Importance of Standardisation in the Industry & Academia

Sandoche BALAKRICHENAN

Dec. 16 2022

afnic
Internet
made in France

Presented for PEC @Pondicherry(2022)

afnic | Labs

Agenda

- About me & my Company
- Setting the stage
- Industry Use-Case
- Academic Use-Case
- About IETF

afnic | Labs



- Sandoche BALAKRICHENAN
  - PhD (Univ. Pierre et Marie Curie), MSc in Comp. & Comm. Networks (Institut Nationales des Télécommunications), MSc in Innovation & Entrepreneurship (HEC)
  - Head of R&D Partnerships @ French Network Information Center
  - RIPE IoT WG Co-Chair
  - LoRa Alliance Academic WG Chair

afnic | Labs

About Afnic

afnic | Labs

About Afnic



TLDs Operated by Afnic

As Registry



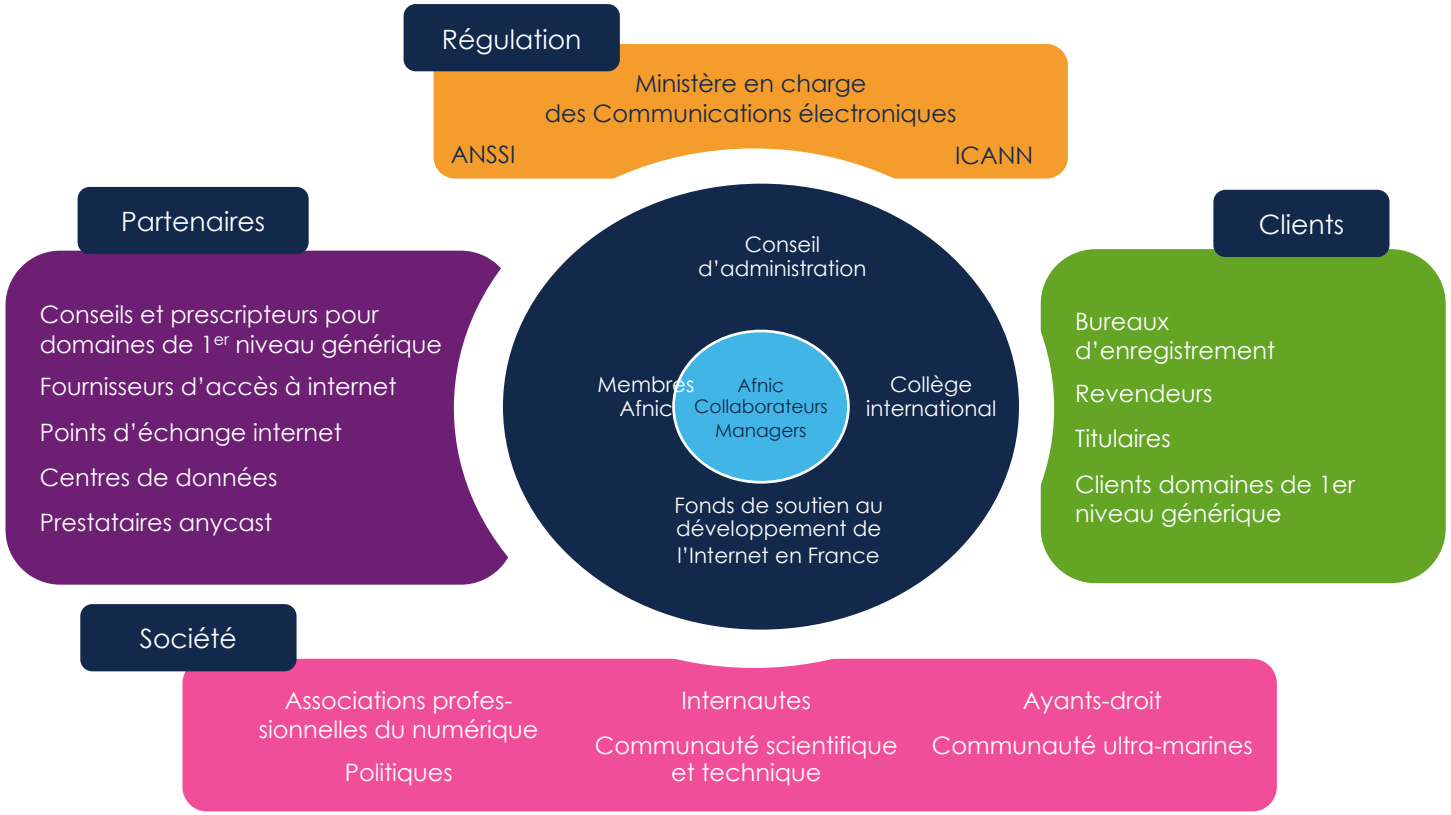
As Technical Operator



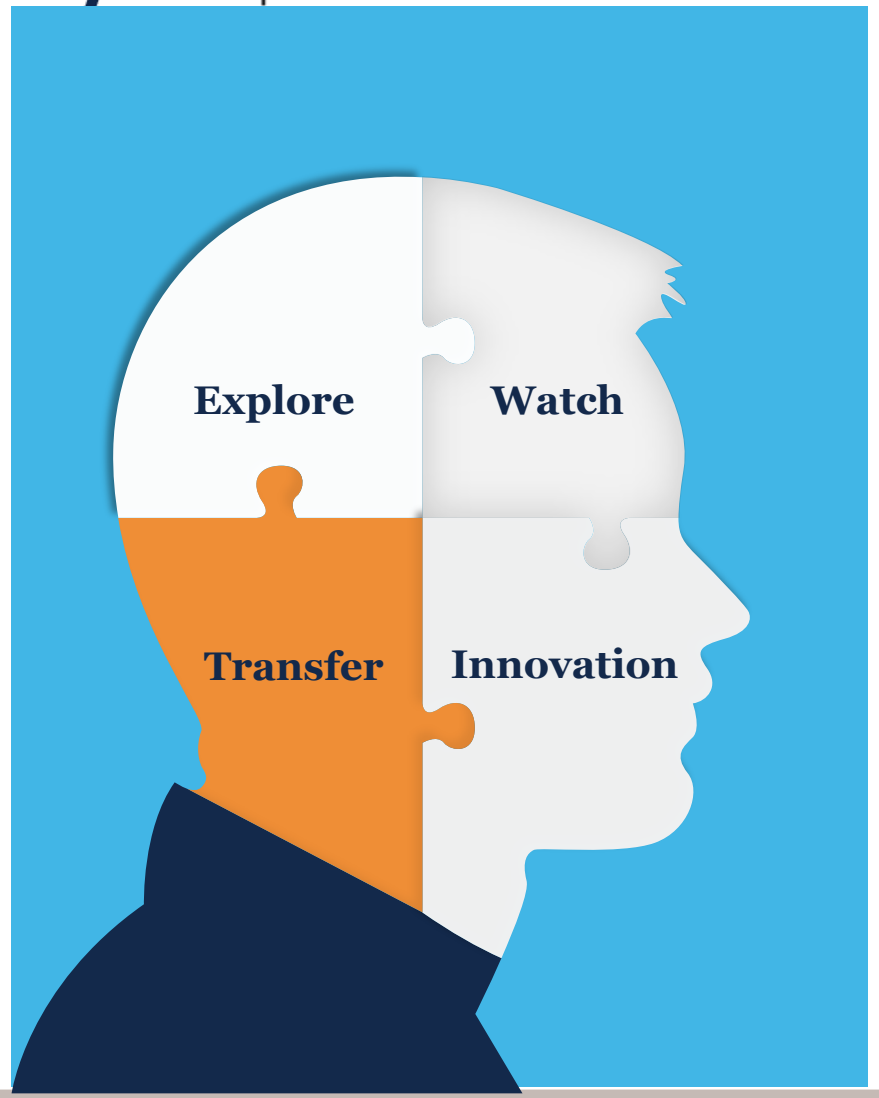
As Technical Operator for Closed TLDs



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

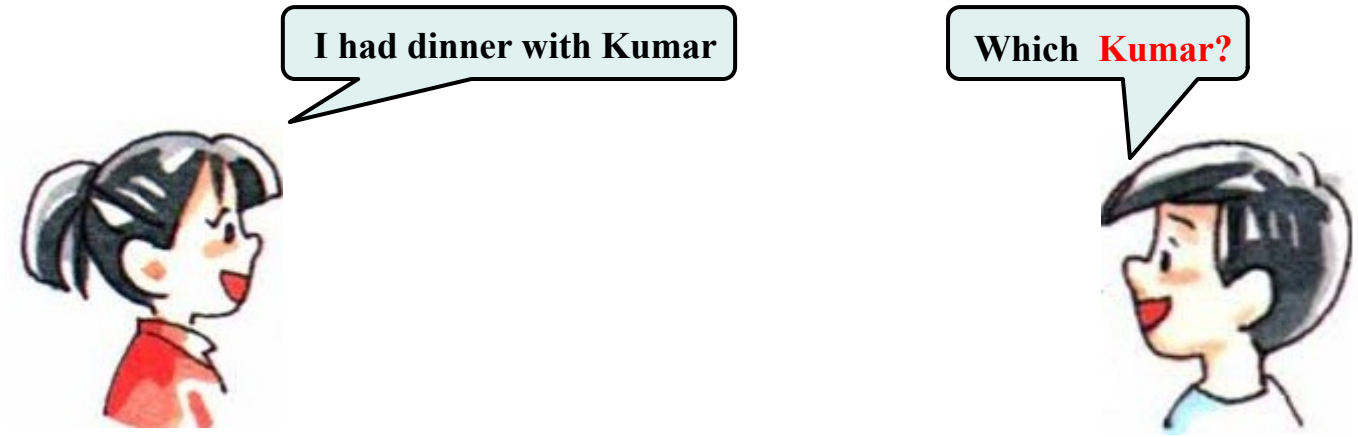
Why India doesn't qualify for the FIFA World Cup?



afnic | Labs

Importance of Identification in Communication


IoT Course .. Sandoche
Balakrichenan

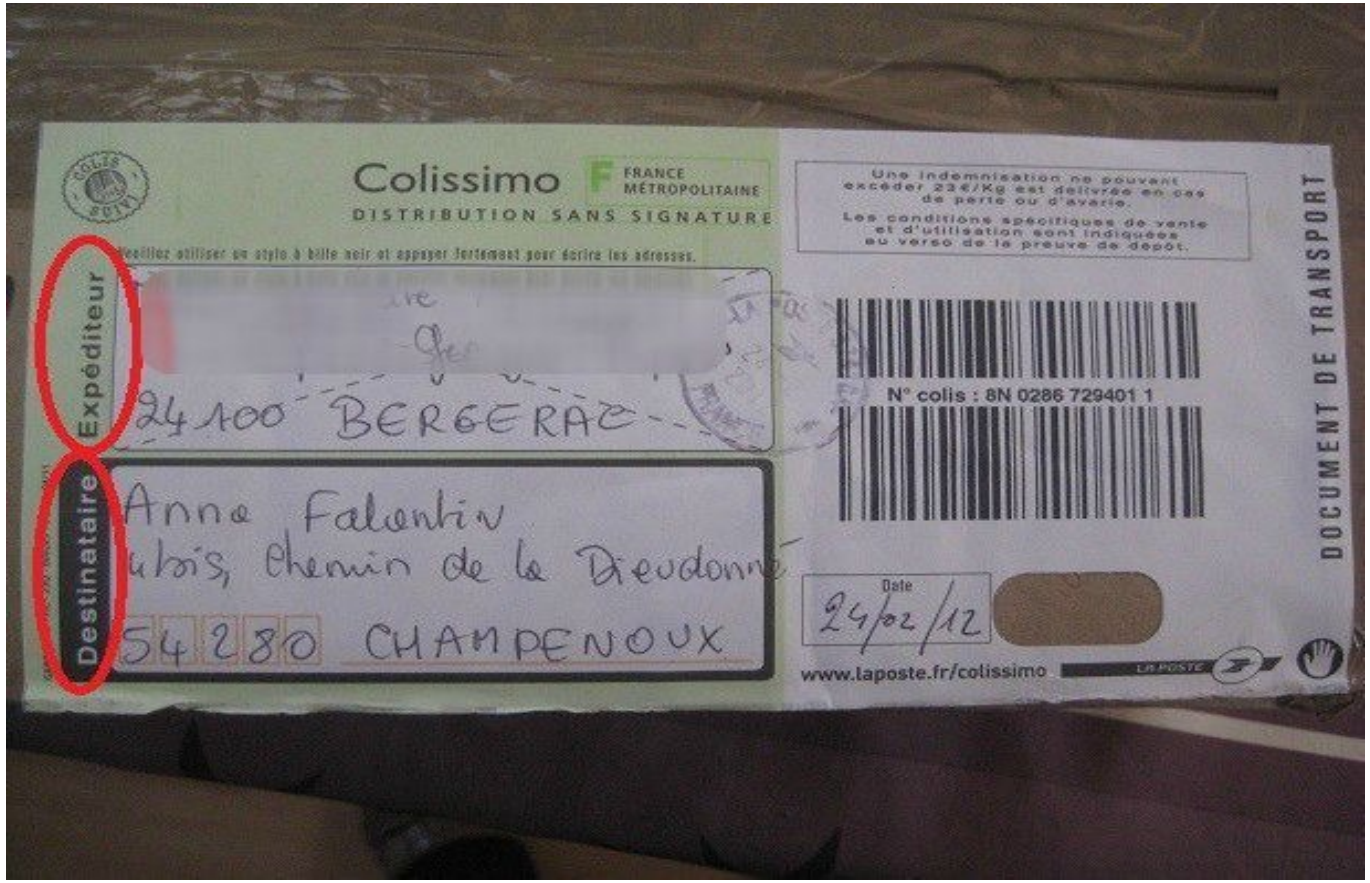

I had dinner with Kumar
Which Kumar?


CAUTION
THIS MACHINE
HAS NO BRAIN
USE YOUR OWN


Study the past if you would define the future.
Confucius
HISTORYHIT

afnic | Labs

Identity – Core for communication



Identifiers – PSTN and Mobile

00 33 1 40 00 00 00

+33 6 86 57 90 14

Identifiers in the Internet

- balakrichenan.fr, .இந்தியா

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

afnic | Labs

Need for Identifier Standardisation

afnic | Labs

John	Fitzgerald	Kennedy
First	Middle	Last
Given	Middle	Family
Fore-	Middle	Sur-





Shaikh = Title

Mohammad = Name

Bin = Son of

Rashed = Father's name

Al Maktoum = Surname/Family name or Tribe name

afnic | Labs

Format	Example
Name of recipient	Mr A. Payne
Company name	ARAMARK Ltd.
Street number, name	30 Commercial Road
City area/District	Fratton
City/Town/Village	PORTSMOUTH
County	Hampshire
Postal code	PO1 1AA
Country (in French or English)	UNITED KINGDOM

Format	Example
Name Son/Daughter Of (DO/SO) Or Husband/Wife Of (H/O or W/O)	*Ms Rajaram S/O Amirthalingam*
Door number:	*32-B*
Street Number, Street Name	*V.NAGAR, ROAD NO : 1*
VIA NAME (VIA)	*RASIPURAM*
Post Name (PO)	*RASIPURAM*
Taluk Name (TK)	*RASIPURAM*
Locality or Neighbourhood	*Near SAMUNDI THEATRE*
CITY - Postal Code (PIN)	*NAMAKKAL 637408*
District Name	*NAMAKKAL*
State	*TAMILNADU*
Country	*INDIA*

AmbilyRajan
Vallarkkottu House
East Marady P o
Muvattupuzha
Ernakulamdist
Pin:686673

afnic | Labs

IETF

- balakrichenan.fr, .இந்தியா
- 192.134.4.84, 2001:db8:85a3:8d3:1319:8a2e:370:7348

ITU-T (E.164)

00 33 1 40 00 00 00

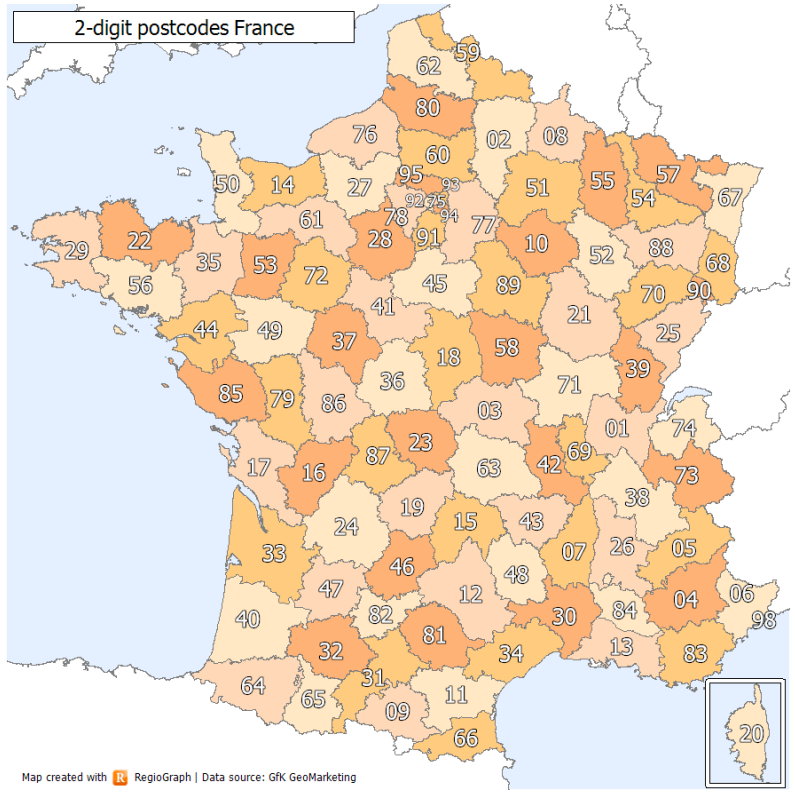
ITU-T (E.212)

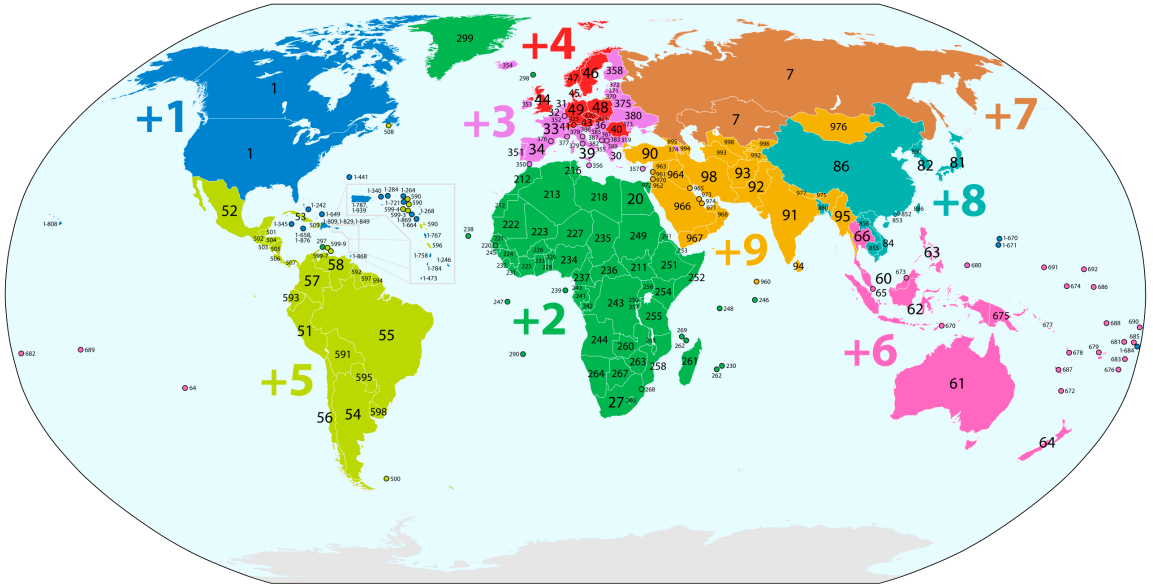
+33 6 86 57 90 14

afnic | Labs

Commonalities of different identifiers

Identifiers - Hierarchical





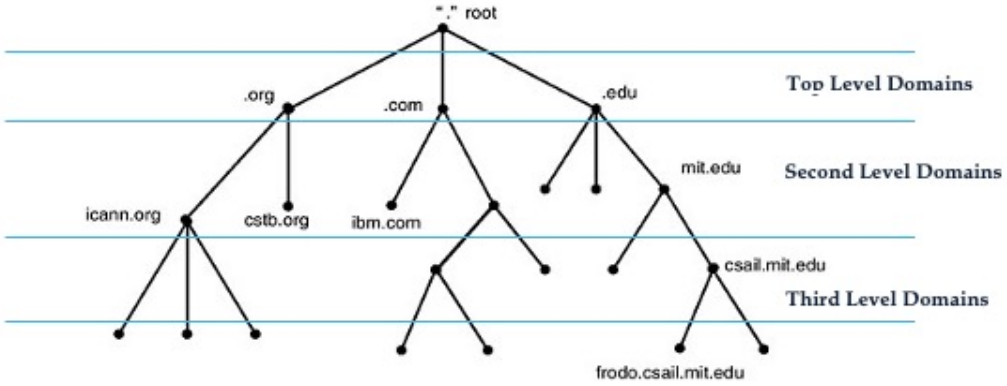
33

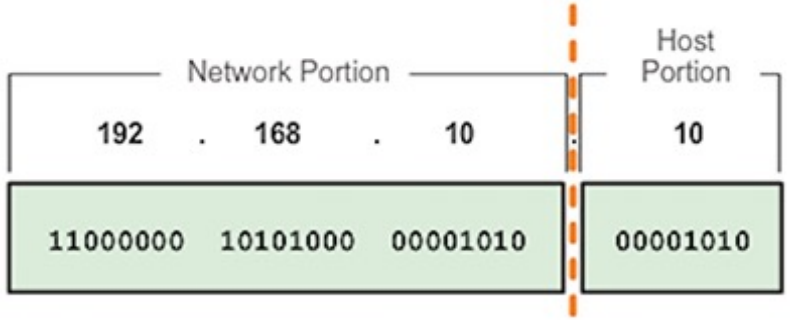
1

39654200

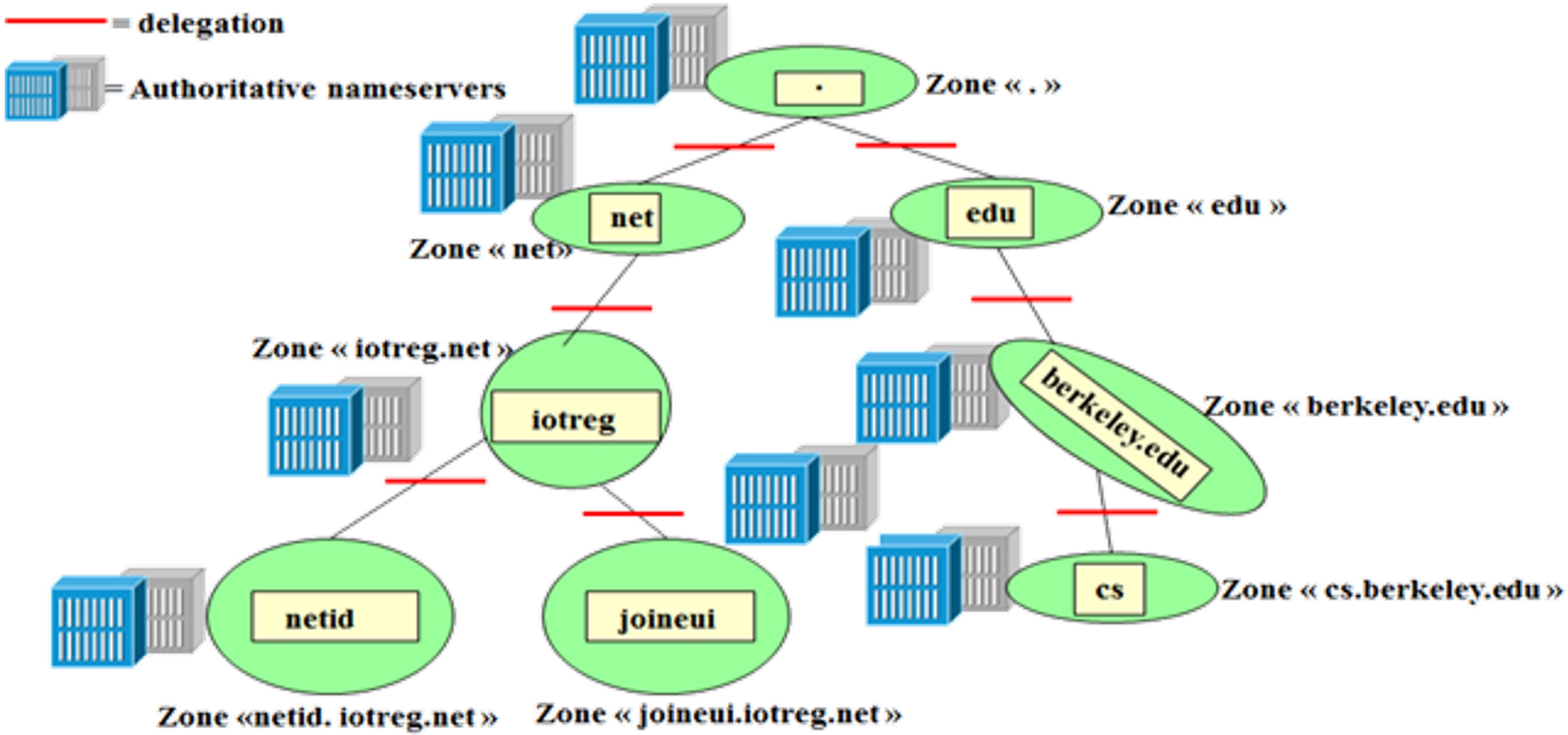


Identifiers - Hierarchical



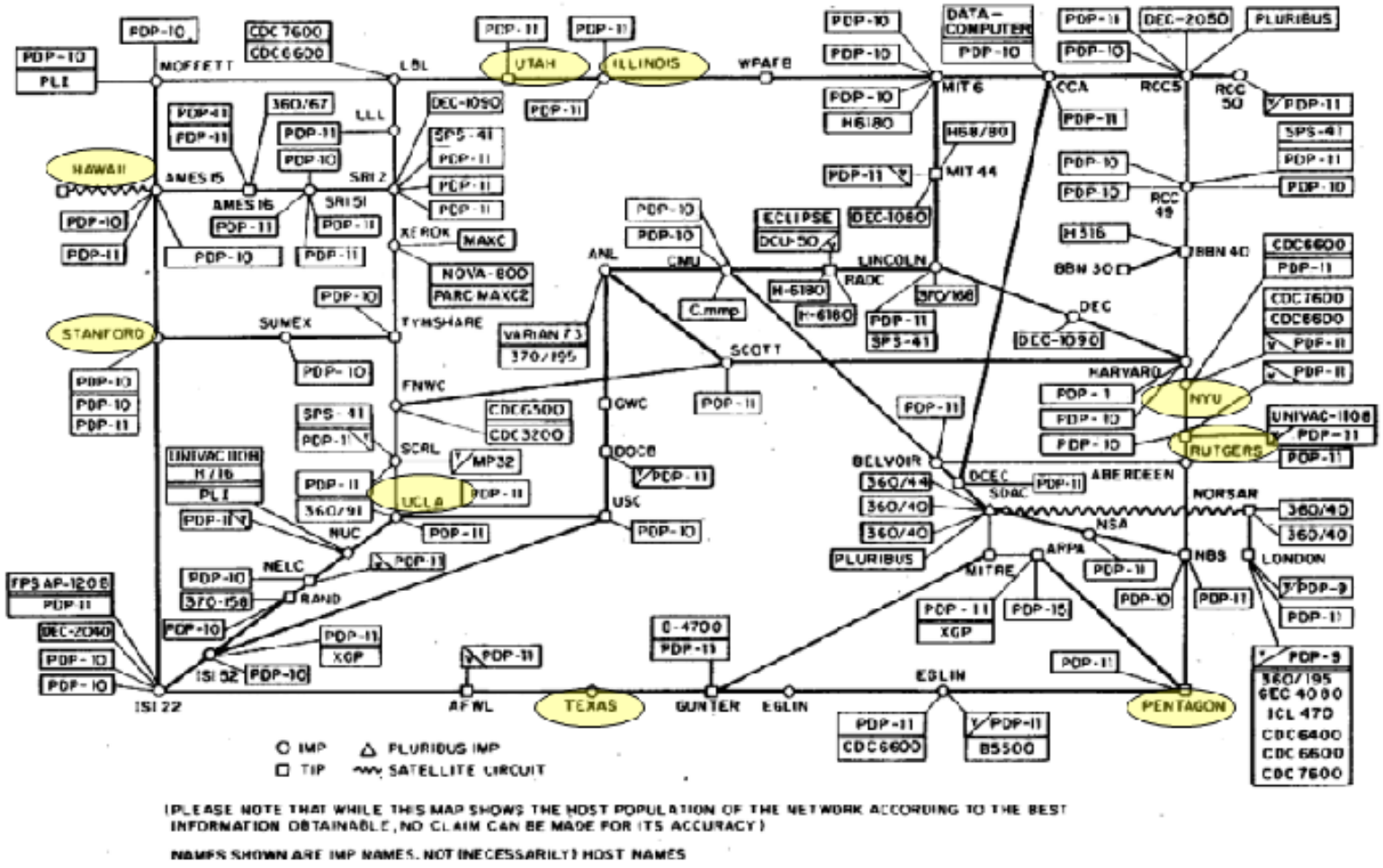


Identifiers – Distributed Database & management



afnic | Labs

Identifiers – Distributed Database & management



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

Accessing the Internet domain name database - *Resolution*

VeriSign: 48 Billion DNS Queries A Day

Google Public DNS receives 70 billion queries per day

Cloudflare handles 86 **billion DNS queries per day**, a

Three steps to resolve an Identifier in the Internet

1. Naming Conventions

IETF is the SDO

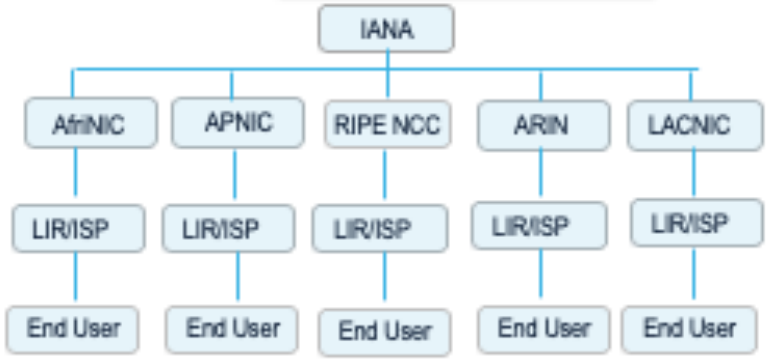
- Domain names, URI
- IP Addresses (IPv4/IPv6)

2. Provisioning

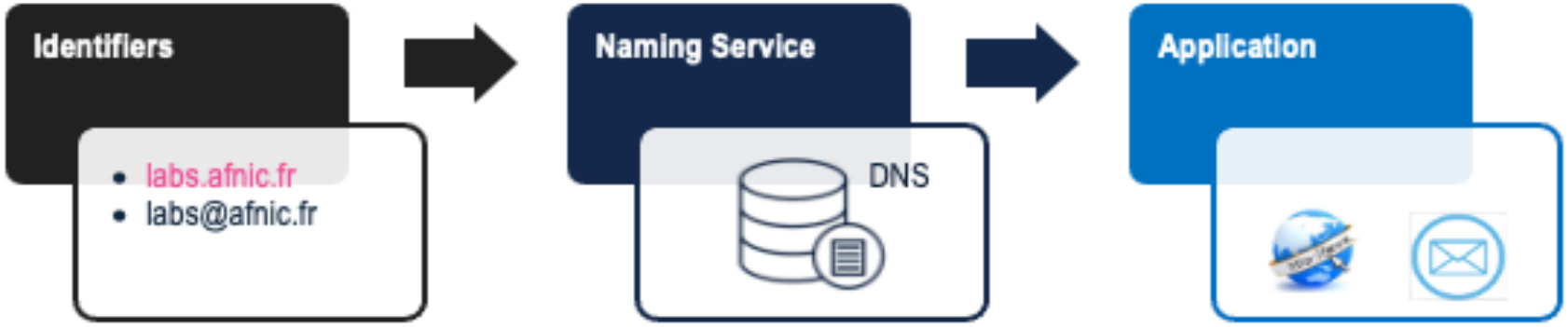
2.1. Domain registry



2.2 Internet number registry



3. Resolution



Three steps to resolve an Identifier in the Internet

1. Naming Conventions

IETF is the SDO

RFC 1034

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

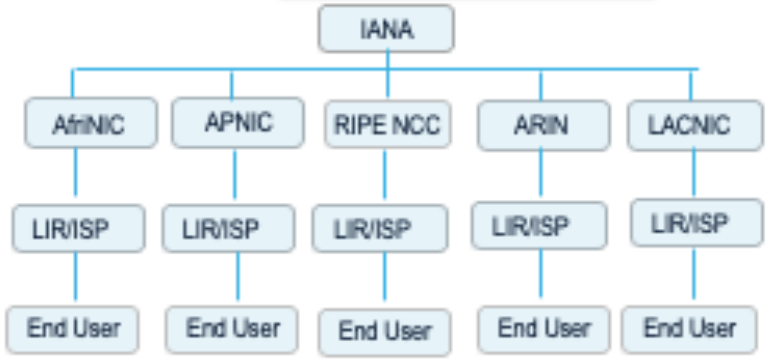
RFC 791, 4291

2. Provisioning

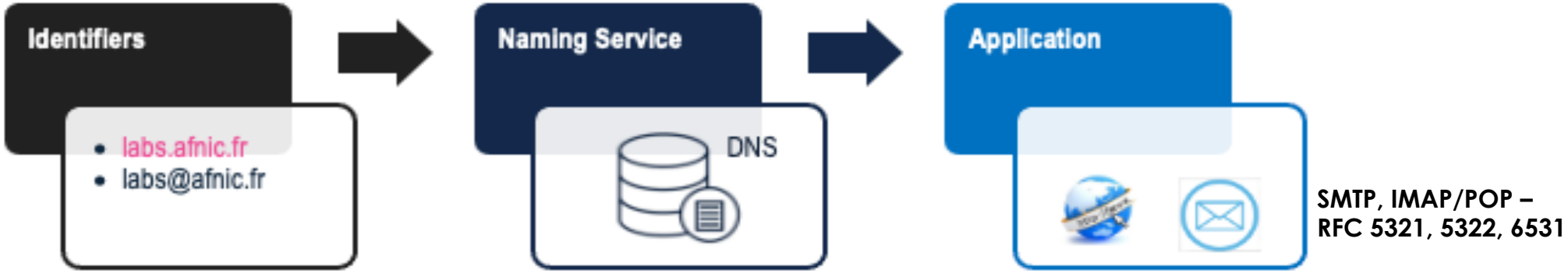
2.1. Domain registry



2.2 Internet number registry



3. Resolution

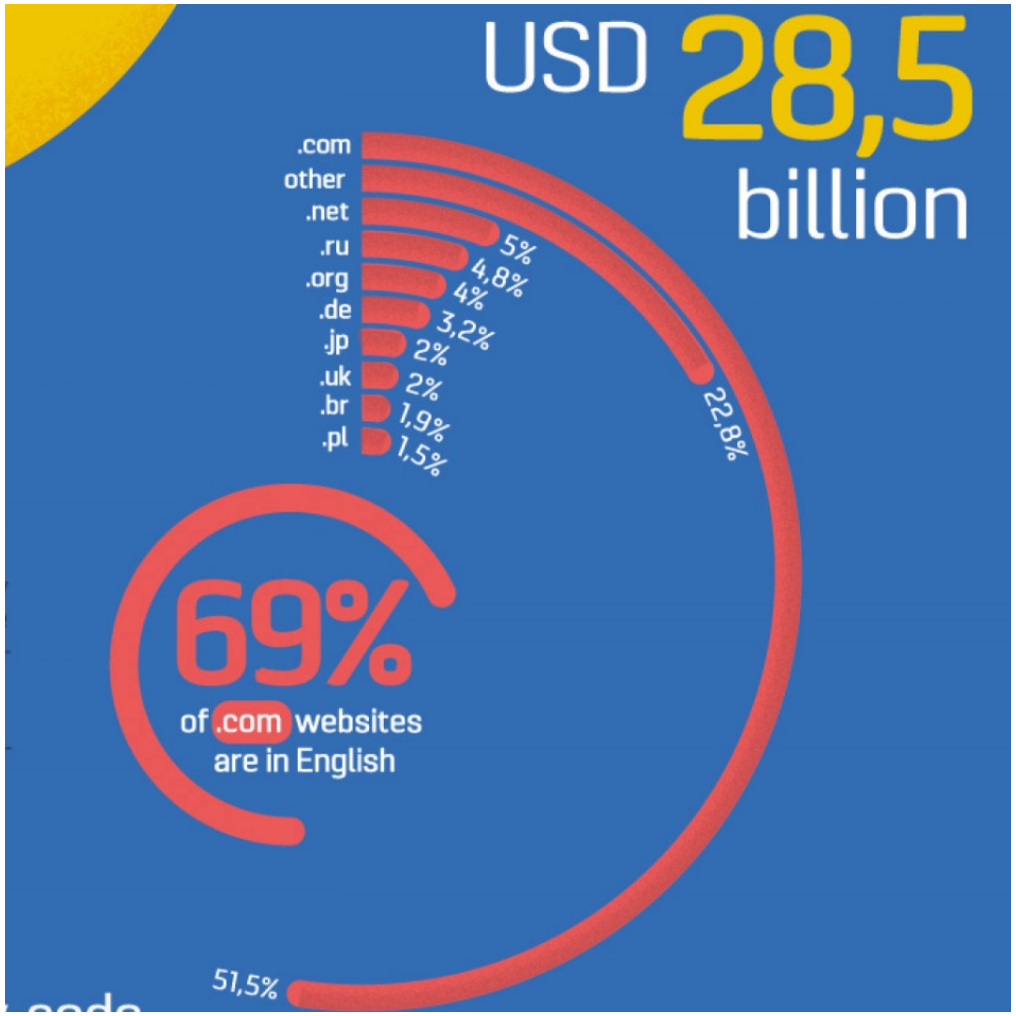


DNS – RFC 1034, 1035

HTTP – RFC 2616

SMTP, IMAP/POP – RFC 5321, 5322, 6531

The TLD Identity management market



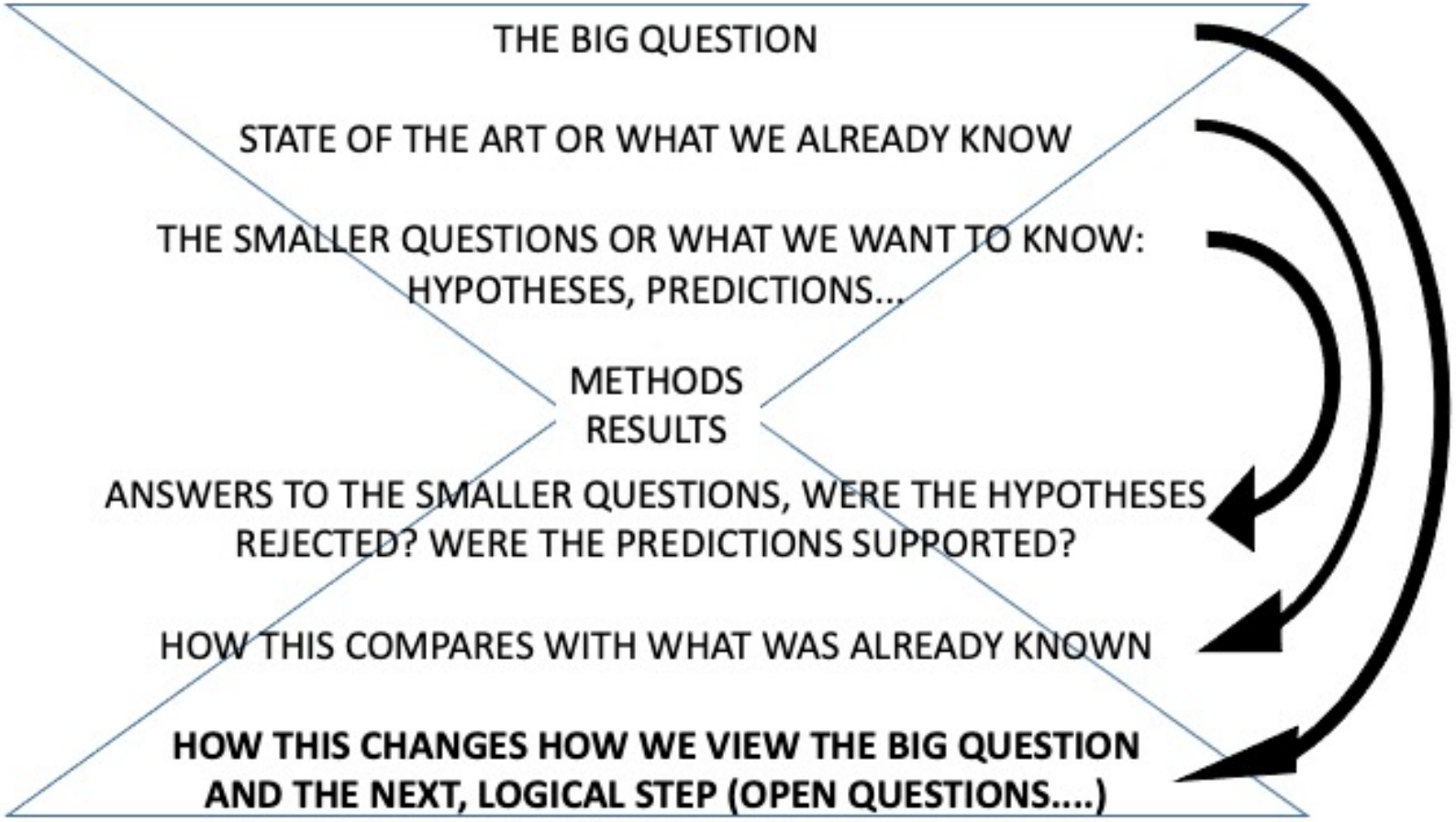
afnic | Labs


Internet Ecosystem
Naming and Addressing
ICANN
IANA/PTI
RIRs
gTLDs
ccTLDs
Local, National, Regional, and Global Policy Development
Governments
Intergovernmental Organizations
Businesses
Internet Society
Chapters, Individual Members, Organization Members, and Special Interest Groups (SIGs)
Other Policy Discussion Forums
Education and Capacity Building
Governments
Internet Community Organizations, Businesses, and Initiatives
Multilateral Development Banks and International Financial Institutions
Universities, Academic Institutions, and National Research and Education Networks (NRENs)
Internet Society
Chapters, Individual Members, Organization Members, and Special Interest Groups (SIGs)
Users
Civil Society
Organizations
Individuals
Governments
Service Creators and Vendors
Shared Global Services and Operations
Root Servers
Network Operations
Internet Exchange Points (IXP)
Service Creators and Vendors
gTLDs
ccTLDs
Open Standards Developments
ITU-T
Specialized Standards Bodies
Internet Society Affiliated Organizations
IETF, IAB, and IRTF
W3C

afnic | Labs

Takeaway

- Past defines the future
- Delegation is pivotal for scaling

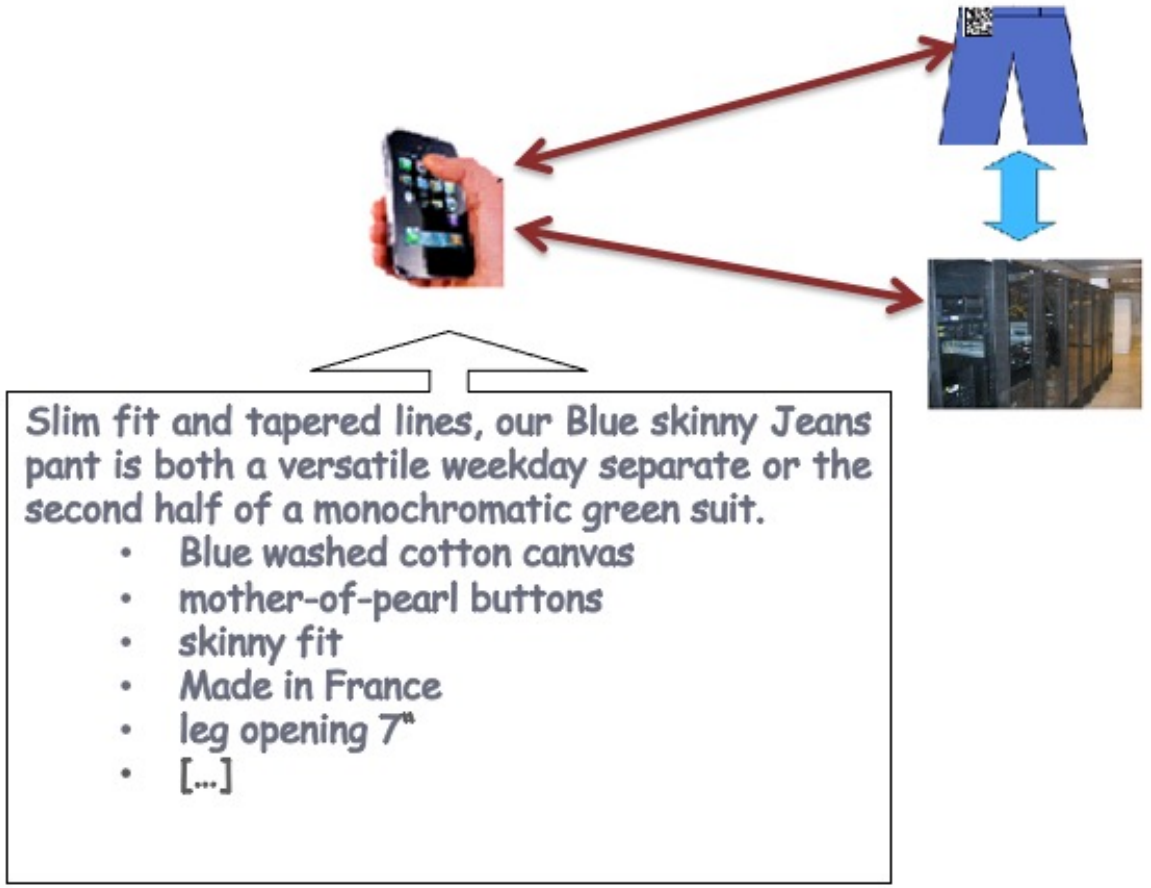

THE BIG QUESTION
STATE OF THE ART OR WHAT WE ALREADY KNOW
THE SMALLER QUESTIONS OR WHAT WE WANT TO KNOW:
HYPOTHESES, PREDICTIONS...
METHODS
RESULTS
ANSWERS TO THE SMALLER QUESTIONS, WERE THE HYPOTHESES
REJECTED? WERE THE PREDICTIONS SUPPORTED?
HOW THIS COMPARES WITH WHAT WAS ALREADY KNOWN
HOW THIS CHANGES HOW WE VIEW THE BIG QUESTION
AND THE NEXT, LOGICAL STEP (OPEN QUESTIONS....)

afnic | Labs

Industry – Use Case

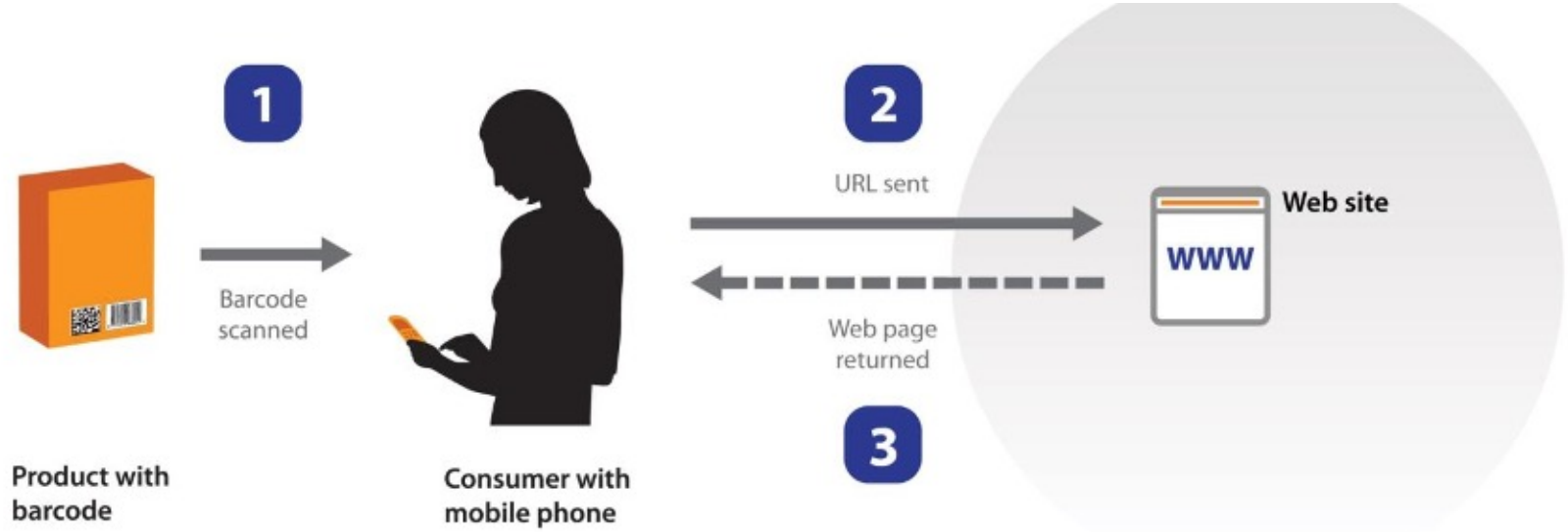
afnic | Labs

Extended Packaging



afnic | Labs

Direct mode resolution



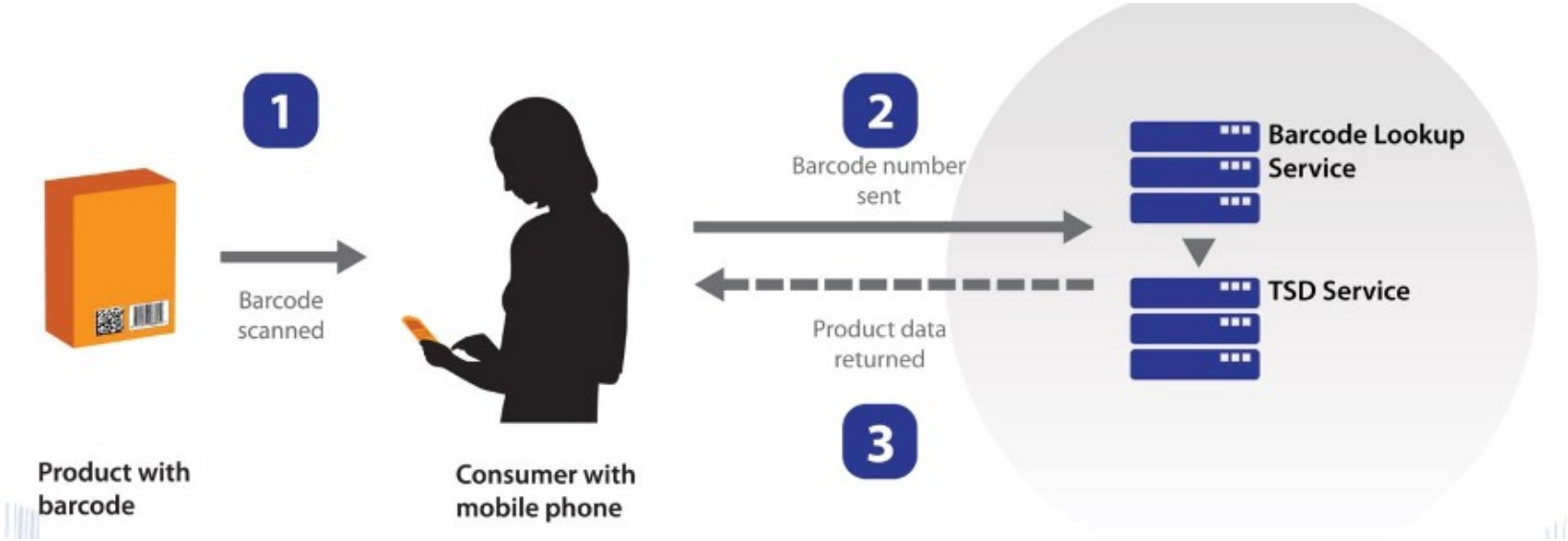
http://www.proxiproduit.fr/0950700000001118200

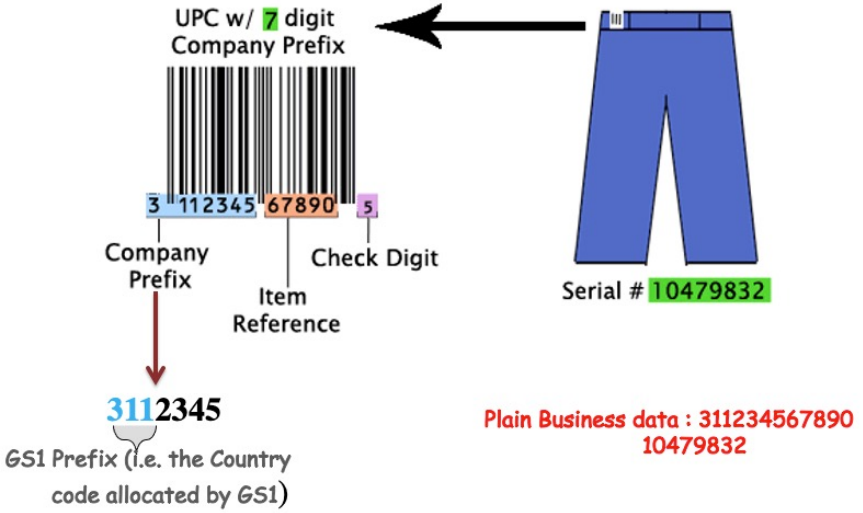
afnic | Labs


Evernote
iTunes
Chanel
Huffin...Post
RjDj Album
Pageonce
Poll Tracker
nyc weather
SGN Golf
LiveView
Air Mouse
Shopper
tvChatter
Things
Stocks
Things
LiveView
Yahoo!
colorendar
Quordy
Flickr
Remote
Calculator

afnic | Labs

Indirect resolution





Plain Business data : 311234567890 (GTIN)
10479832 (Serial Number)



GS1 DataMatrix Bar Code containing GS1 Element String

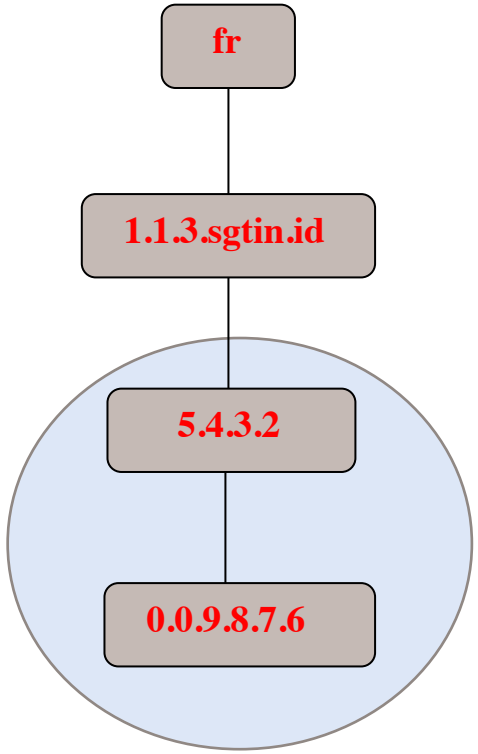
(01)311234567890(21)10479832



RFID Tag containing EPC Binary Encoding

(3014BDF664A3F480009FE8D8)

Provisioning in the DNS

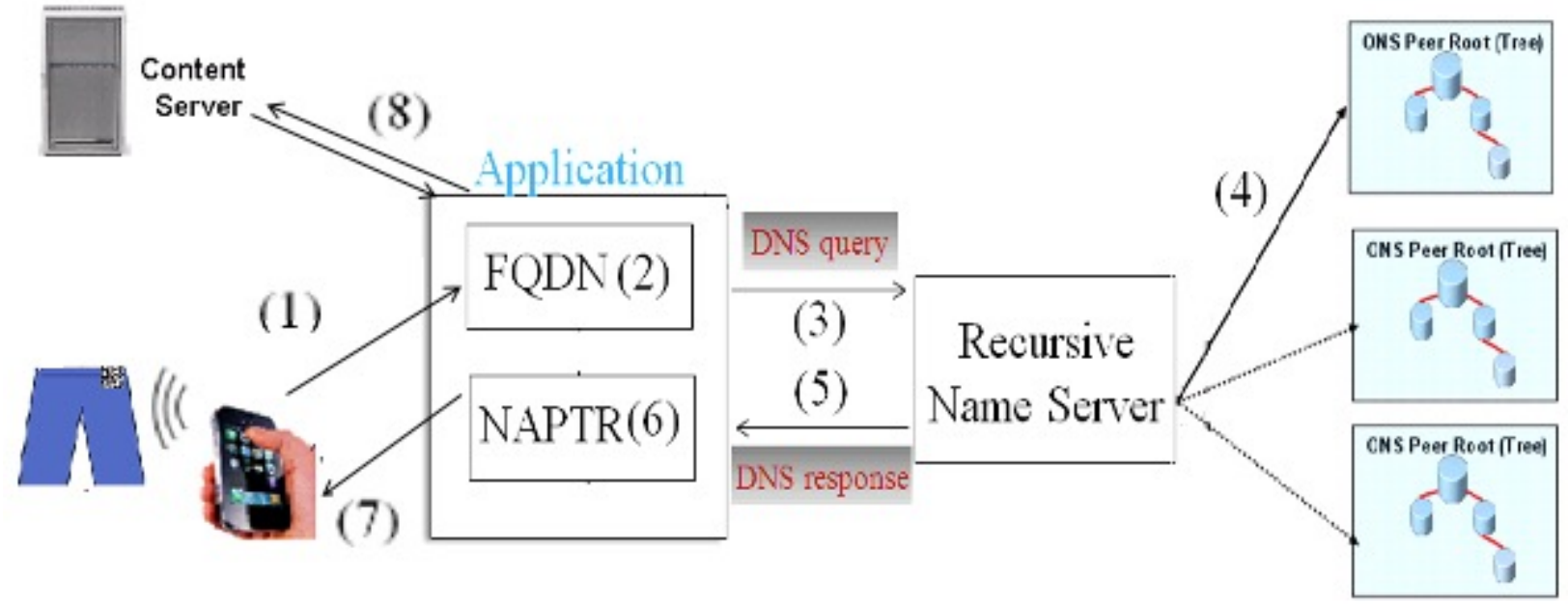


0.0.9.8.7.6.5.4.3.2.1.1.3.sgtin.id.fr

IN NAPTR 0 0 "u" EPC+http "!^it\.*$!http://example.com/italian!" .

IN NAPTR 0 0 "u" EPC+http "!^fr\.*$!http://example.com/french!" .

IN NAPTR 1 0 "u" EPC+DS "!^*$!http://example.com/discoveryservice!" .



FQDN : Fully Qualified Domain Name

NAPTR : Name Authority Pointer (a DNS Resource Record type like A,MX etc.)

Dynamic Delegation Delivery System - RFC 3401, 3402, 3403

afnic | Labs



Document Summary

Document Item	Current Value
Document Title	Draft Standard Specification GS1 Object Name Service (ONS)
Date Last Modified	December 20 , 2012
Document Issue	Issue 1 of Ratified Standard
Document Status	Ratified Standard
Document Description	

Contributors

Name (& Notable Role)	Organization
Sandoche Balakrichenan-- Conformance Requirements Editor and Prototype Test Participant	AFNIC
Mark Harrison	Auto-ID Labs
Philippe Gautier	Business2Any

afnic | Labs

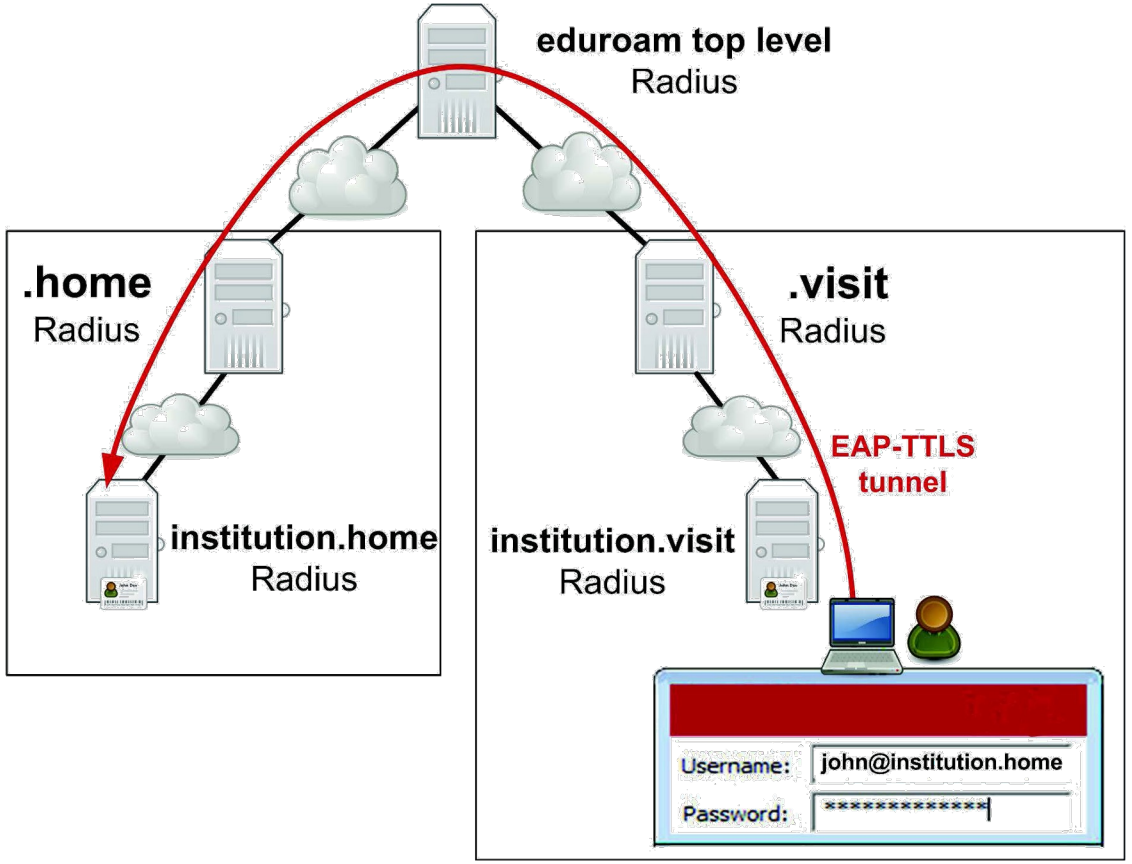
Takeaway

- Long lasting design is Good design
- No need to reinvent the wheel
- Liaison between different Standards organisation

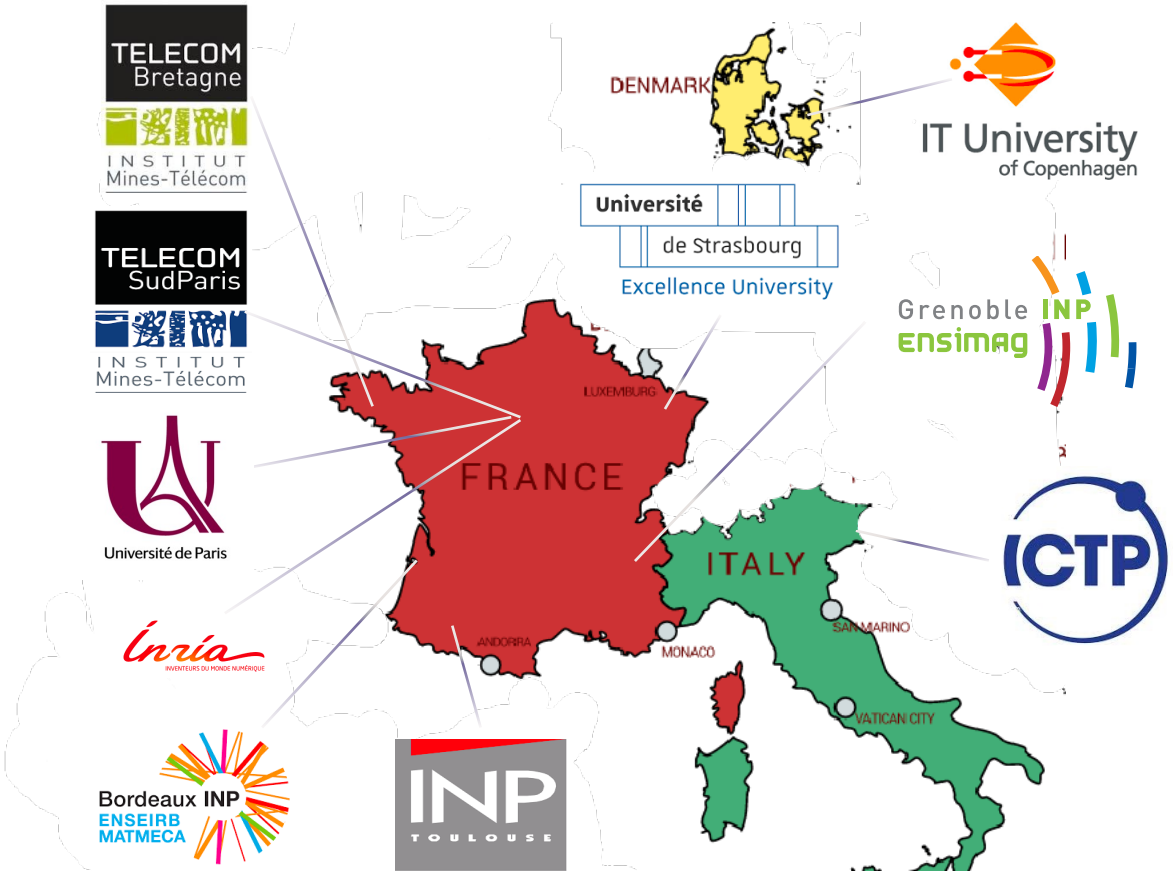
afnic | Labs

Academia – Use Case

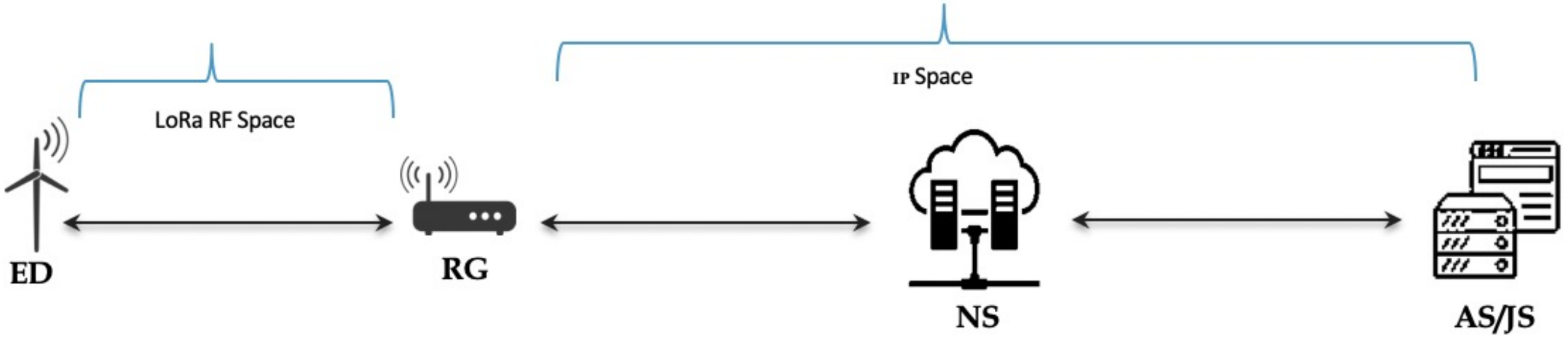
Eduroam example



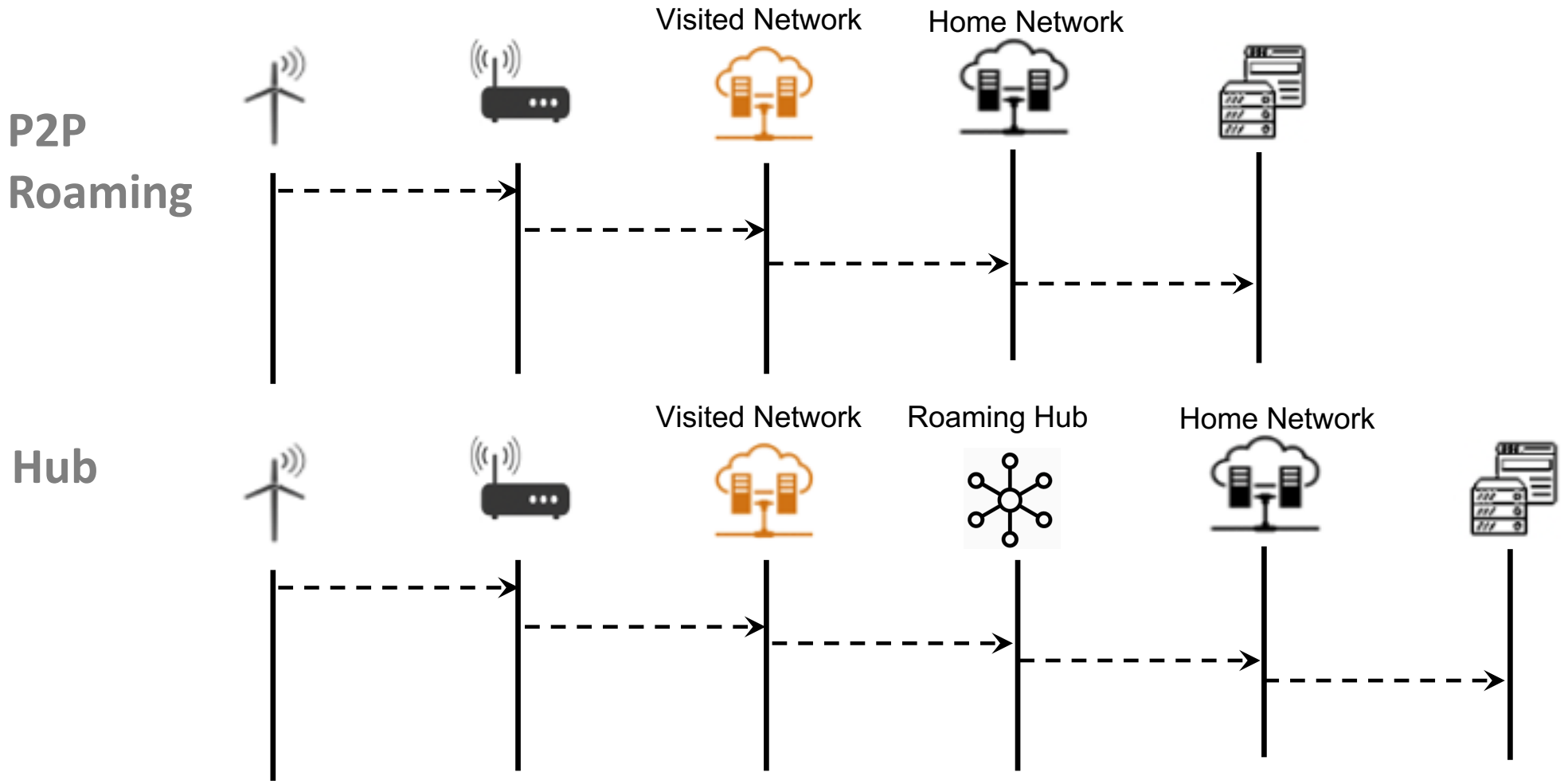
Institutions who have expressed Interest for IoTRoam



LoRaWAN Architecture – RF & IP Space



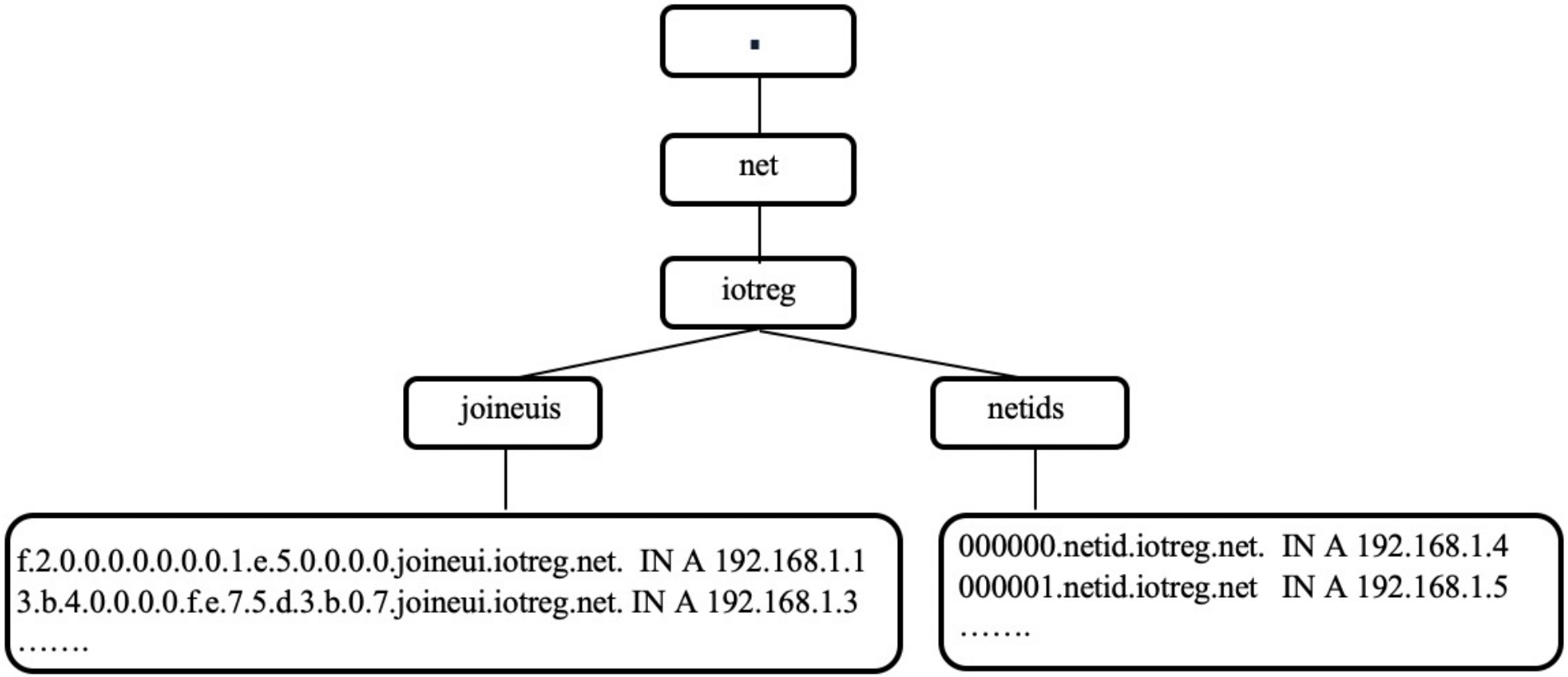
LoRaWAN existing Roaming possibilities – P2P & Hub



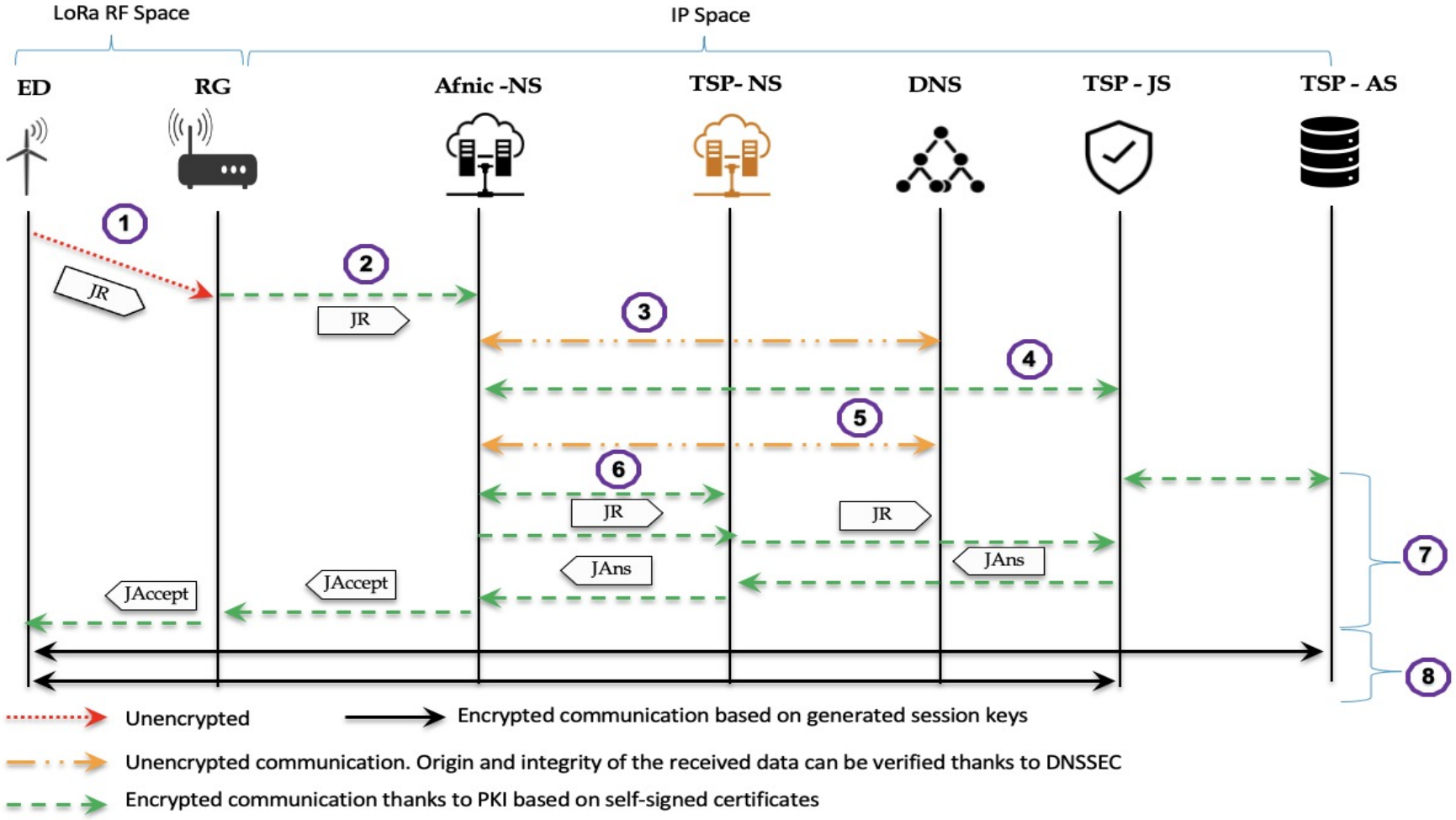
Issues – Required Configuration Parameters for roaming

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

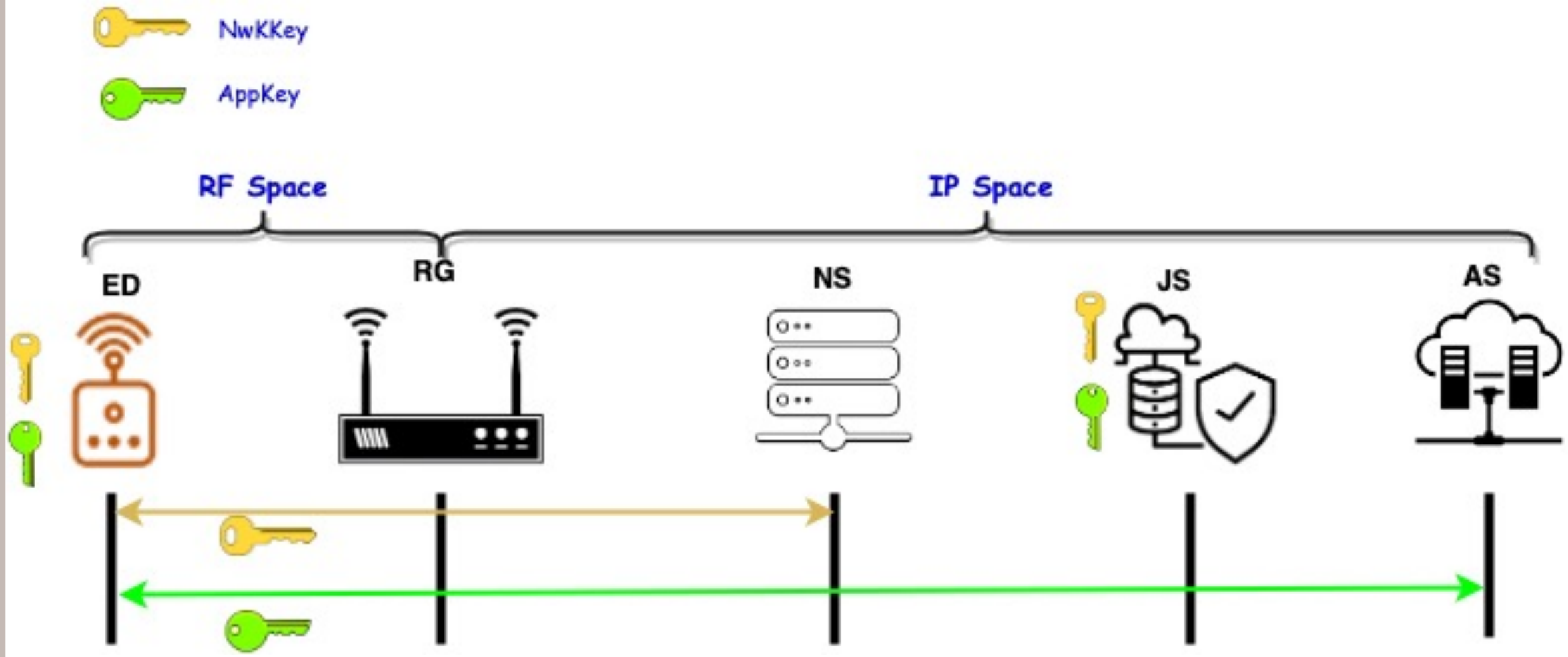
Dynamic discovery – Using DNS for roaming



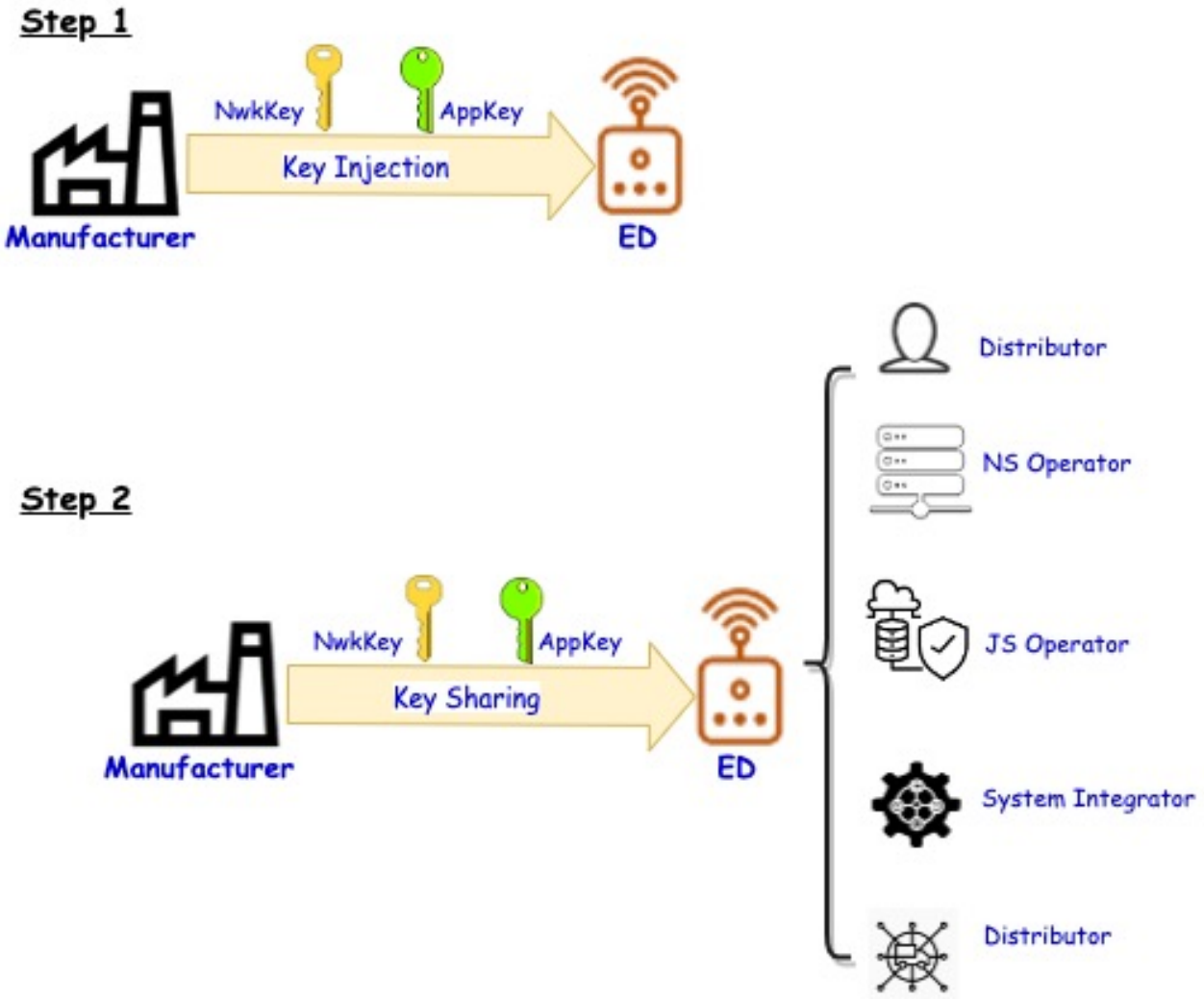
Passive Roaming message flow



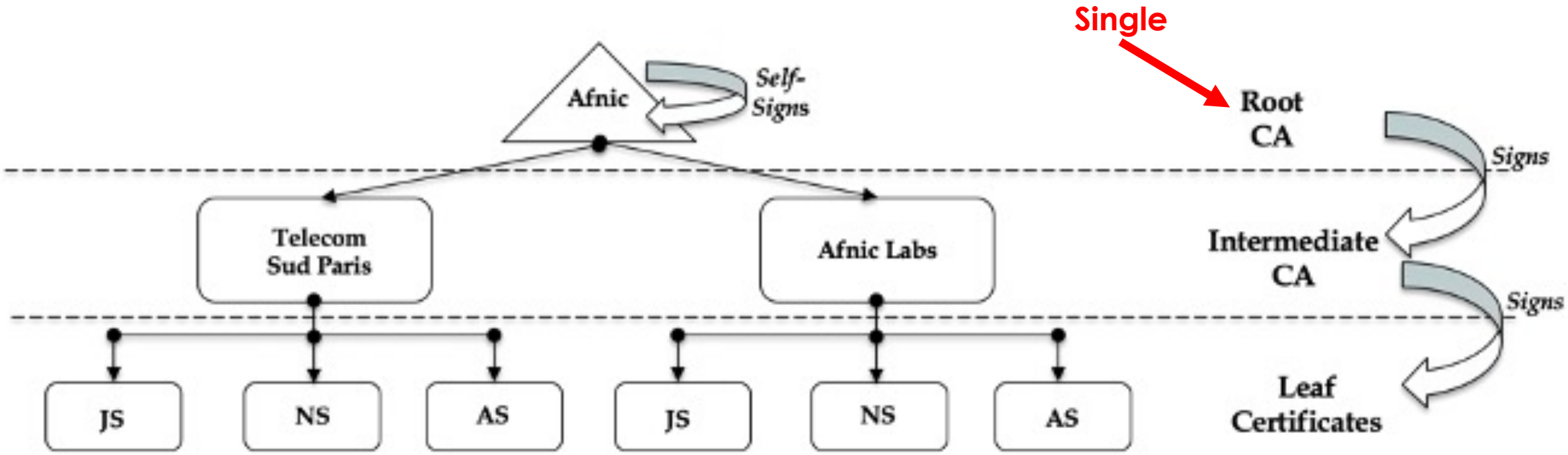
Secured IoT communication – LoRaWAN example



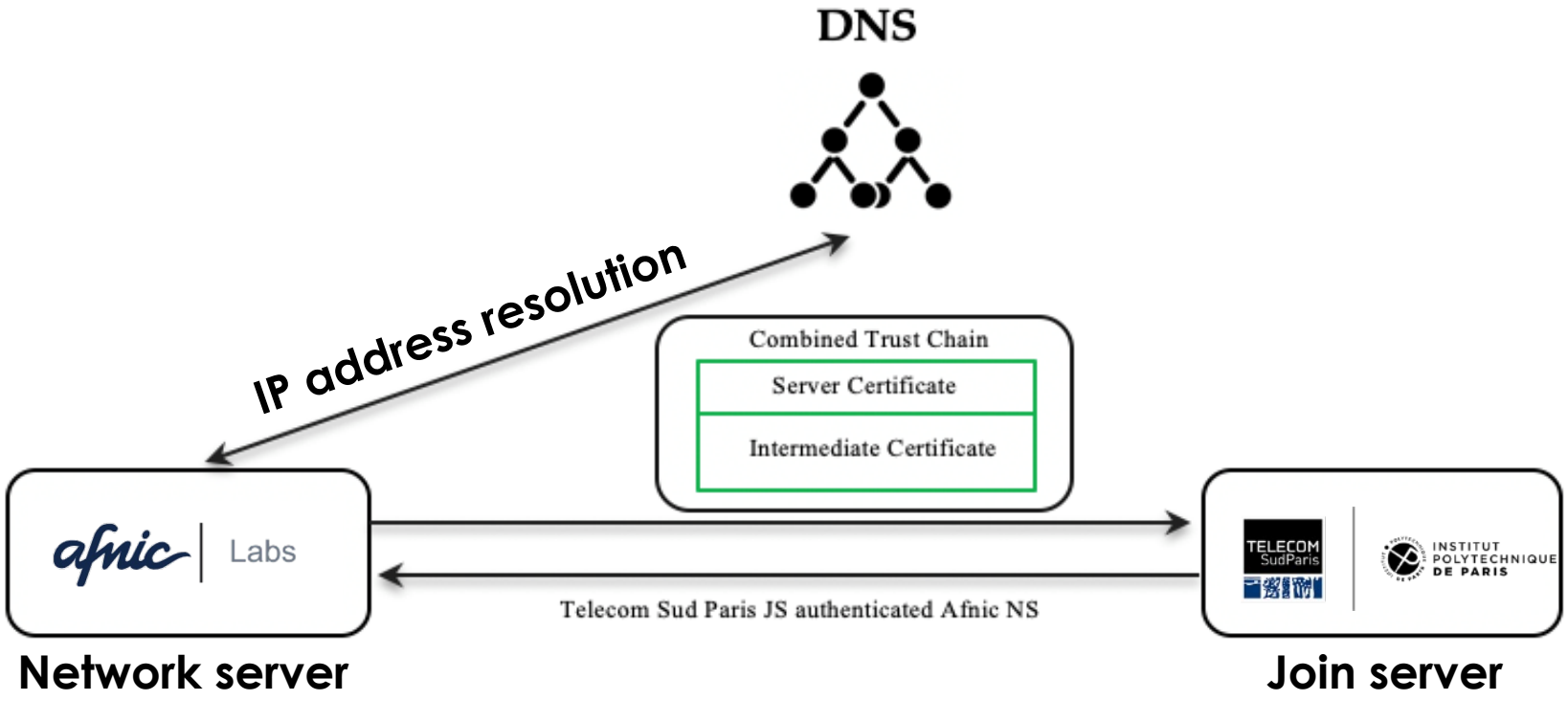
Issues with the current security system in IoT (1/2)



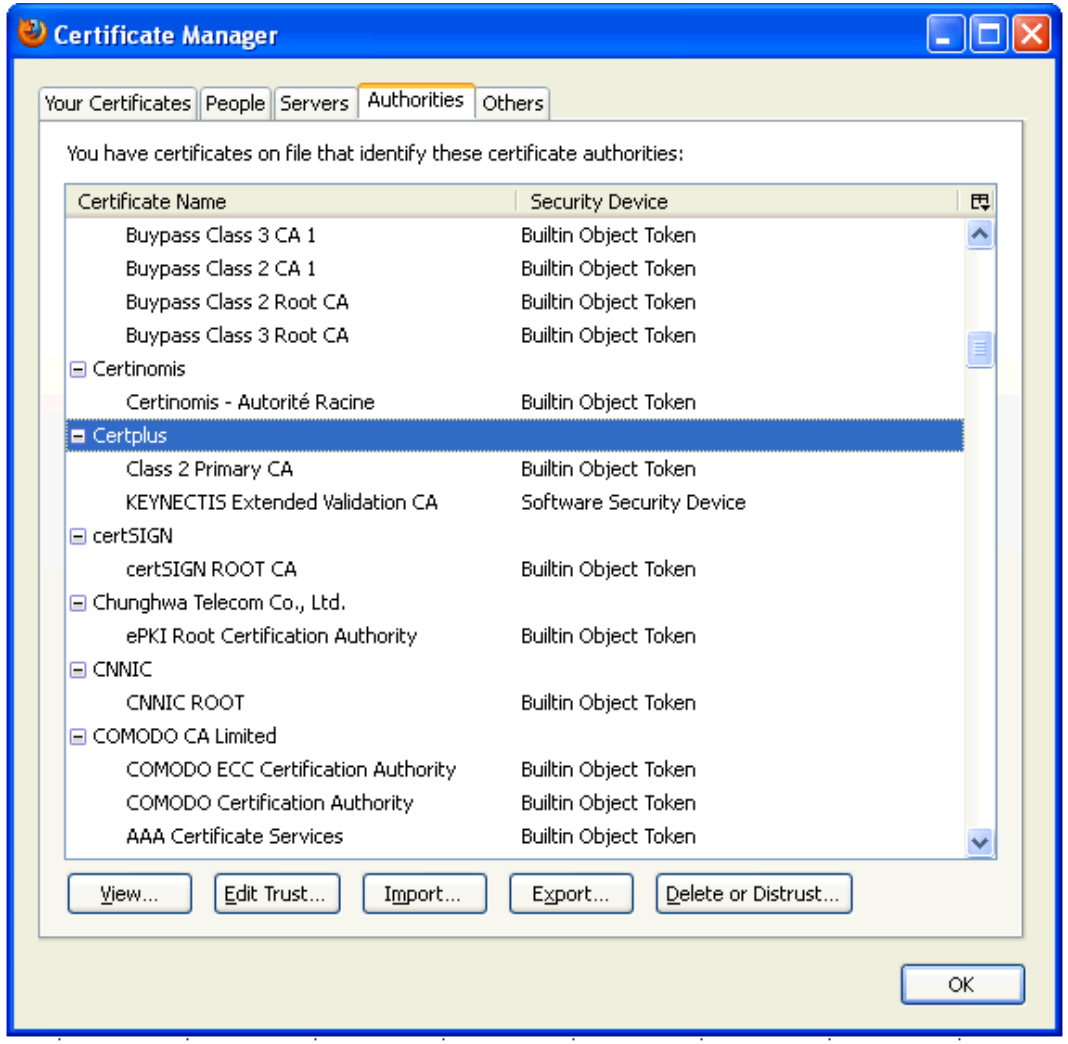
Using DNS based PKI in an IoT Roaming Scenario – Certificate Provisioning based on a single private PKI



Using DNS based PKI in an IoT Roaming Scenario – Certificate Validation

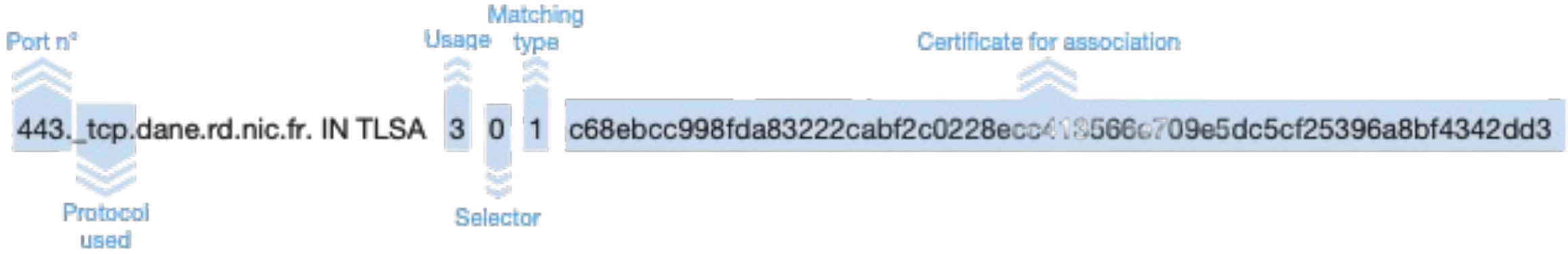


PKI using DNS – DANE Primer (1/2)





PKI using DNS – DANE Primer (2/2)



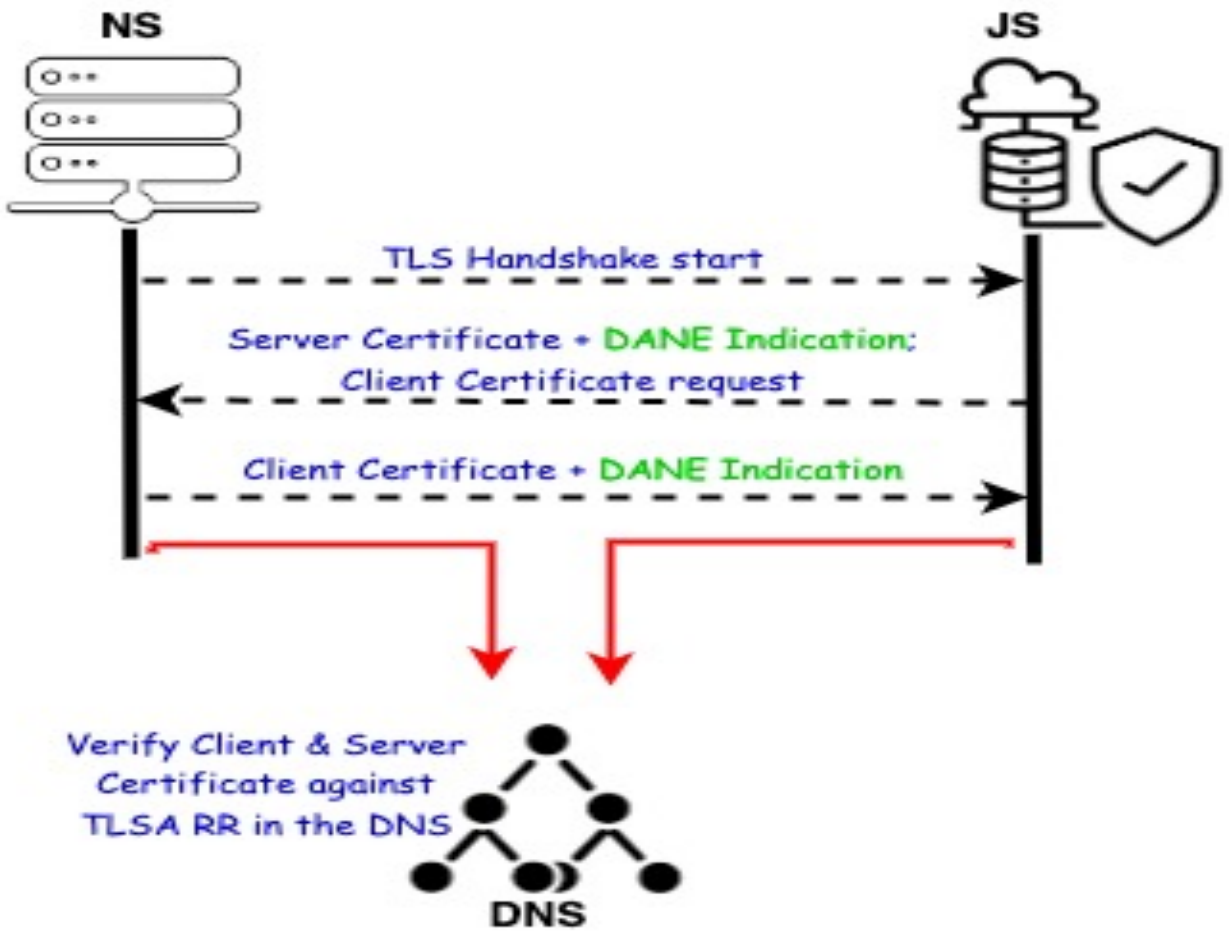
Using DANE indication Client/Server Authentication – Federated CA's

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



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

Issues with the current security system in IoT – 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**

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

Afnic's Vision

DONE

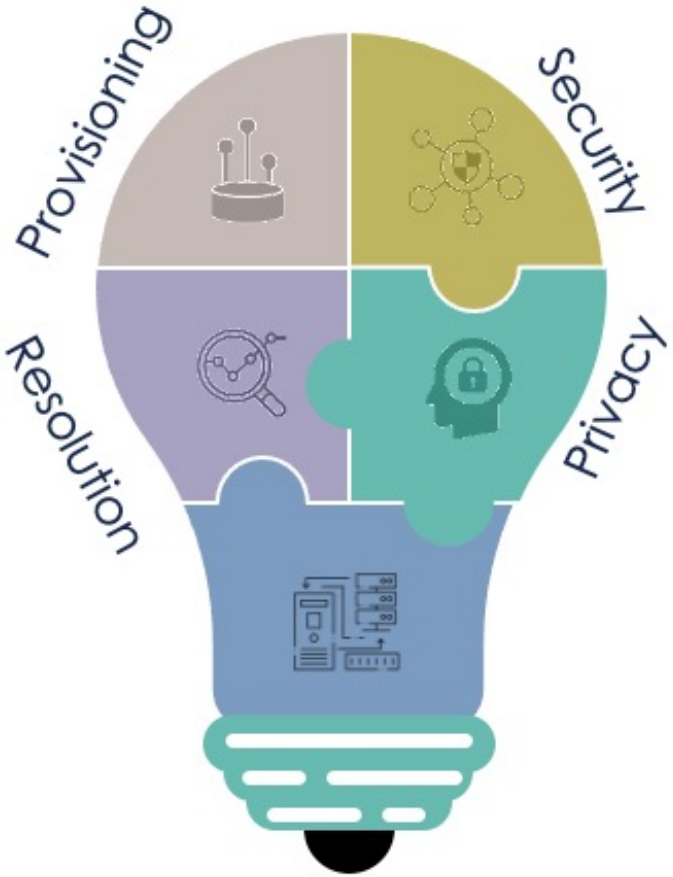
WINGS

Widening interoperability for networking Global supply Chains

DONE

LoRa Alliance

DNS Service



ONGOING

DINS*

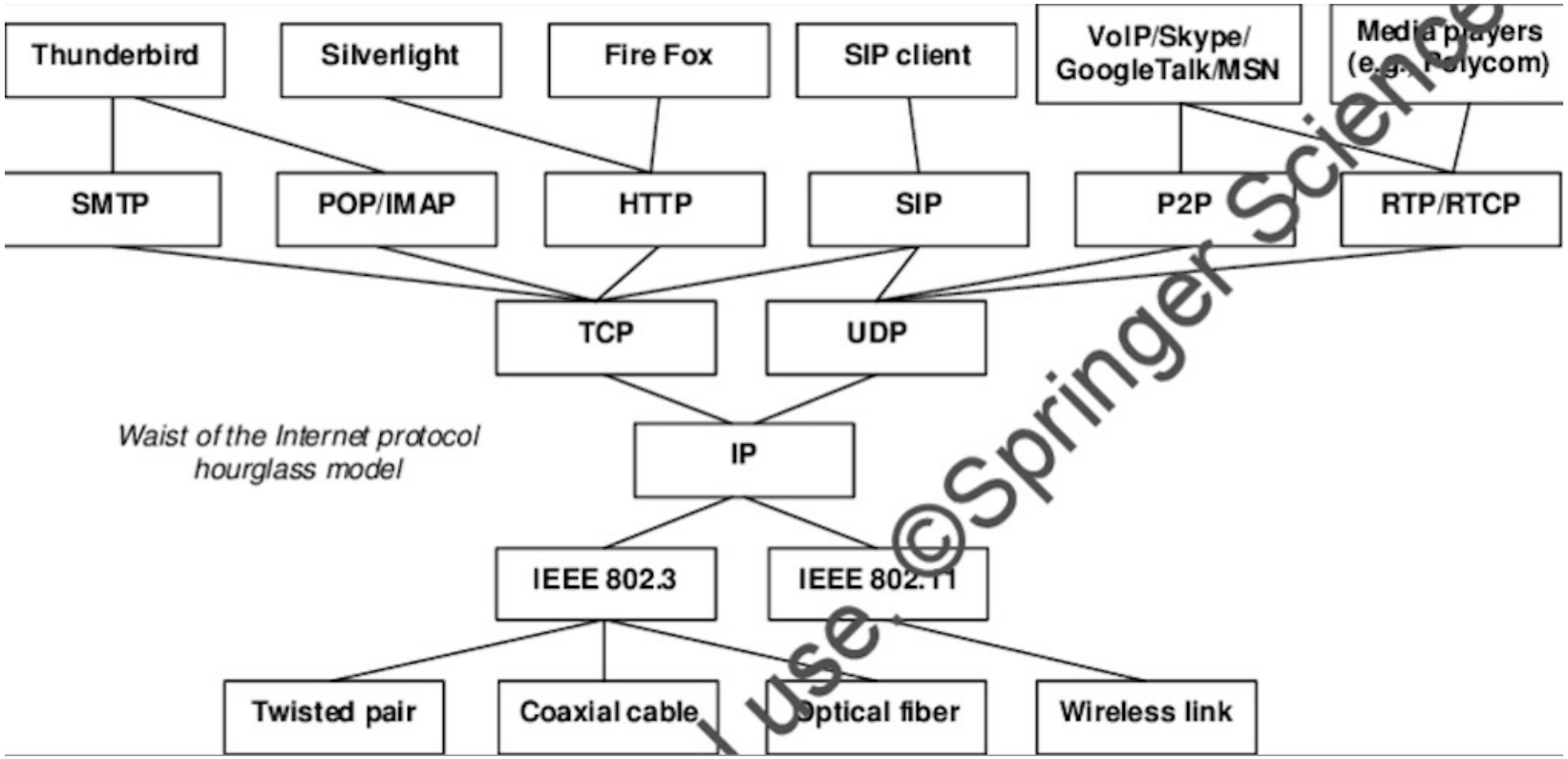
DNS Naming and Services for Secure Seamless IoT

ONGOING

PIVOT*

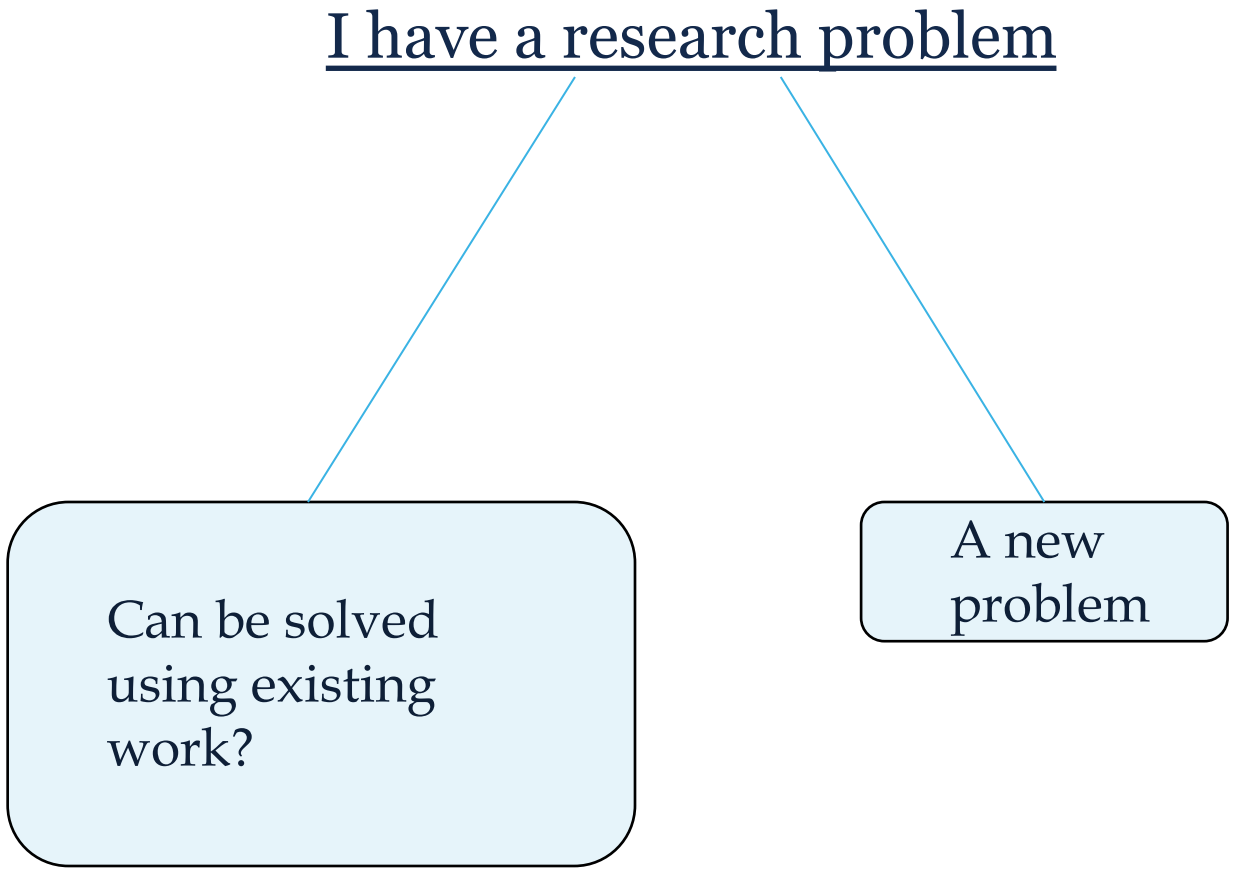
Privacy-Integrated design and Validation in the constrained IoT

How can I be part of a SDO



Waist of the Internet protocol hourglass model

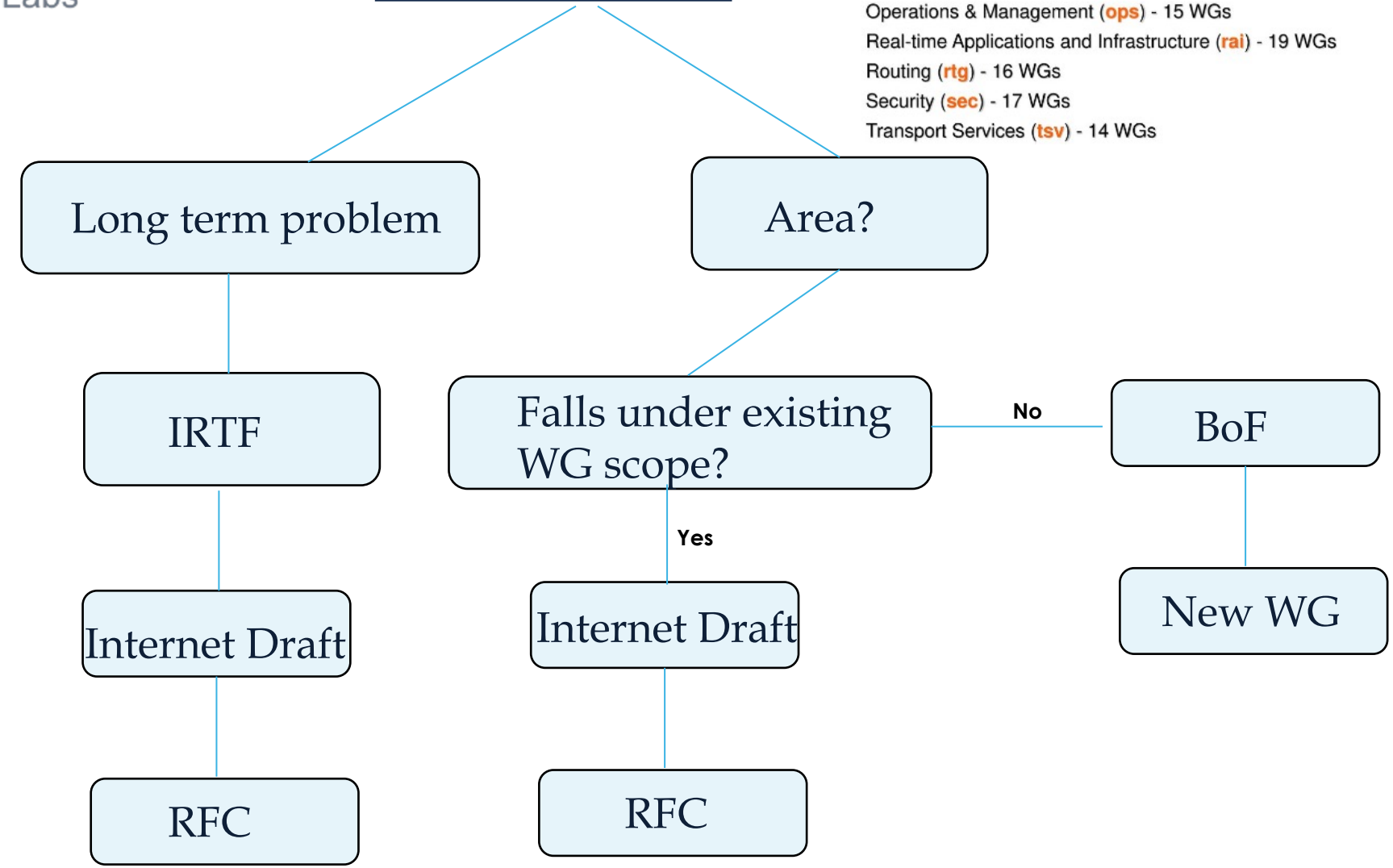
Personal use ©Springer Science


I have a research problem
Can be solved using existing work?
A new problem

afnic | Labs

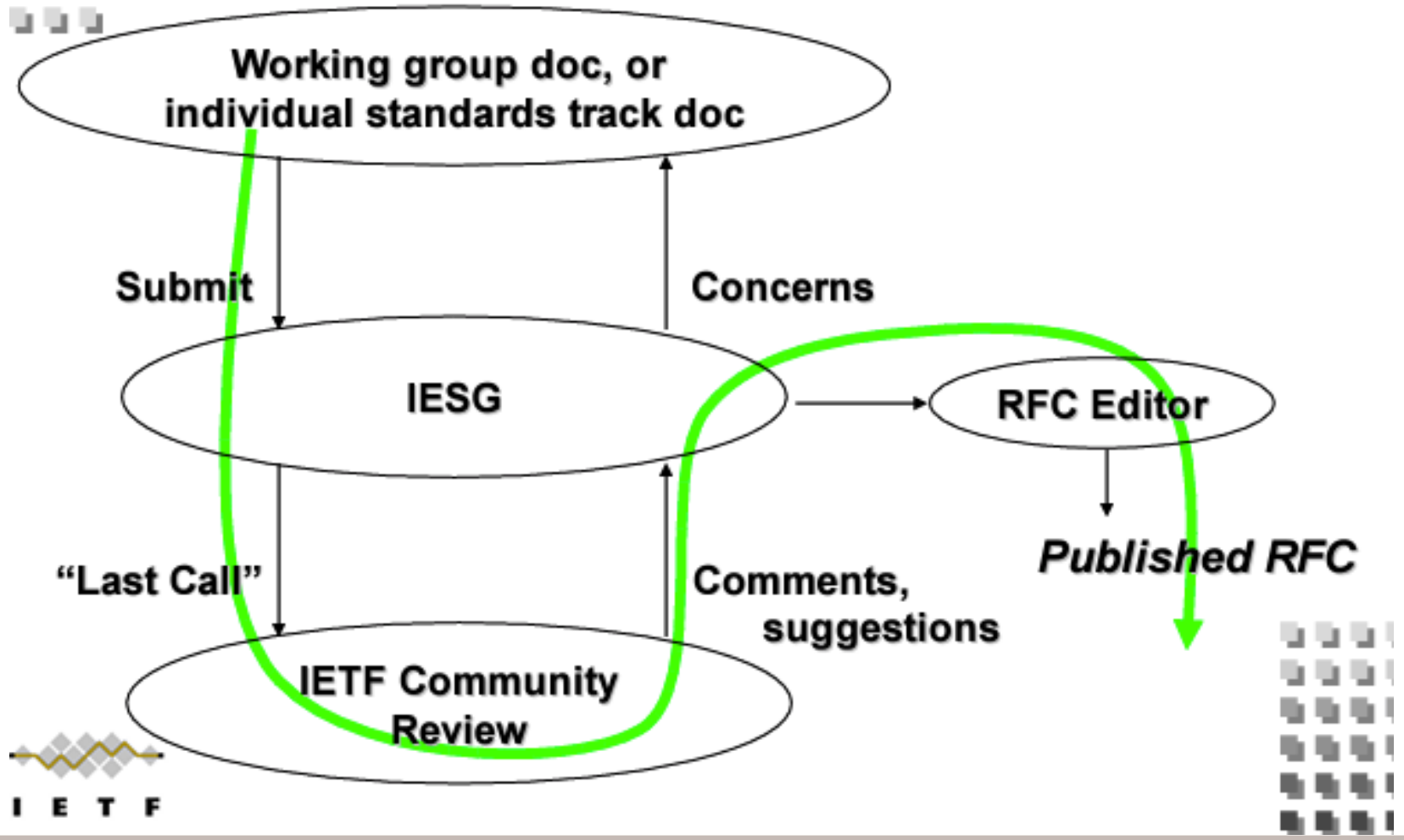
A New Problem

Applications (app) - 15 WGs
Internet (int) - 28 WGs
Operations & Management (ops) - 15 WGs
Real-time Applications and Infrastructure (rai) - 19 WGs
Routing (rtg) - 16 WGs
Security (sec) - 17 WGs
Transport Services (tsv) - 14 WGs



afnic | Labs

IETF Submission




WE REJECT: KINGS,
PRESIDENTS AND VOTING.
WE BELIEVE IN:
ROUGH CONSENSUS
AND RUNNING CODE.
IETF 83

What next?

- *join mailing lists*
  - *this is where the work happens*
- *read the drafts*
- *don't be shy*
- *talk to people*
- *look for common ground*
- *help people*
- *don't settle for second-rate*

