
- GS1 Standards

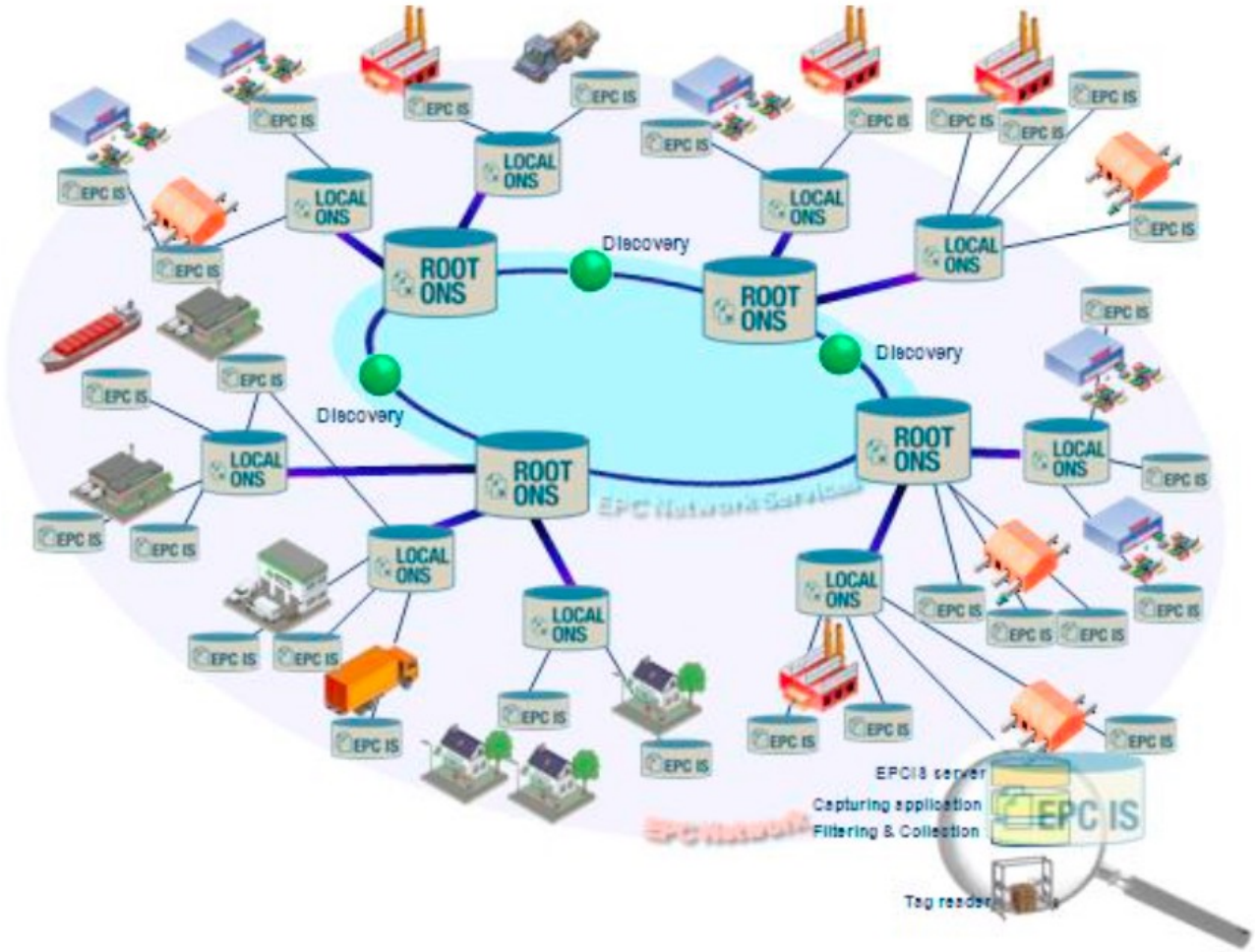
2. Provisioning



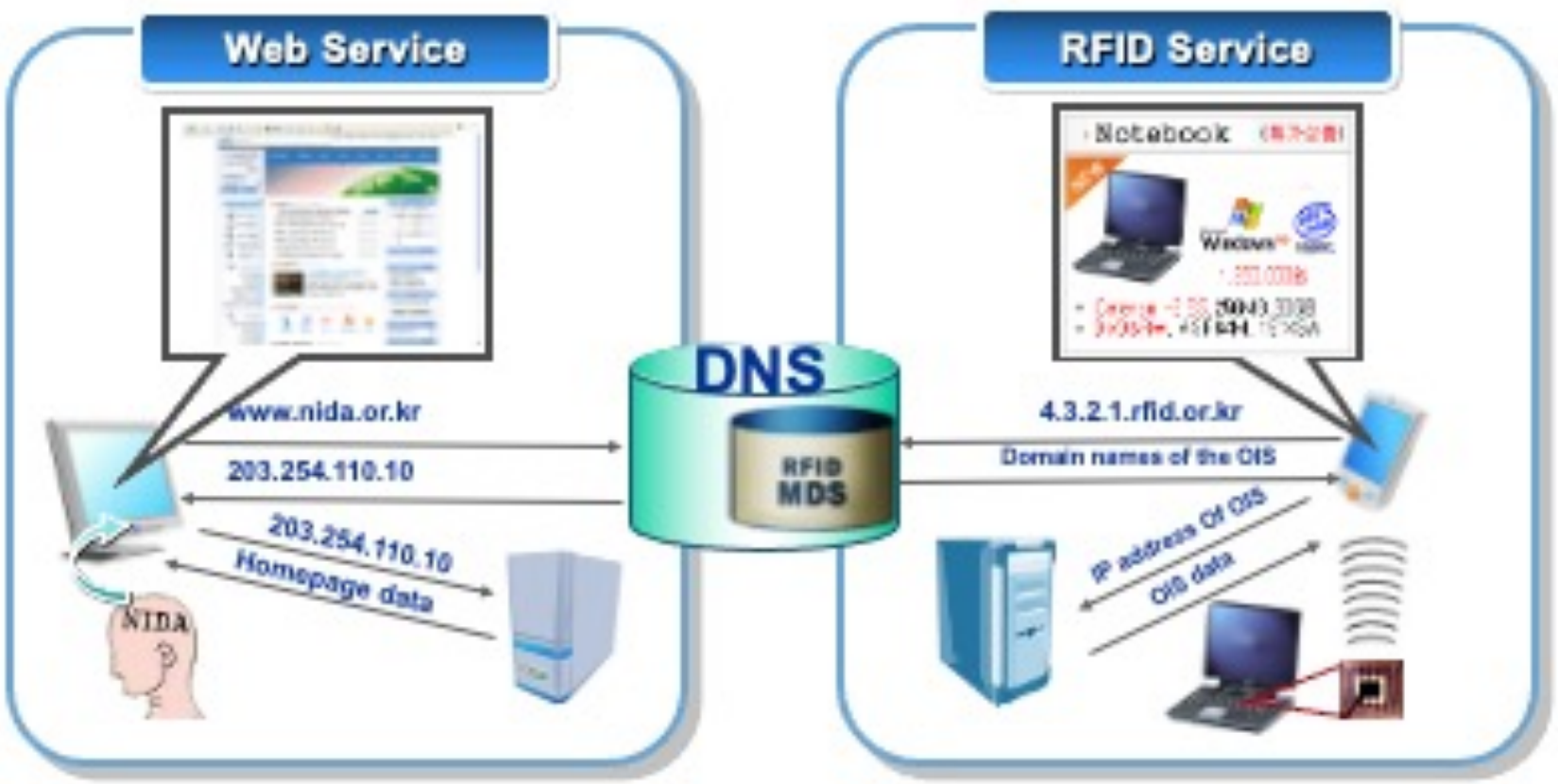
3. Resolution



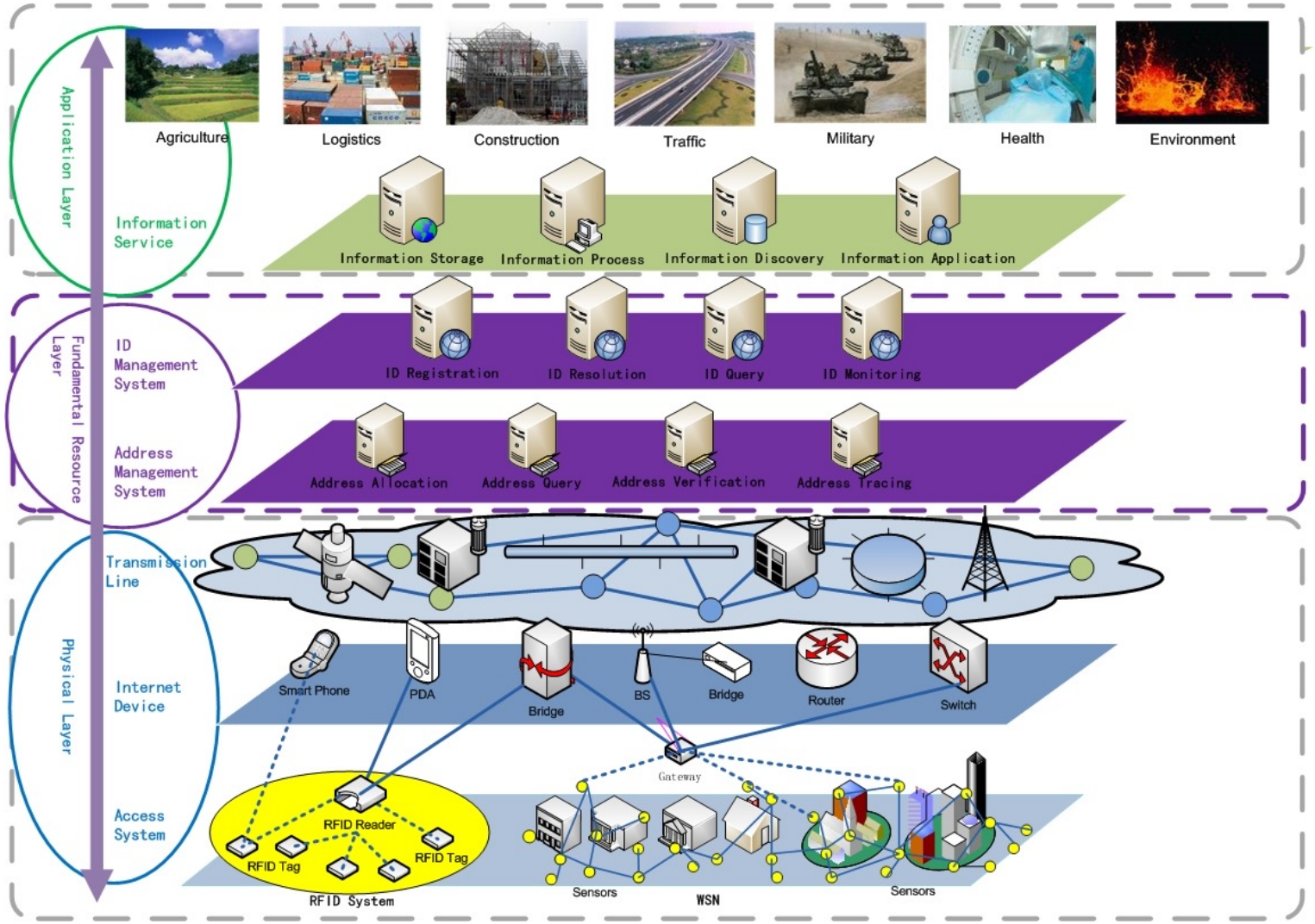
Interoperate between different Intranets' using DNS – Supply Chain Industry use-case



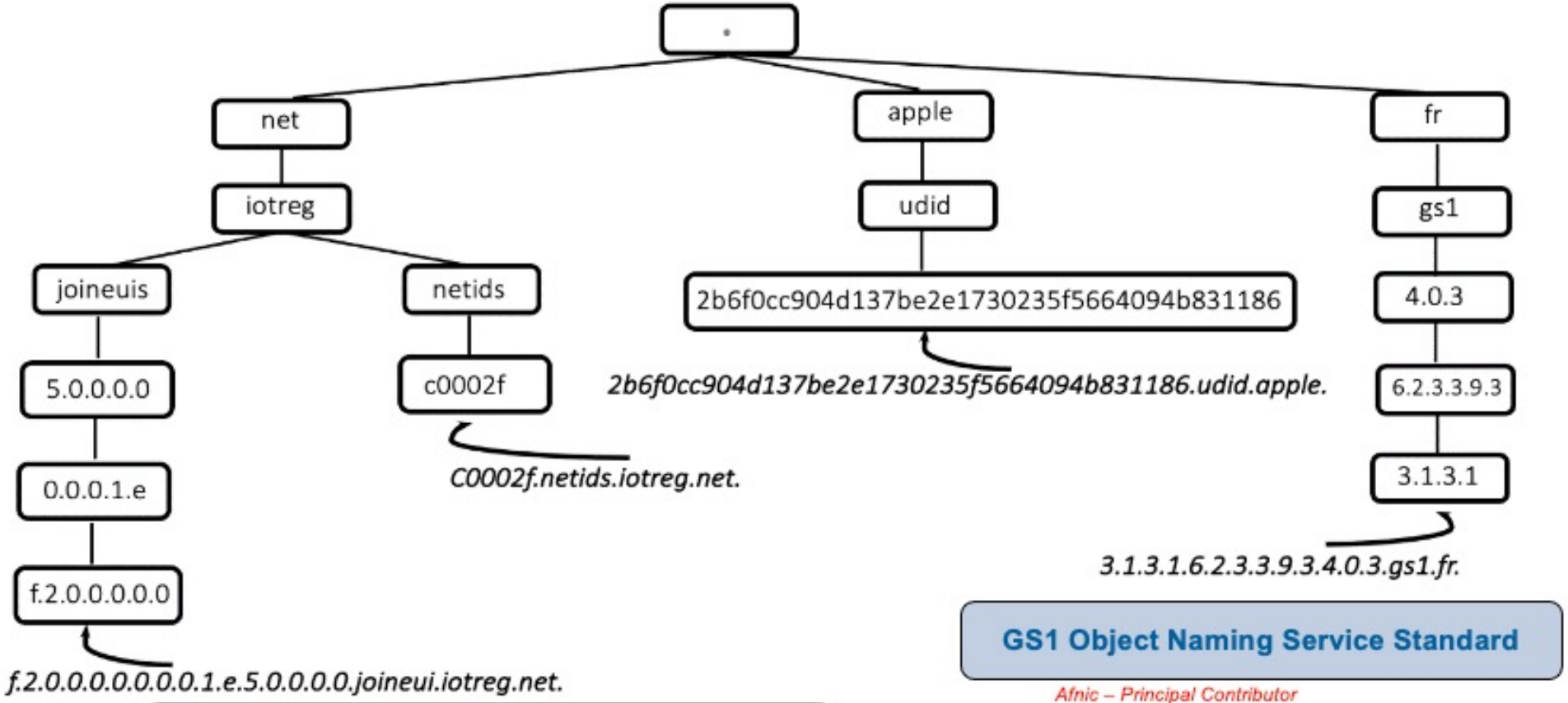
Interoperate between different Intranets' using DNS – Object Directory Service Resolution



Interoperate between different Intranets' using DNS – Chinese IoT registry



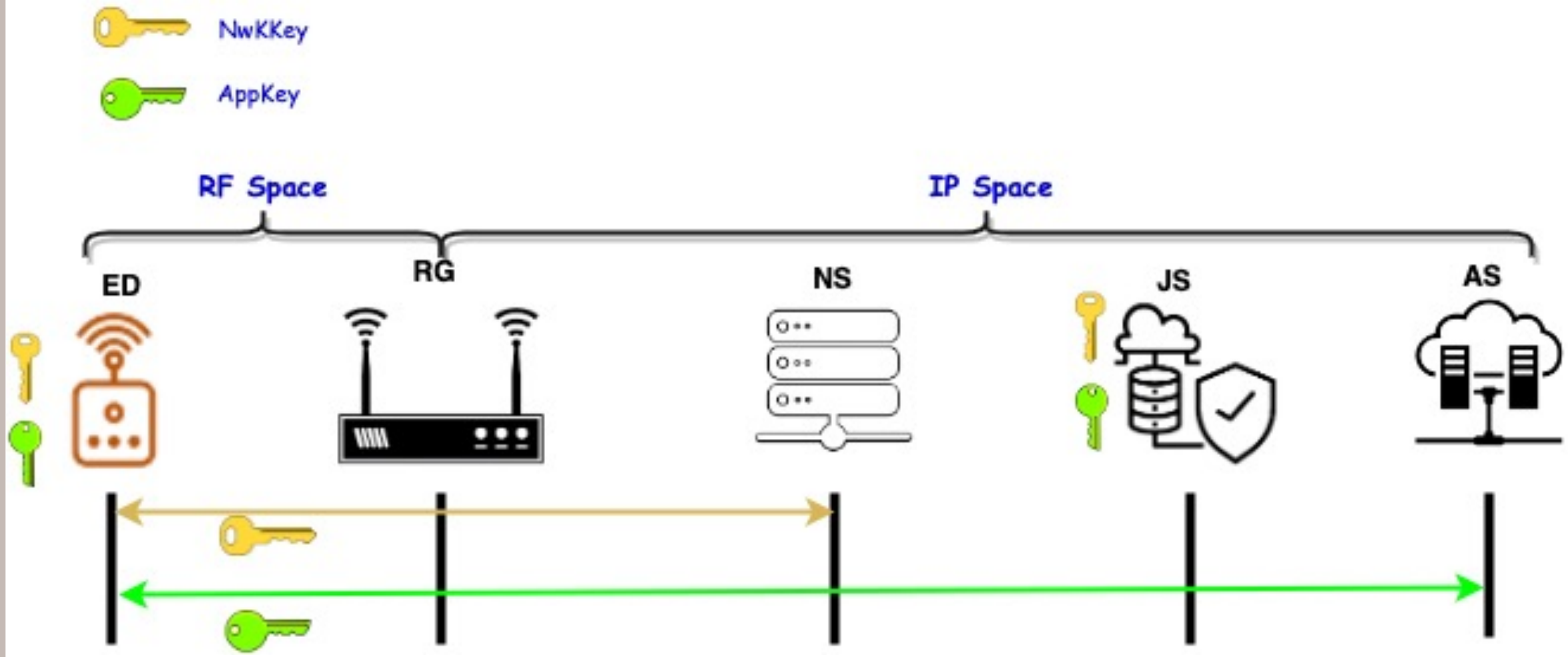
Afnic's contribution using DNS for IoT Interoperability



afnic | Labs

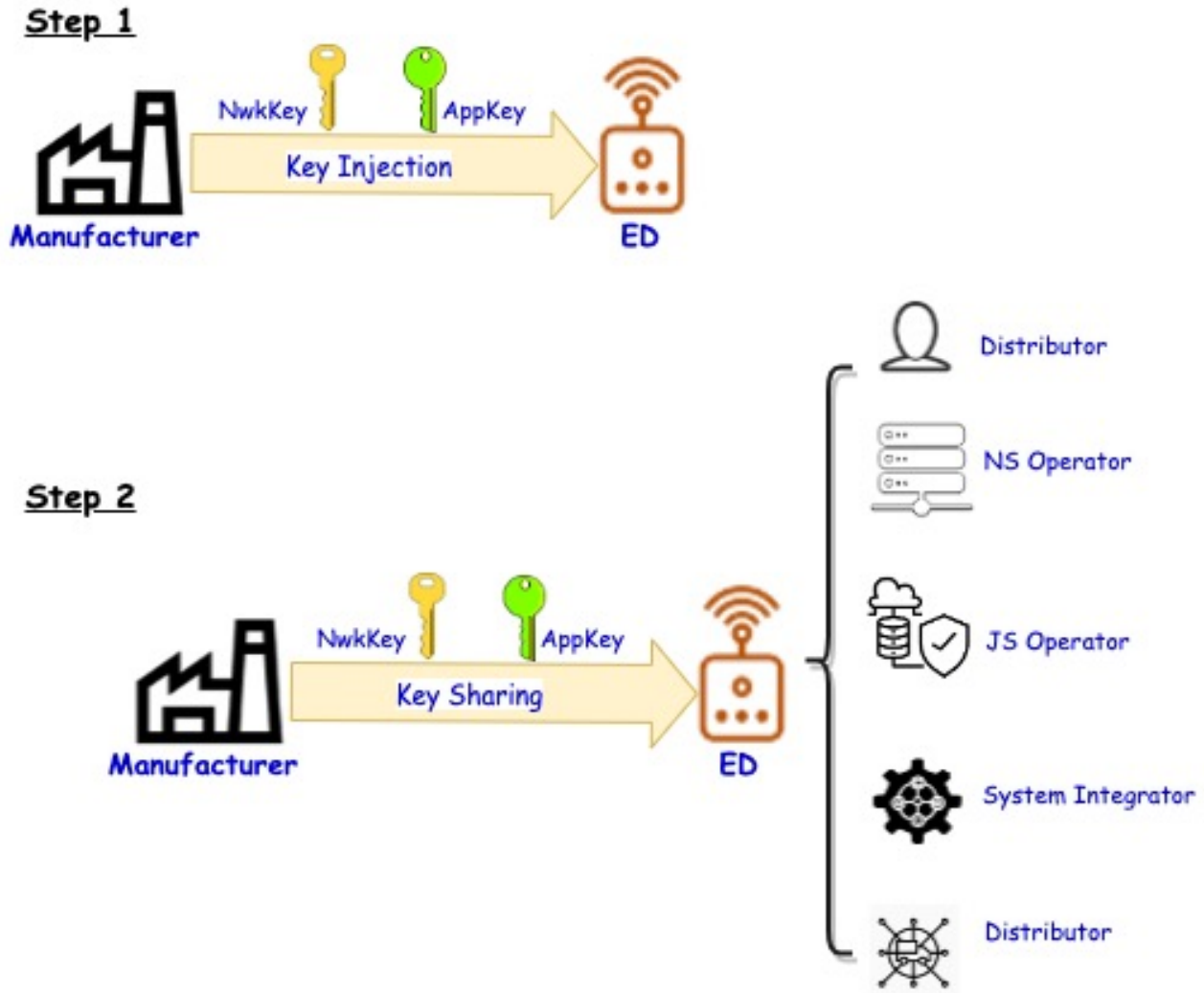
Using DNS for safely and securely connection in a real IoT use case

Symmetric Cryptography & RF, IP Space – LoRaWAN Use case



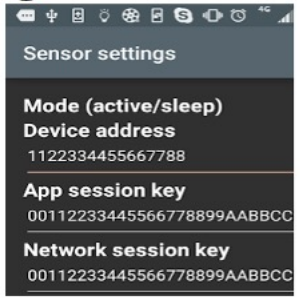
afnic | Labs

Key sharing dilemma between the RF & IP space



afnic | Labs Examples of how PSK's are shared?

1 Accessible via NFC
On mobile phones



2 Printed behind the ED



3 Sent via mail



Key sharing dilemma within the IP space

- AS-JS
- JS-NS
- NS-NS

From Section 21 of the LoRaWAN Backend Specifications:

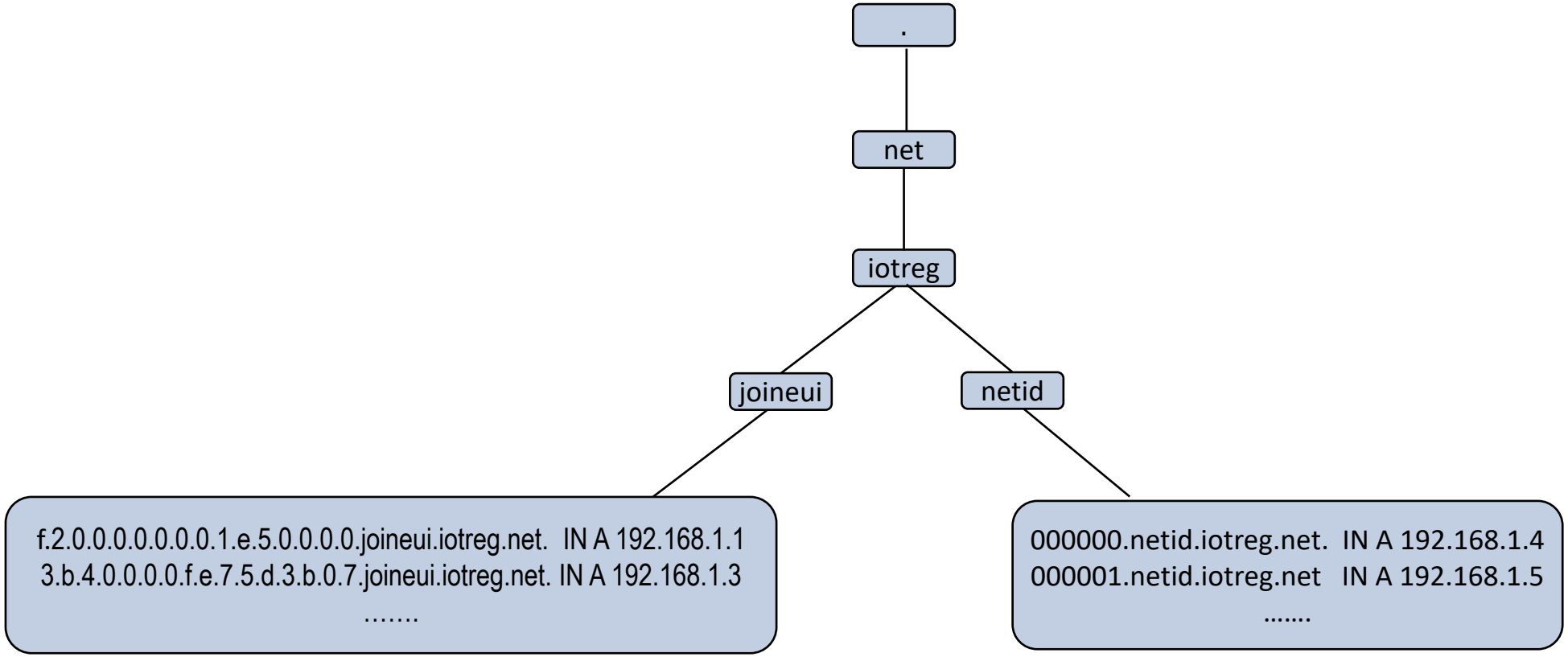
> Network elements SHALL rely on a security solution that can provide mutual end-point authentication, integrity and replay protection, and confidentiality when communicating with each other. The choice of mechanism used for achieving these properties is left to the deployments (e.g., using IPsec VPN, HTTPS, physical security, etc.)

Using the web based *asymmetric cryptography (PKIX)* in IP space

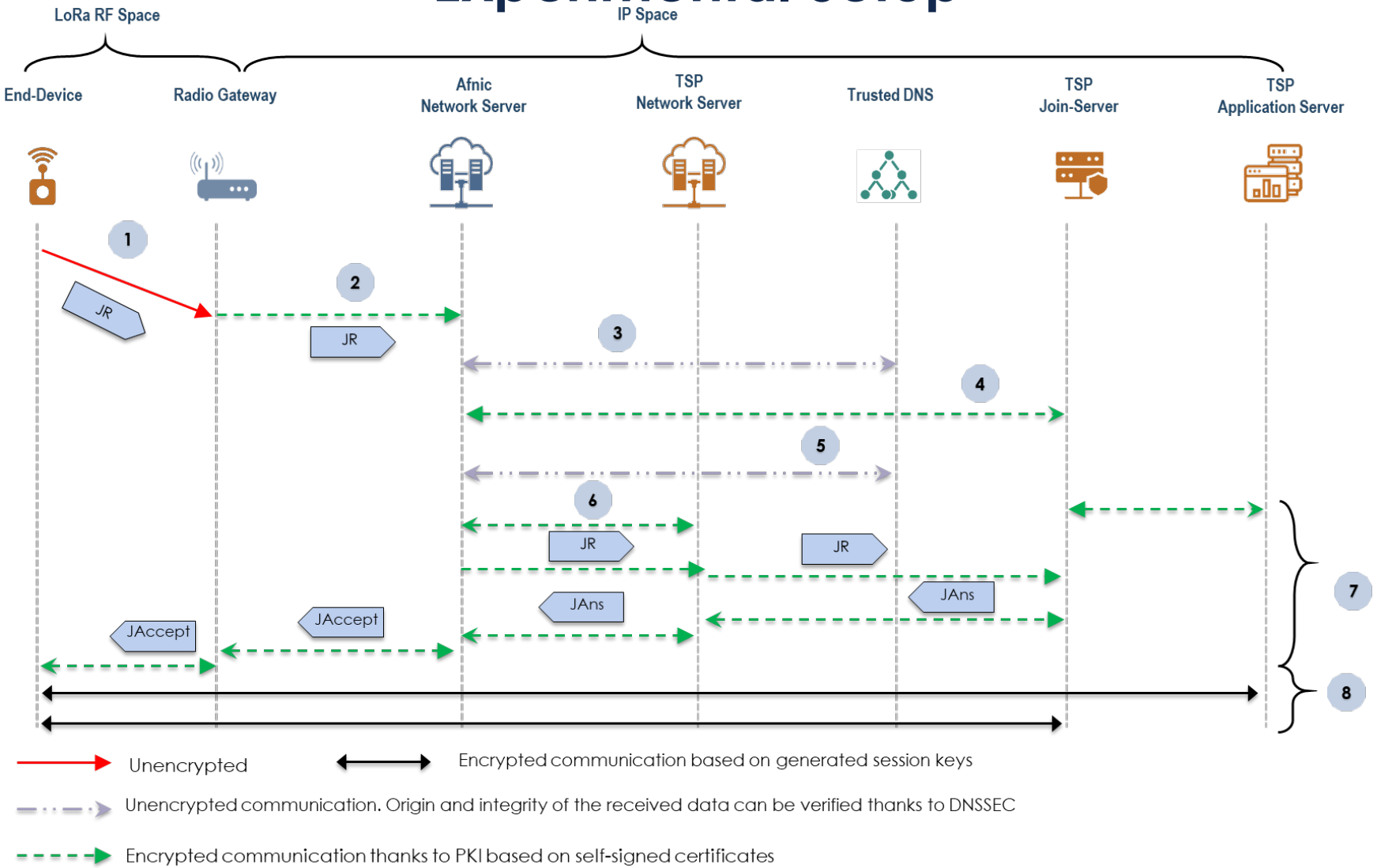
Issues	Solutions
Cost	Self-Signed Certificates
Label length	Self-Signed Certificates
Non-Availability of CA trust-store	**DNS-Based PKI**

	Comodo PositiveSSL	Comodo InstantSSL Premium	Comodo PositiveSSL EV
Pricing	Listed Price: $49.00/yr. Our Price: **$7.27**/yr.	Listed Price: $179.95/yr. Our Price: **$56.06**/yr.	Listed Price: $149.00/yr. Our Price: **$74.99**/yr.

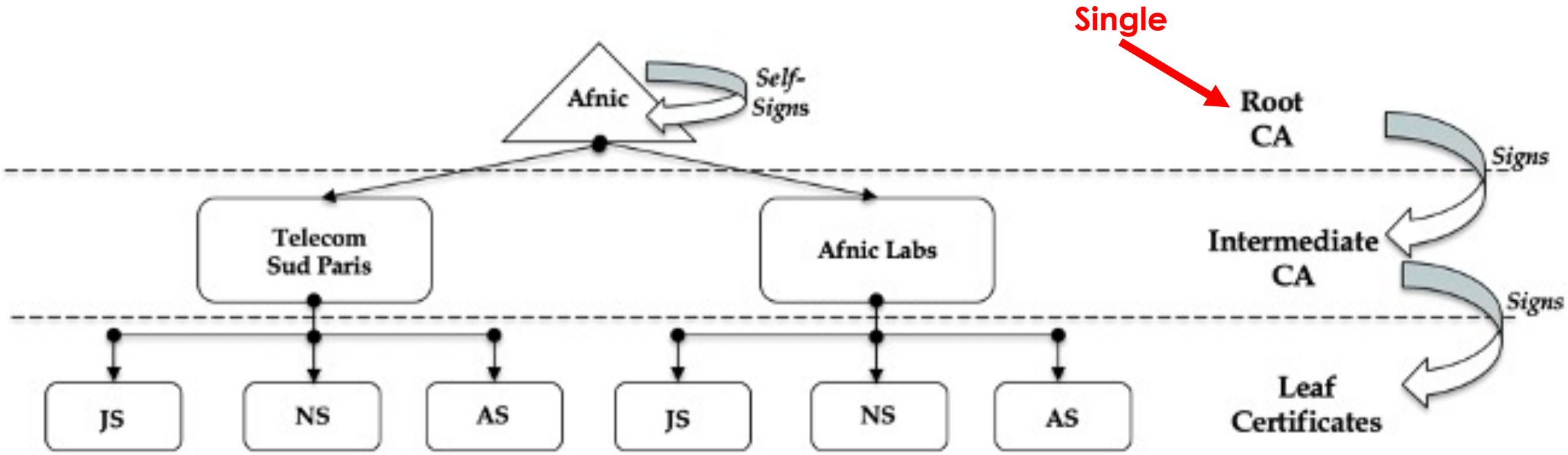
DNS Provisioning



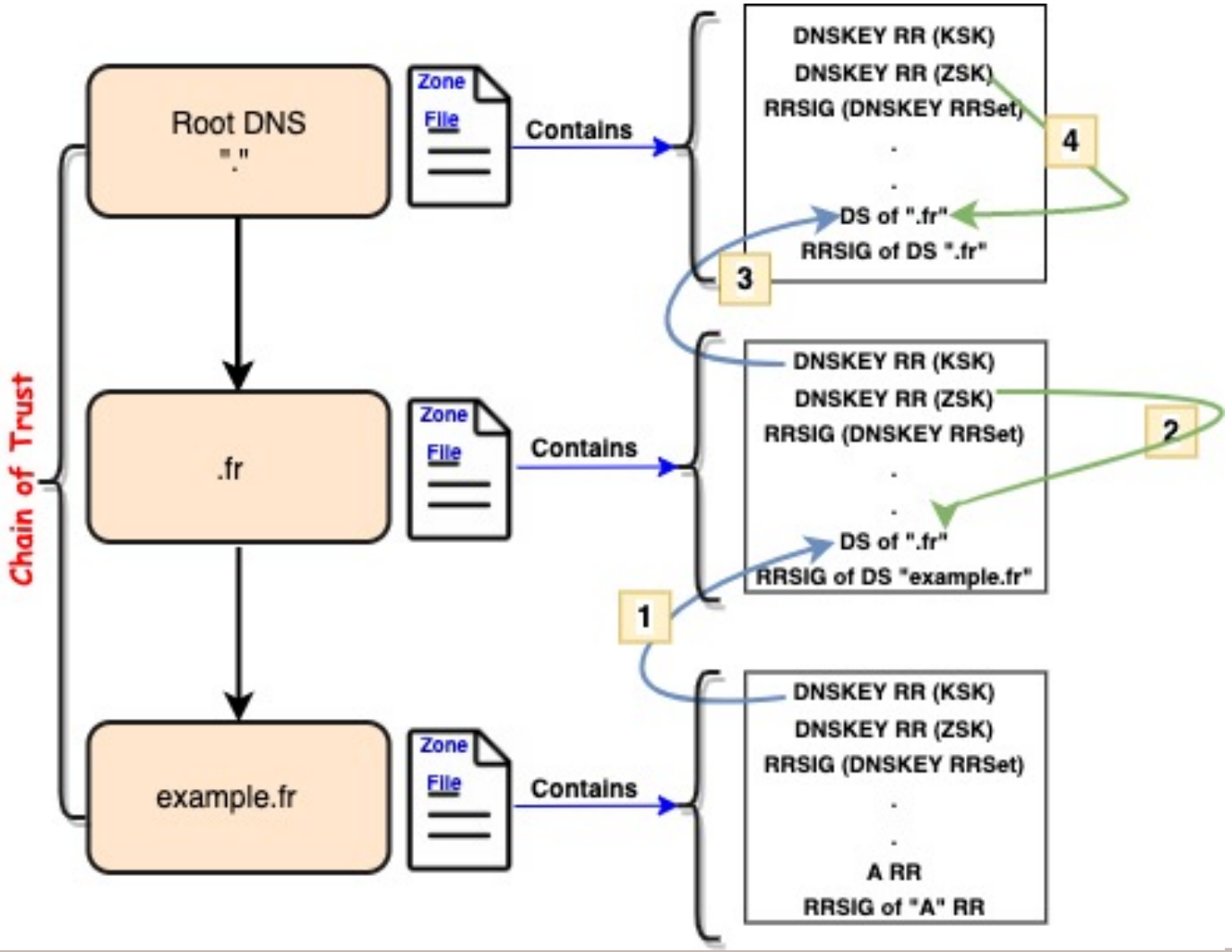
Experimental Setup



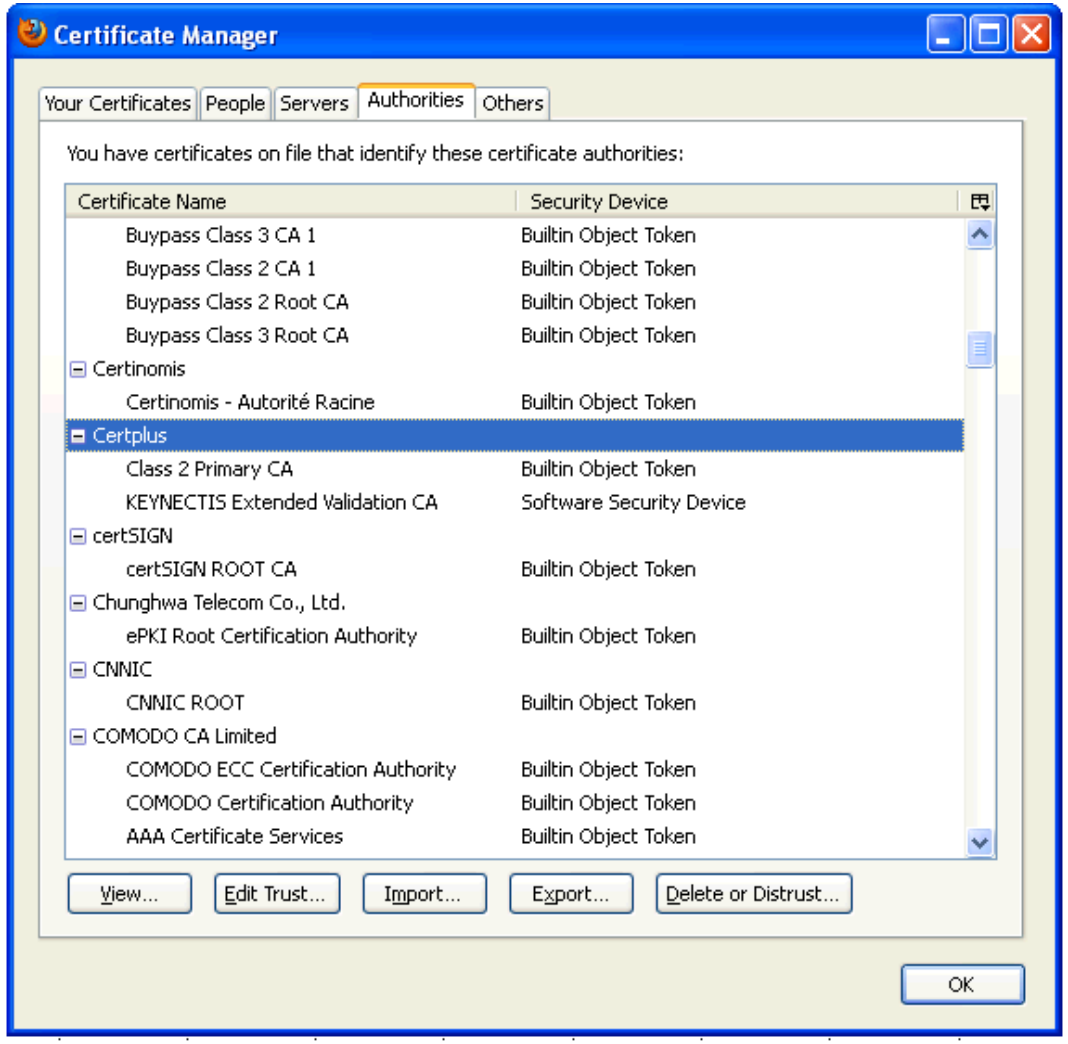
Issue in using Self-signed certificates



PKI using DNS – DNSSEC Primer

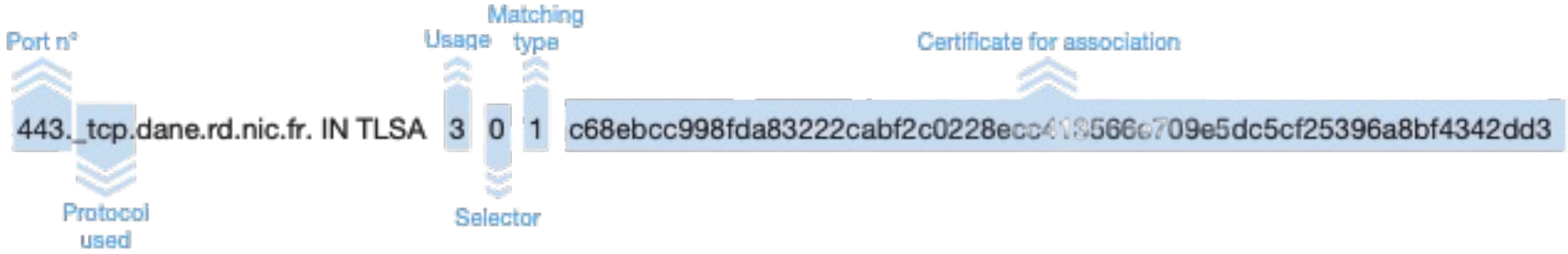


PKI using DNS – DANE Primer (1/2)





DNS Based PKI using DNSSEC & DANE



Using DANE indication Client/Server Authentication – Federated CA's

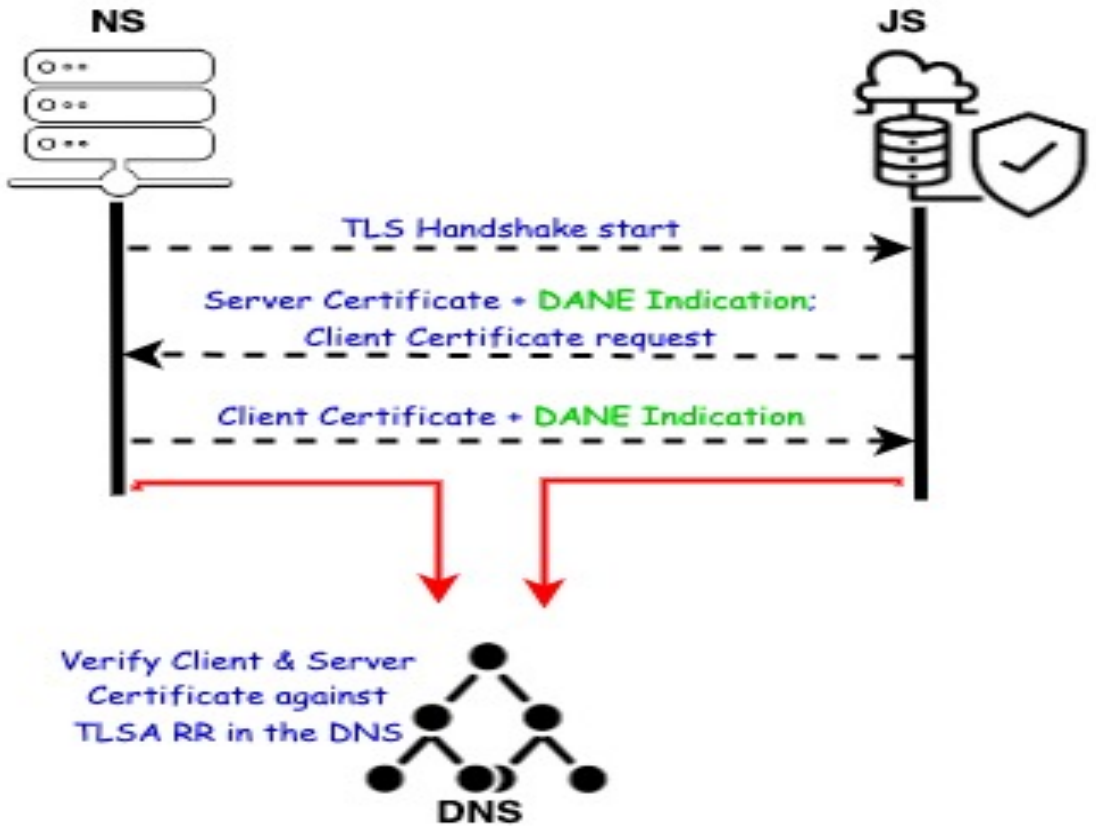
draft-ietf-dance-client-auth-00

TLS Client Authentication via DANE TLSA records

draft-ietf-dance-tls-clientid-00

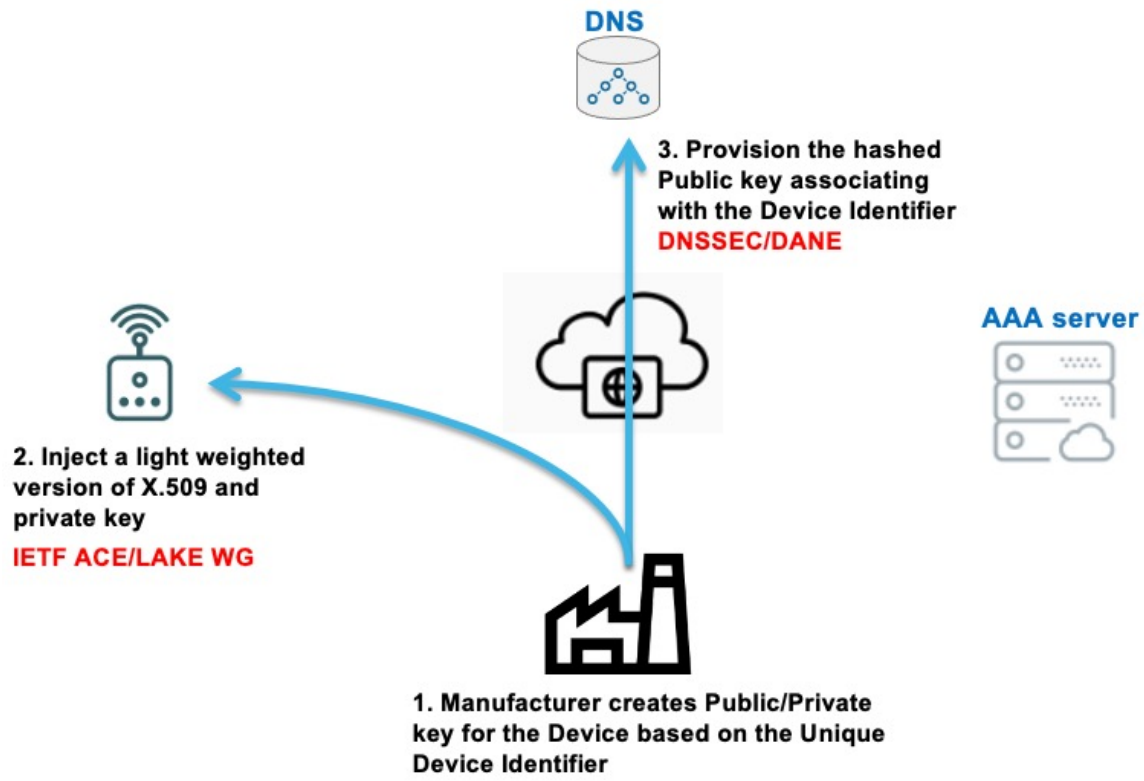
TLS Extension for DANE Client Identity

Afnic –implemented and tested the two IETF drafts during IETF 113 Hackathon



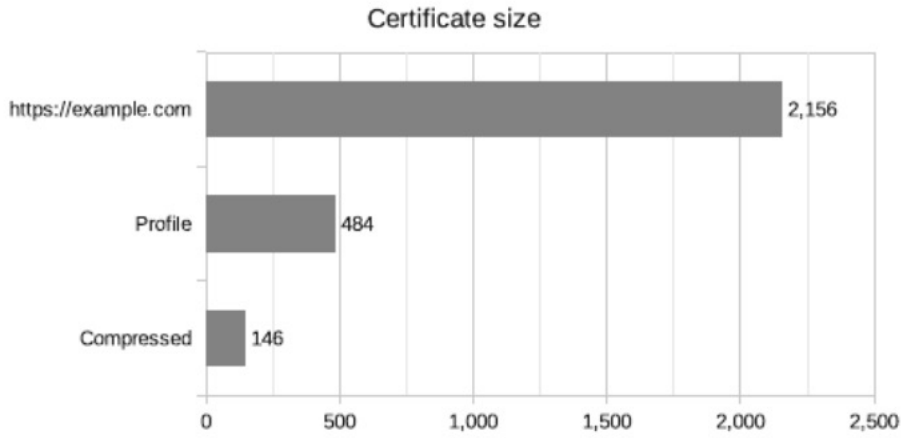
Enables using self-signed certificate with multiple Root CA's

An ideal scenario for E2E Security



Web based X.509 digital certificates cannot be deployed directly in the 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

afnic | Labs

Issues being Solved based on DNS-Based PKI

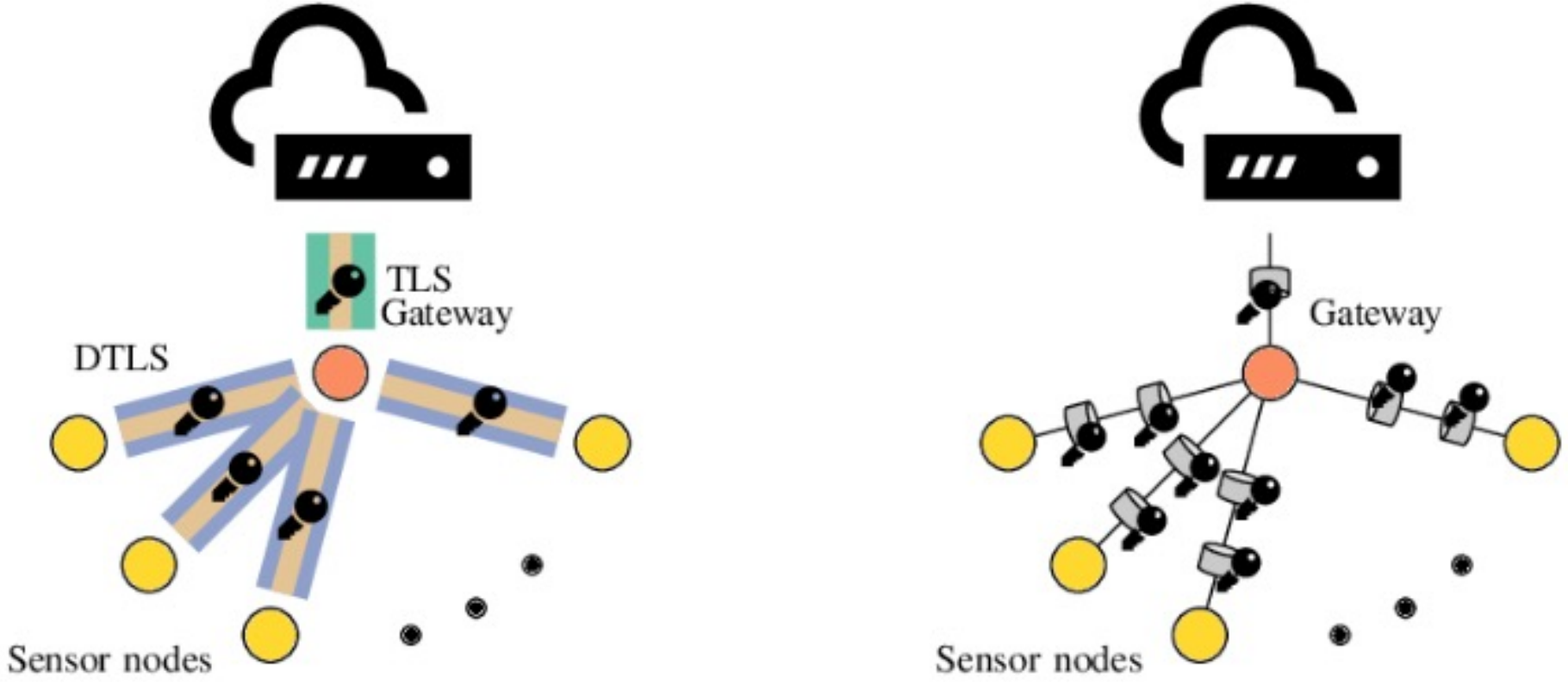
Constrained IoT Device	**WIP**
Constrained IoT Network	**WIP**
Non-Availability of CA Libraries	**Solved**
Cost	**Solved**
Closed Security Infrastructure	**Solved**
Scalability	**Solved**
Bootstrapping trust	**Solved**

afnic | Labs

Extending DNS for privacy in IoT

afnic | Labs

Channel vs Object Security



Source: *IoT Content Object Security with OSCORE and NDN: A First Experimental Comparison*

PIVOT (*Privacy-Integrated design and Validation in the constrained IoT*)

PIVOT focusses on this 4 objectives

Propose a cryptographic system adapted to ultra-constrained objects

Define a trust architecture and the implementation of content security

Establish protocols that integrate decentralized content security

Implement a multi-stakeholder naming architecture that preserves confidentiality requirements and is able to allocate and resolve identifiers independently of applications or networks

Afnic's Vision

DONE

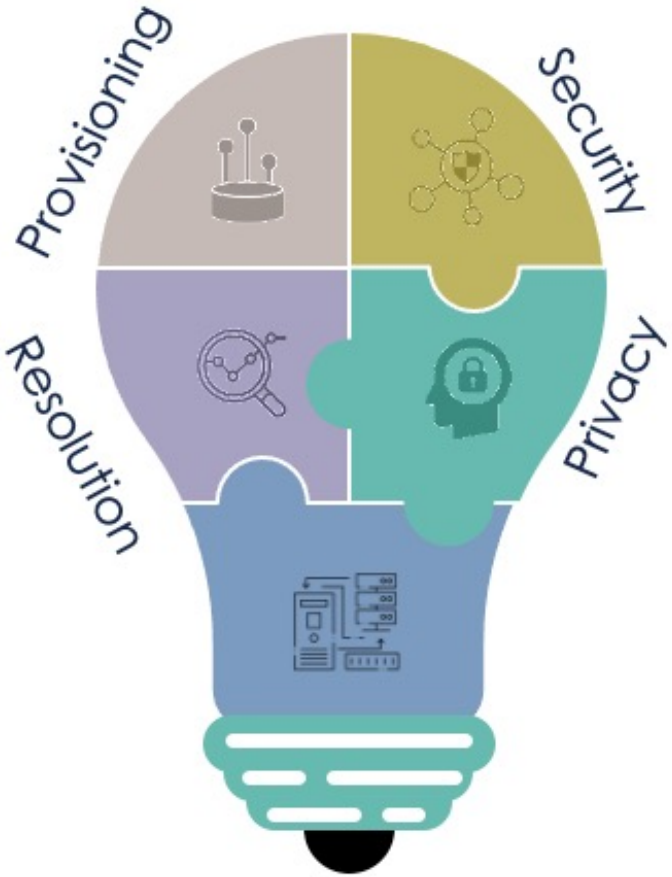
WINGS

Widening interoperability for networking Global supply Chains

DONE

LoRa Alliance

DNS Service



ONGOING

DINS*

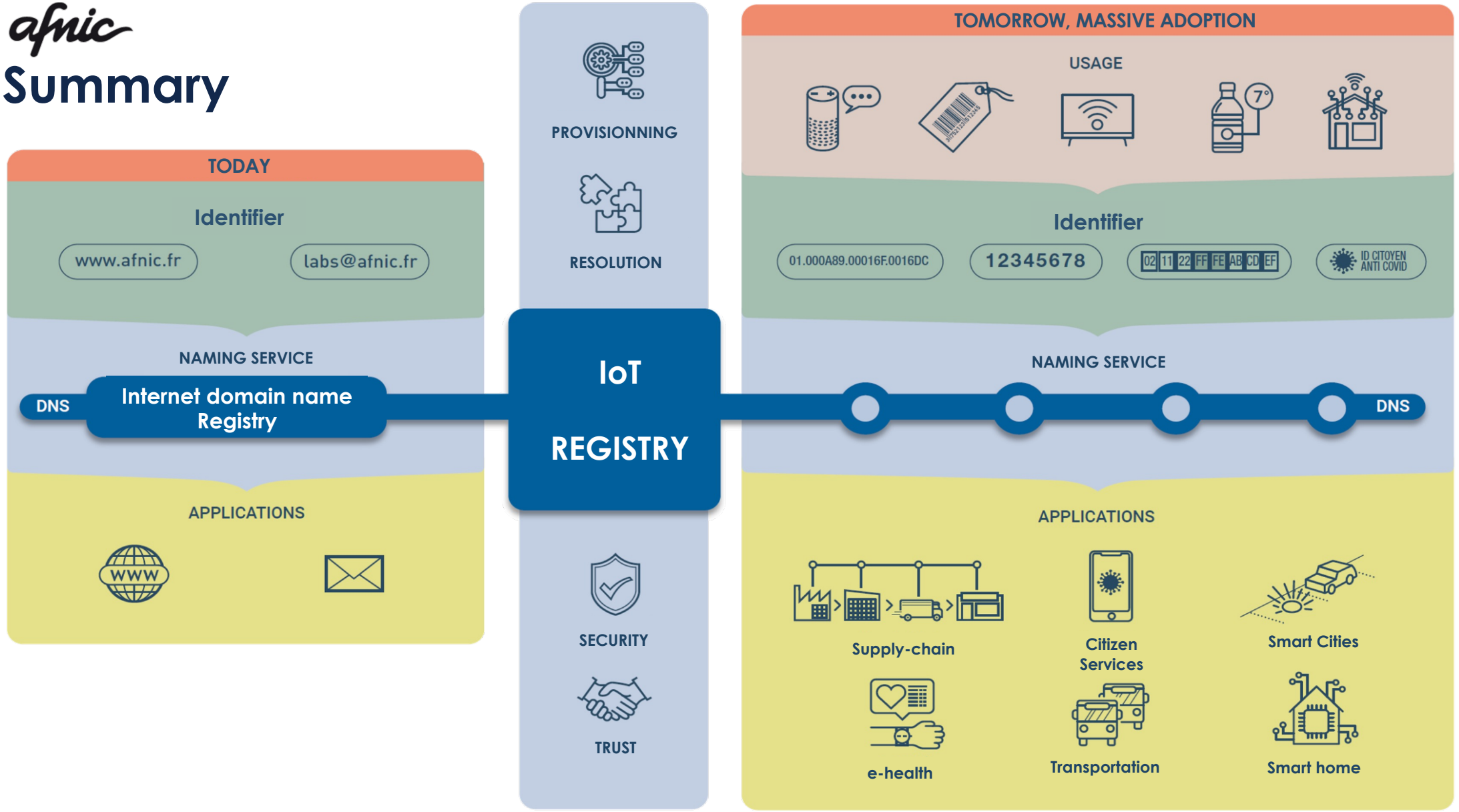
DNS Naming and Services for Secure Seamless IoT

ONGOING

PIVOT*

Privacy-Integrated design and Validation in the constrained IoT

Summary


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