PKI for IoT using the DNS infrastructure

Sandoche BALAKRICHENAN

Sept. 9 2022

afnic
Internet
made in France

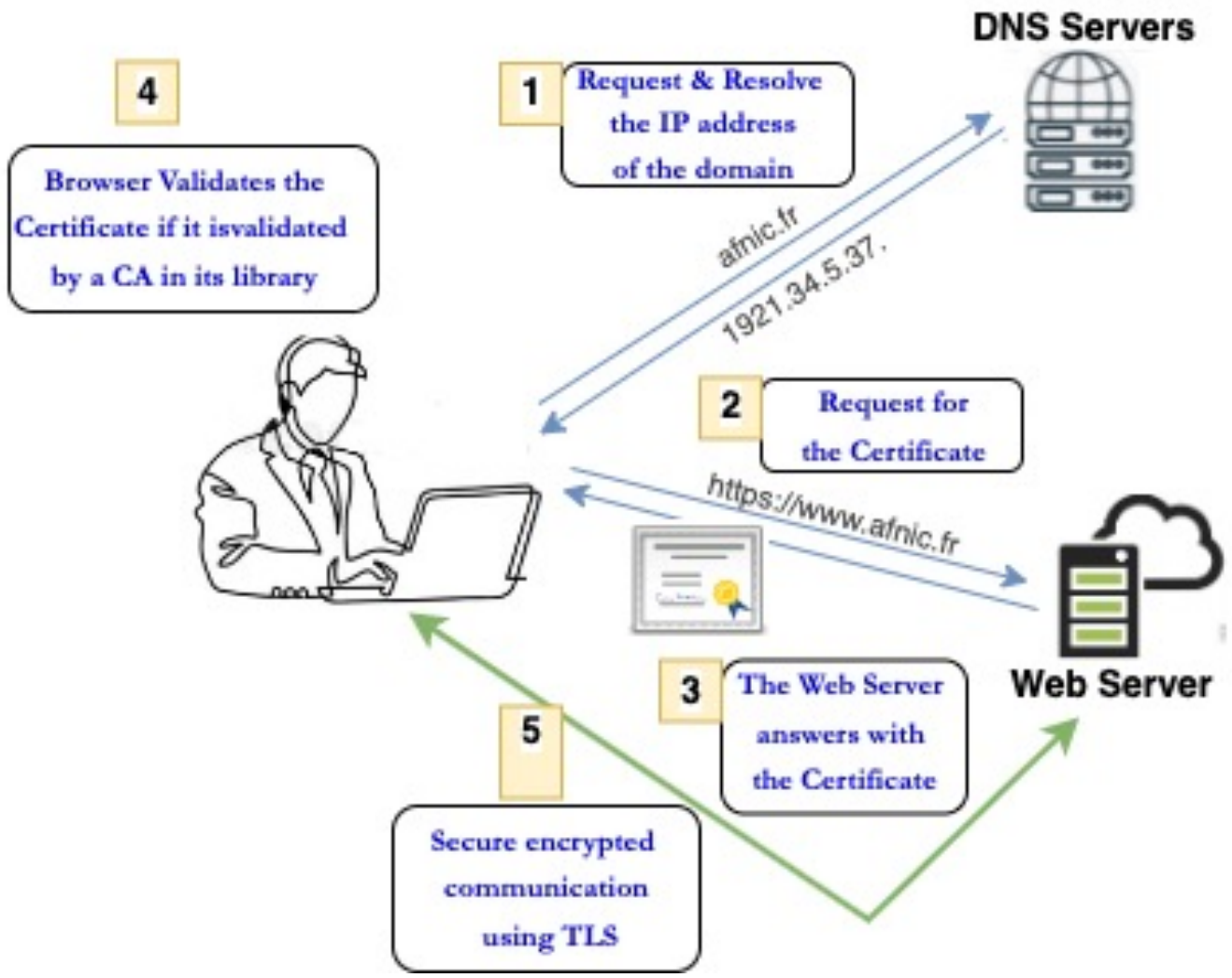
Presented at PKII 2022

afnic | Labs

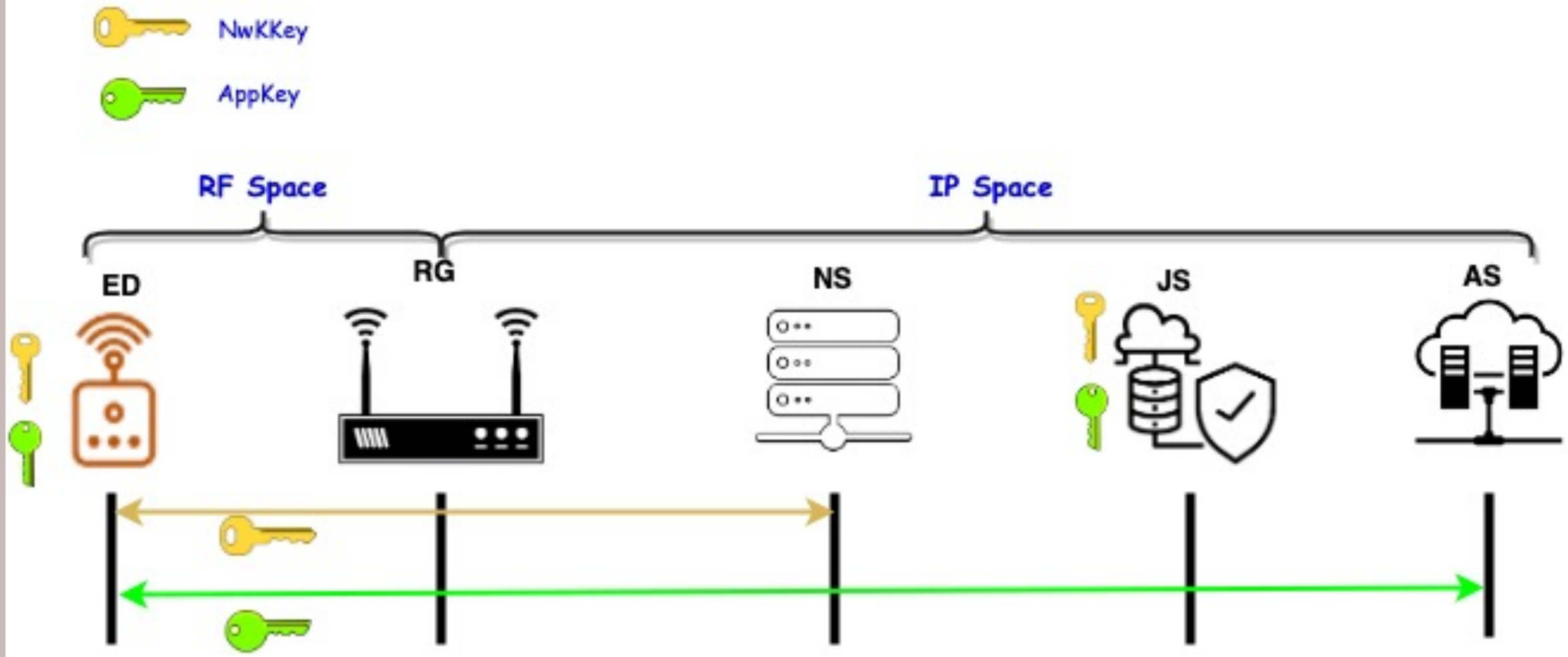
Motivation

- IoT is an extension of Internet with *Constrained* devices and networks
- Experiment by adapting *tested solutions* on the Internet to constrained IoT
- Using *Open* Internet Standards for IoT security
- Operational feasibility is a *mandatory* requirement

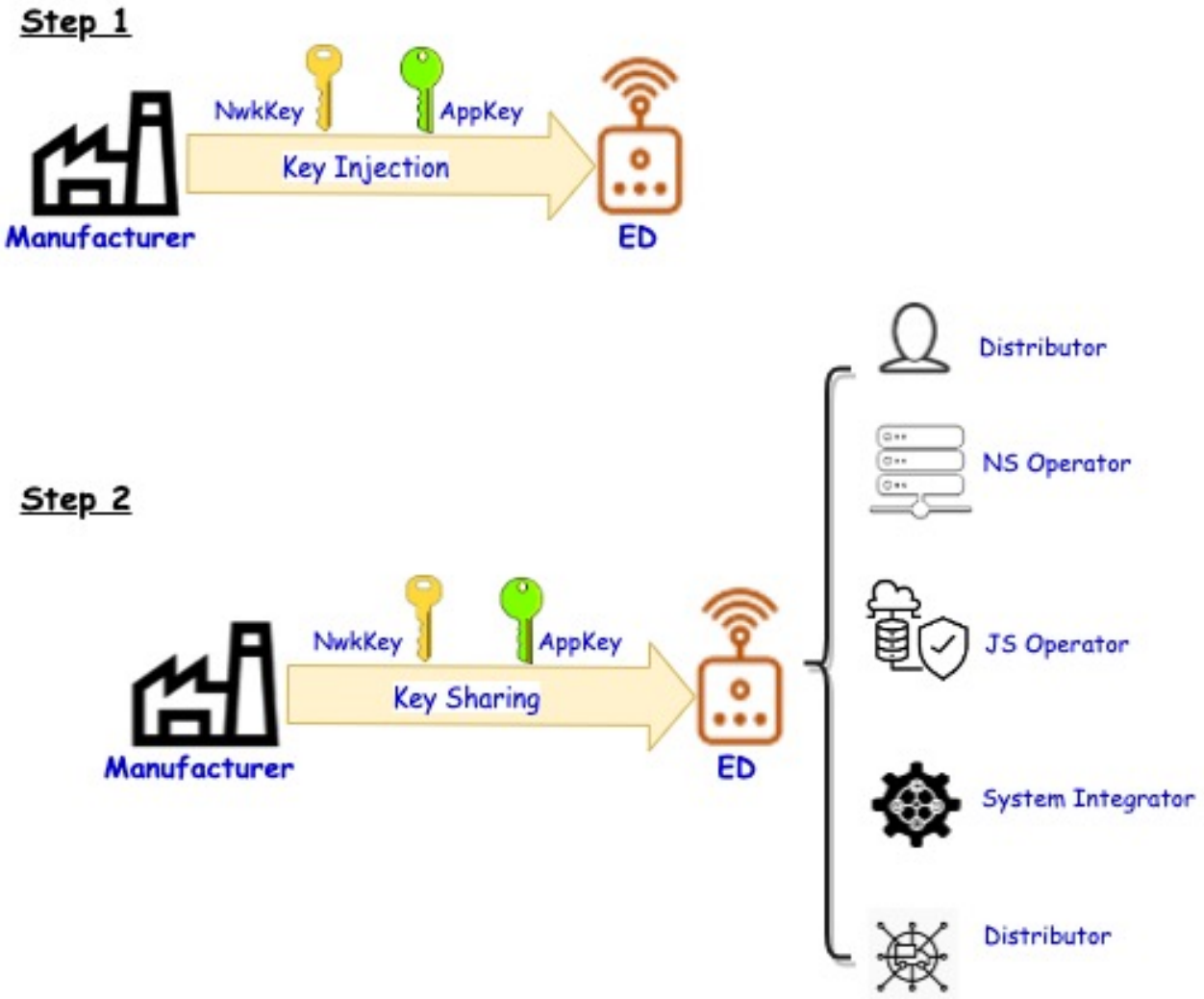
Secured Web communication using PKIX – *Two Governance structures*



Secured IoT communication – LoRaWAN example



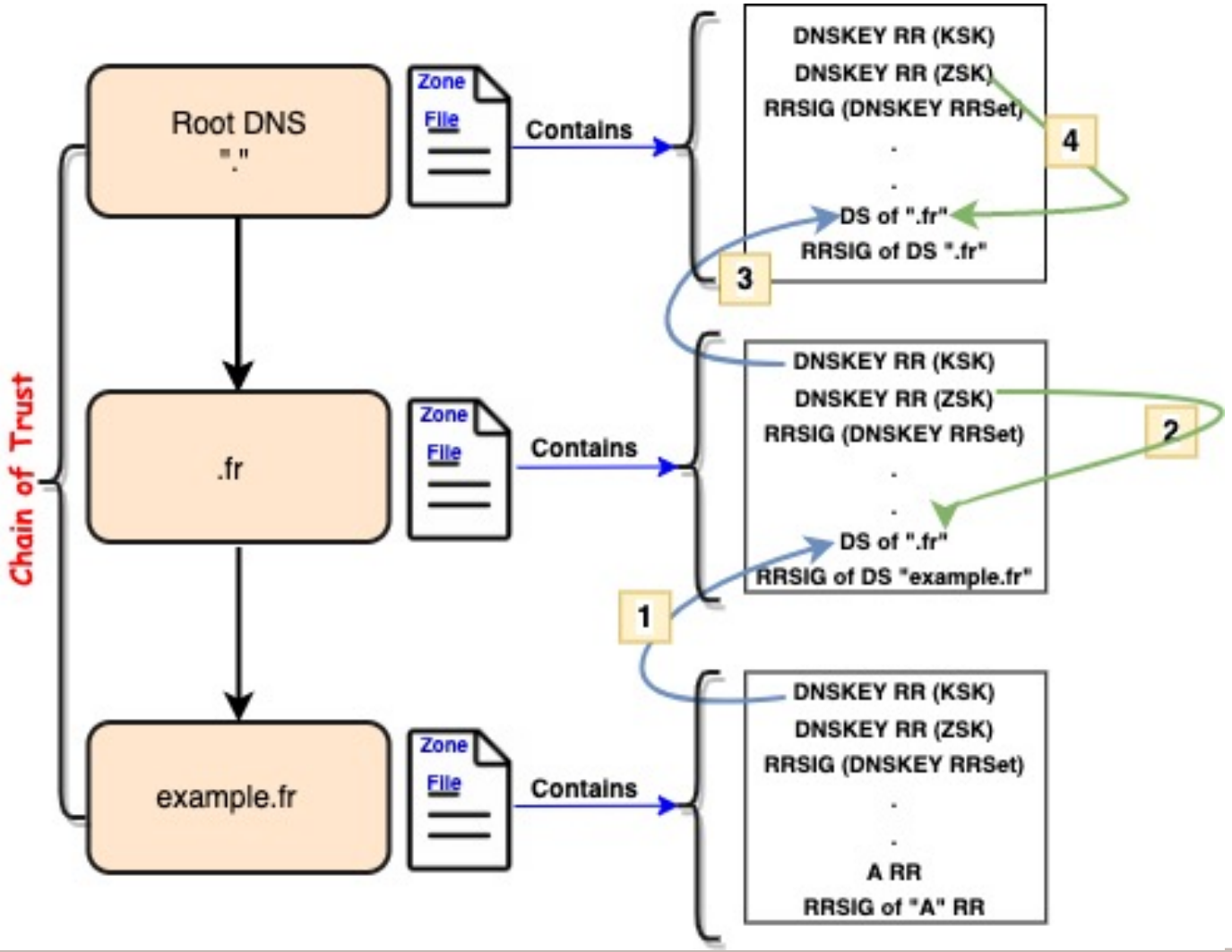
Issues with the current security system in IoT (1/2)



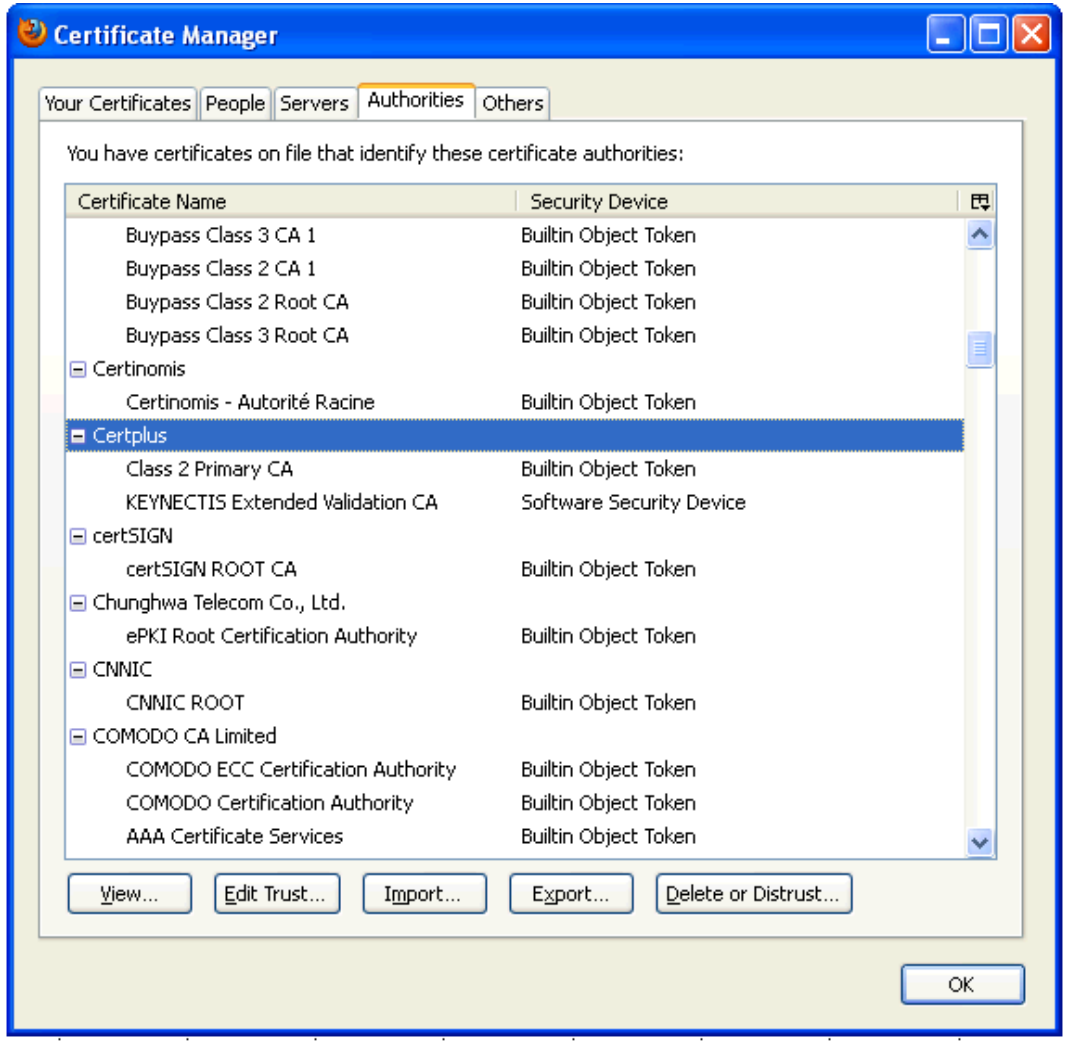
Issues with the current security system in IoT (2/2)

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

PKI using DNS – DNSSEC Primer

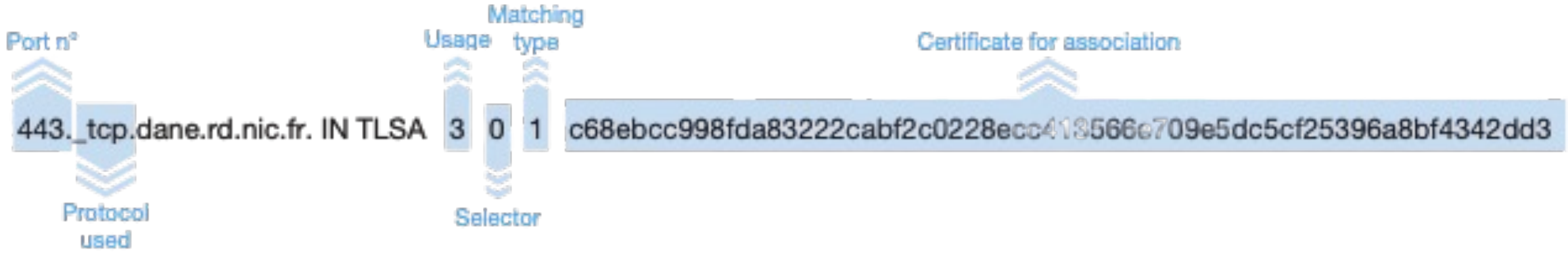


PKI using DNS – DANE Primer (1/2)

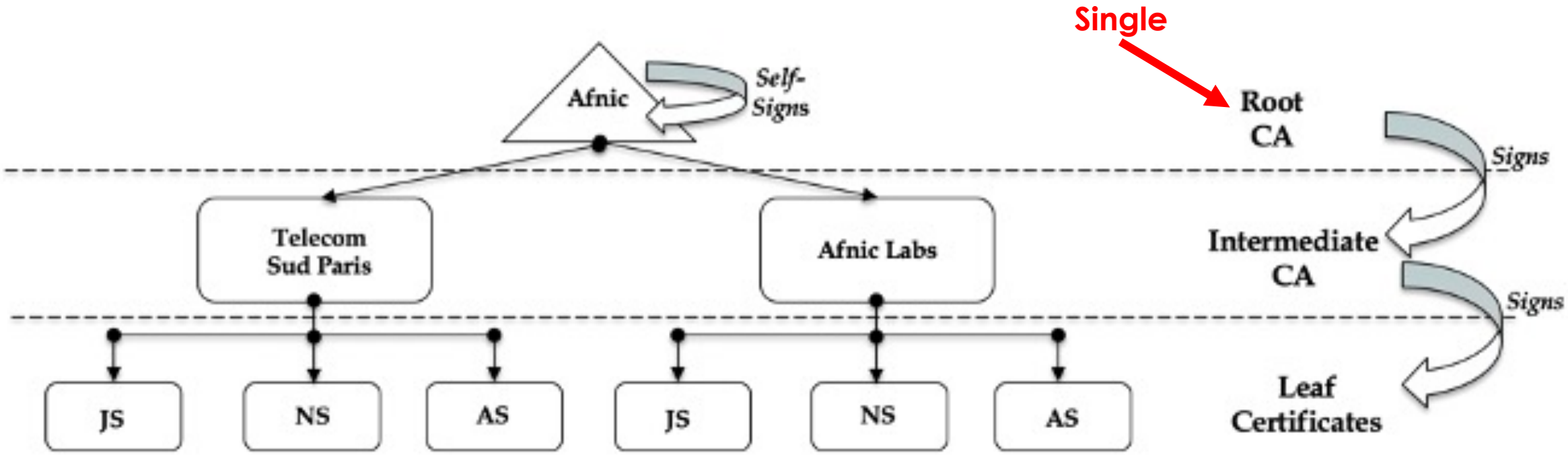




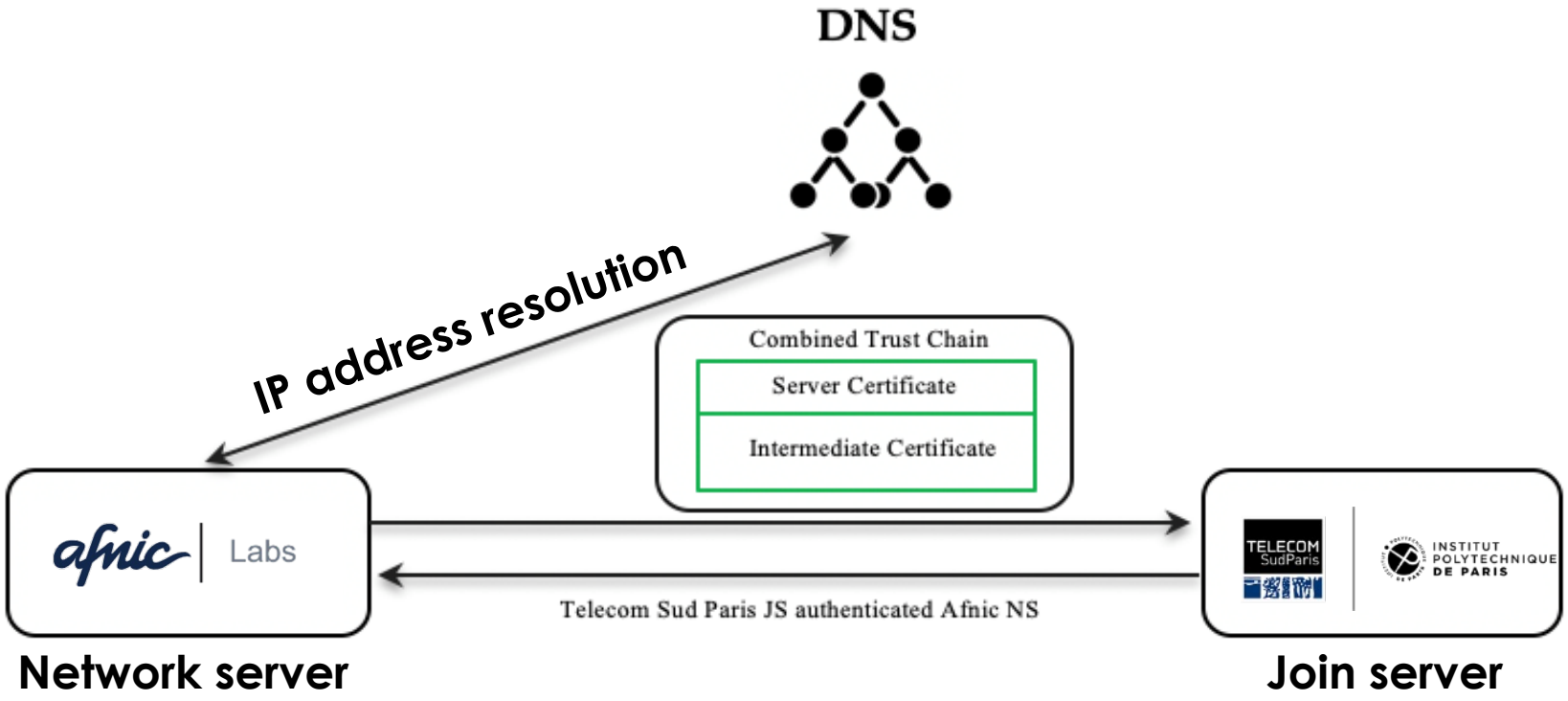
PKI using DNS – DANE Primer (2/2)



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



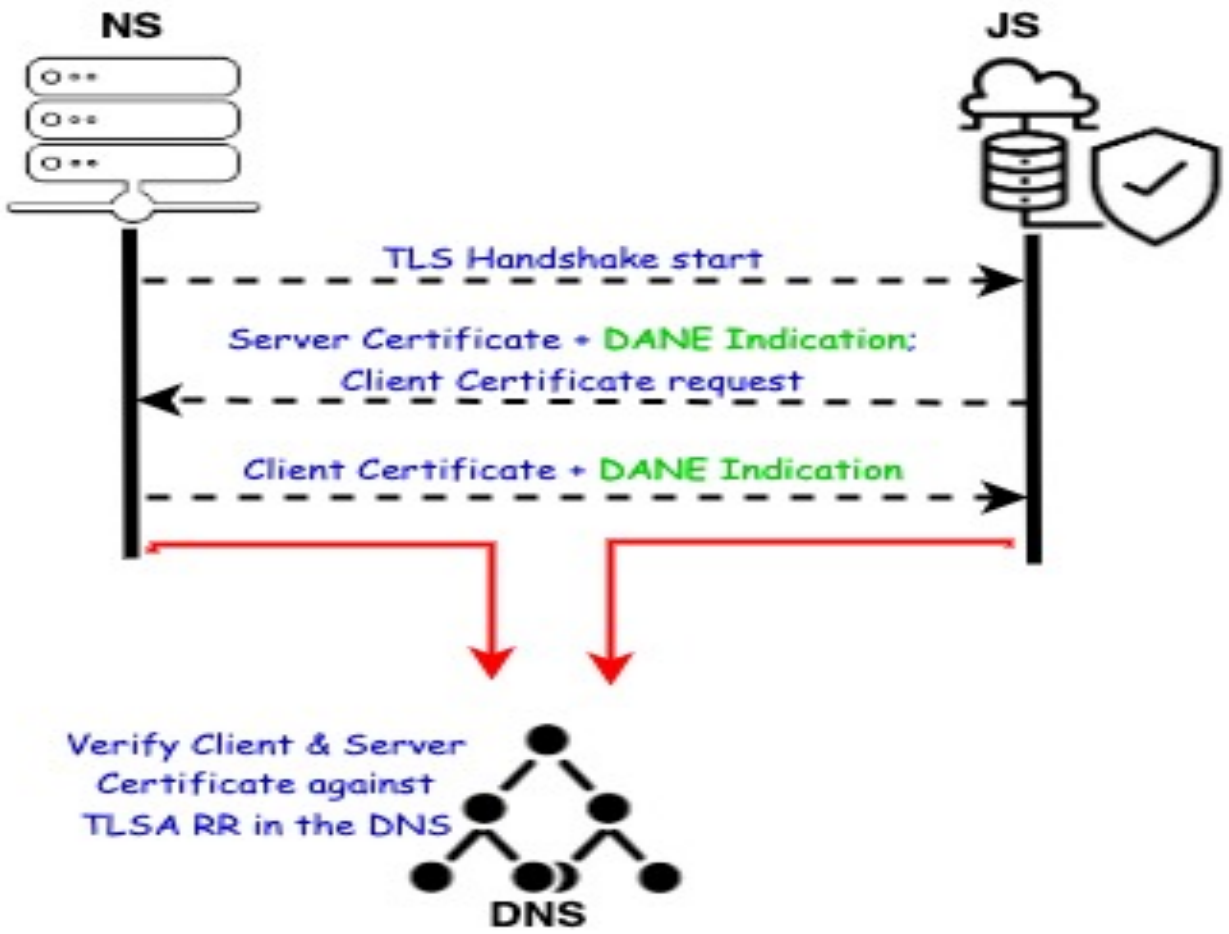
Using DANE indication Client/Server Authentication – Federated CA's

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

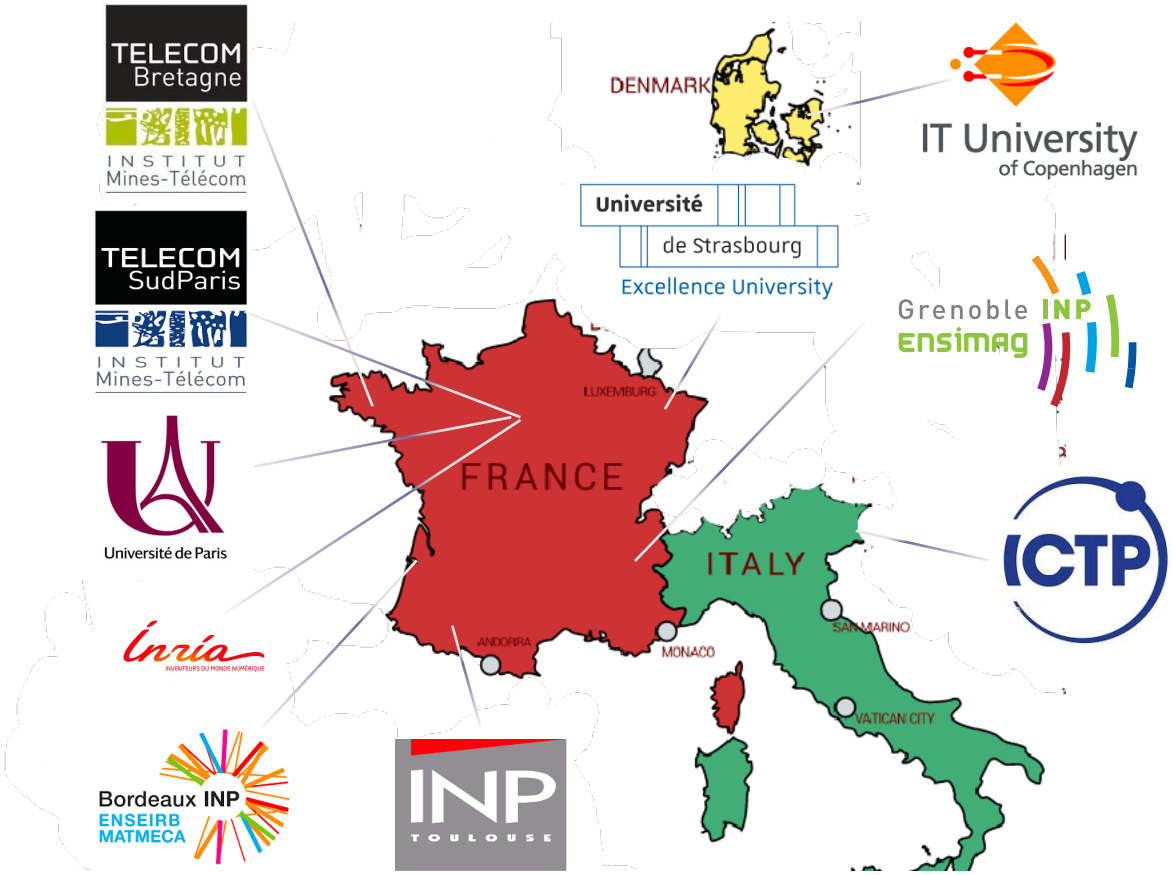


Enables using self-signed certificate with multiple Root CA's

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**

Institutions who have expressed Interest in testing IoTroam



Afnic's Vision

DONE

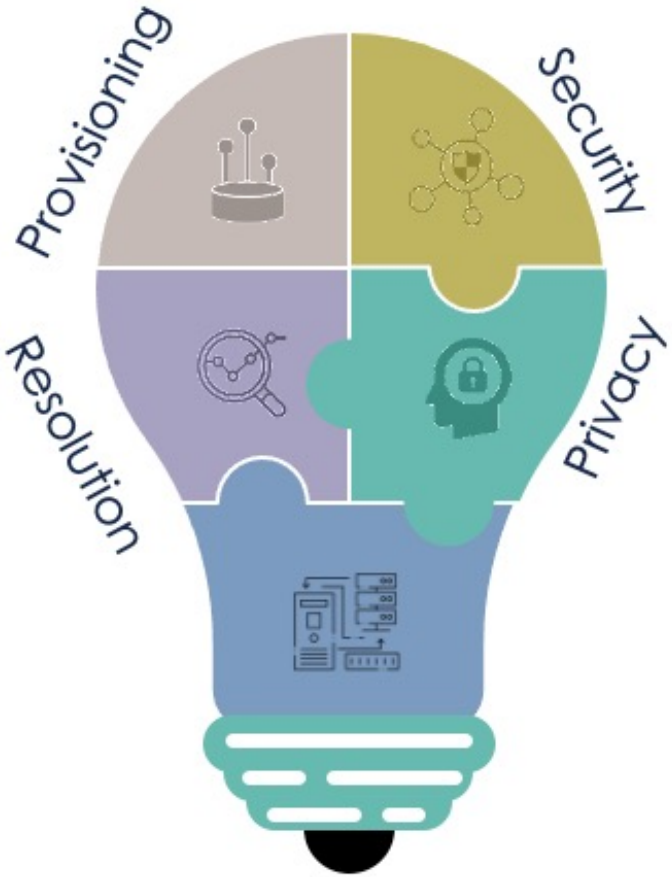
WINGS

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

Afnic's contribution in using DNS for IoT

