Using DNS for Secure/Seamless IoT

-*Sandoche BALAKRICHENAN*

DINR – 22 July 2020

afnic

Agenda

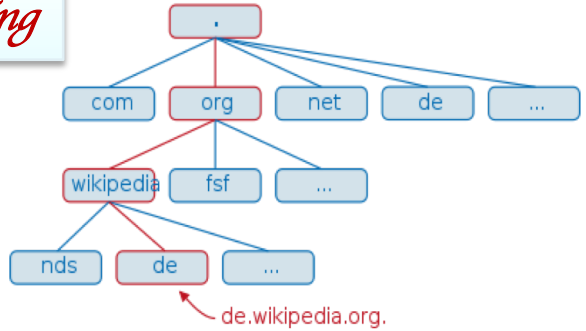
Three Steps to resolve an Identifier in the Internet

1. Naming Conventions

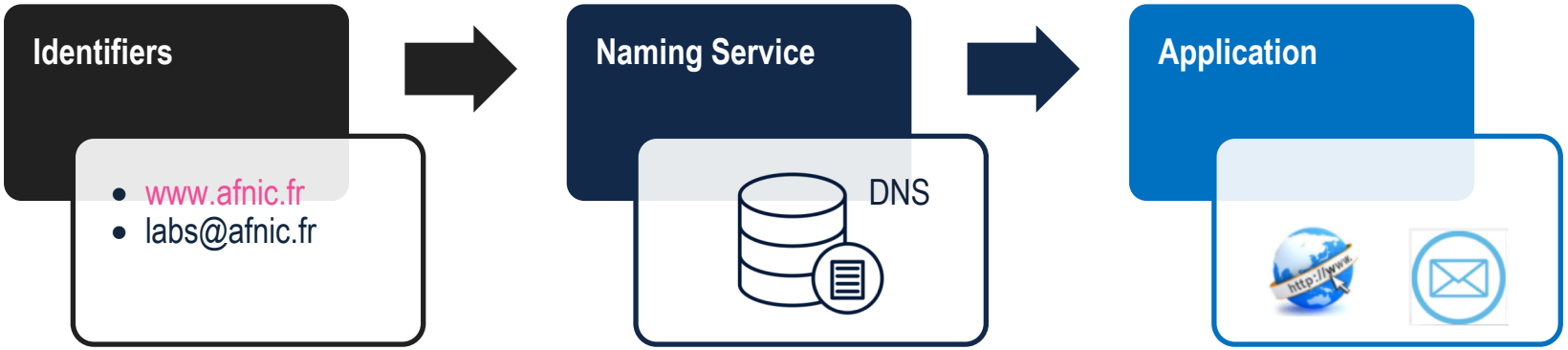
IETF is the SDO

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

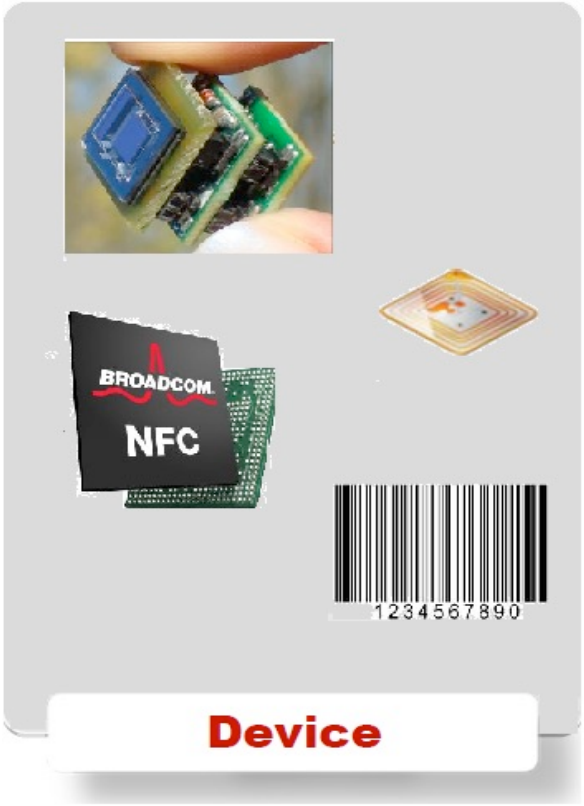
2. Provisioning



3. Resolution



Making the ‘T’ Identifiable in IoT



Naming conventions in IoT

RFC 2396
URI

ISO/IEC 15459
Products & Packages

ISO/IEC 29161
IoT Identification

ISO 14223
RFID for Animals

IEEE 1451
Smart Transducers

ISO 2108
Books

BS 7666
UK Property Reference Number

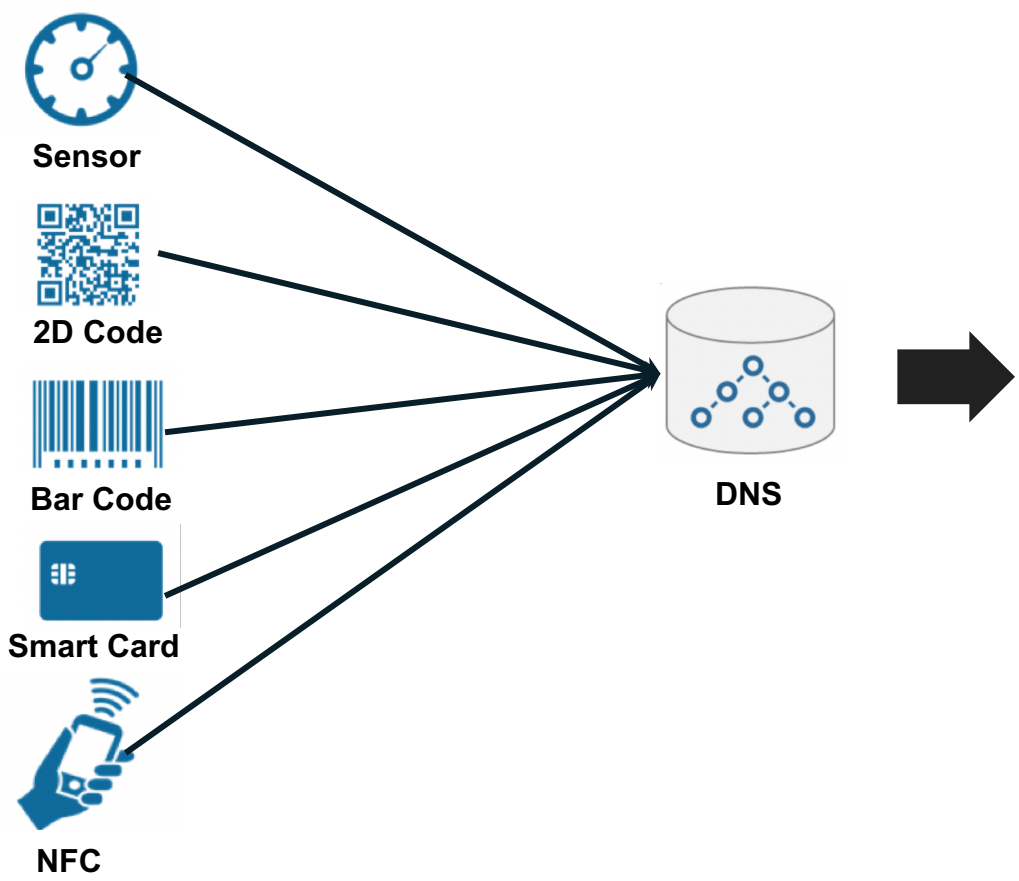
GS1 GTIN
Trade Items

ISO 16739
Construction & Facility Management

Naming conventions, SDOs and Naming Services in IoT

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

Vision – Using DNS as the Naming Service for IoT



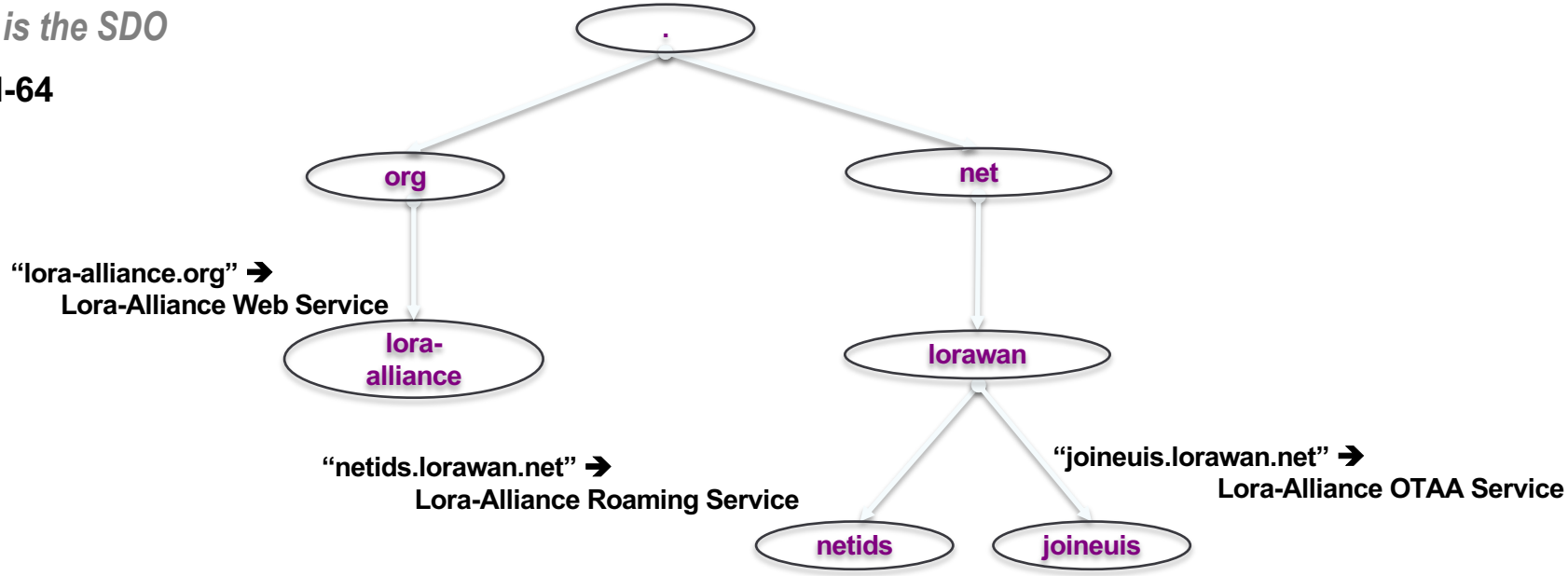
LoRaWAN Provisioning

1. Naming Conventions

IEEE is the SDO

- EUI-64

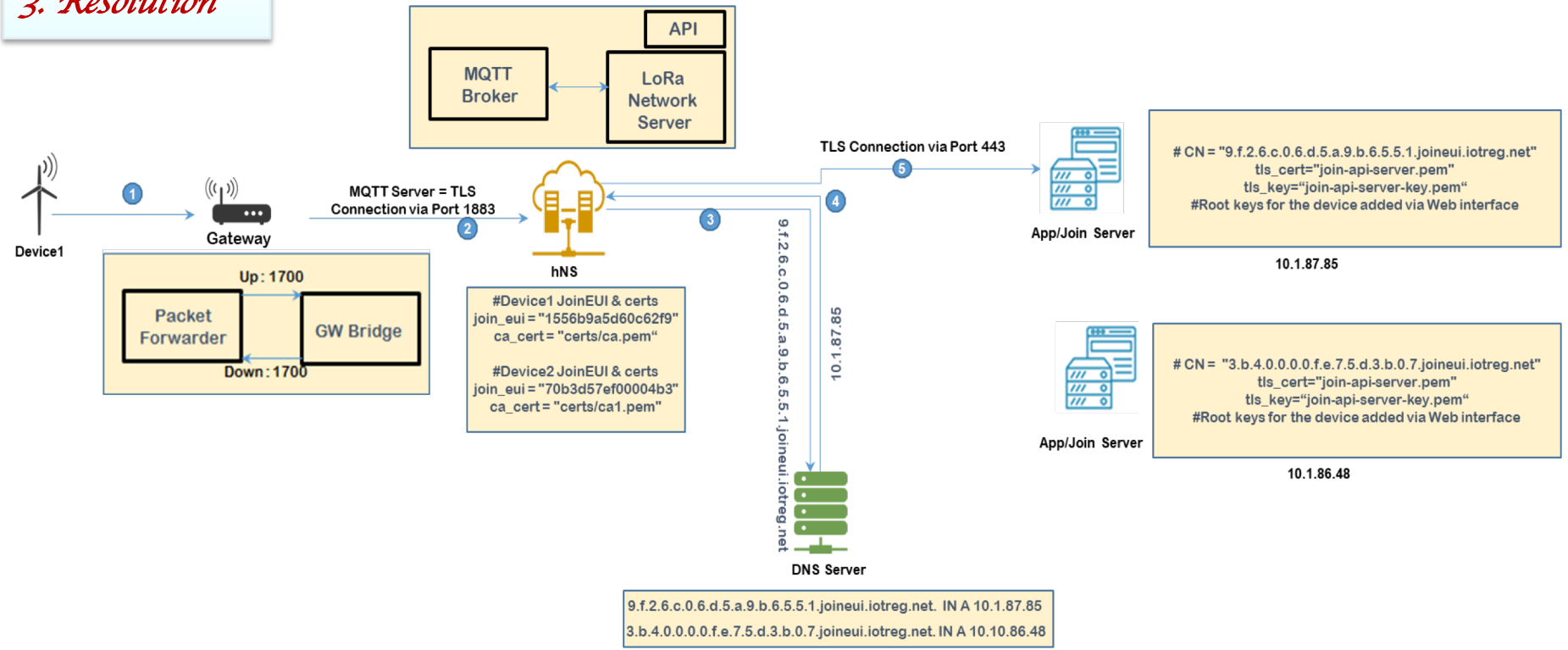
2. Provisioning



Ref: Section 20 of the LoRaWAN Backend Interfaces specification

LoRaWAN Resolution

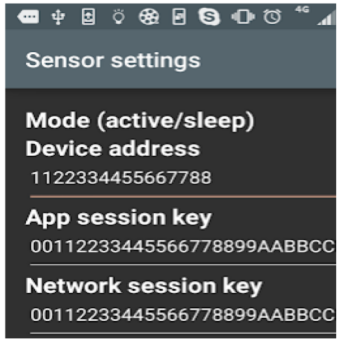
3. Resolution



The Key Sharing problem

- Currently Pre-shared Keys (PSKs) are used for securing IoT communication with the AAA server
- Sharing the PSKs is an operational nightmare
- Currently the PSKs are shared without any security such as :

Accessible via NFC on mobile phones



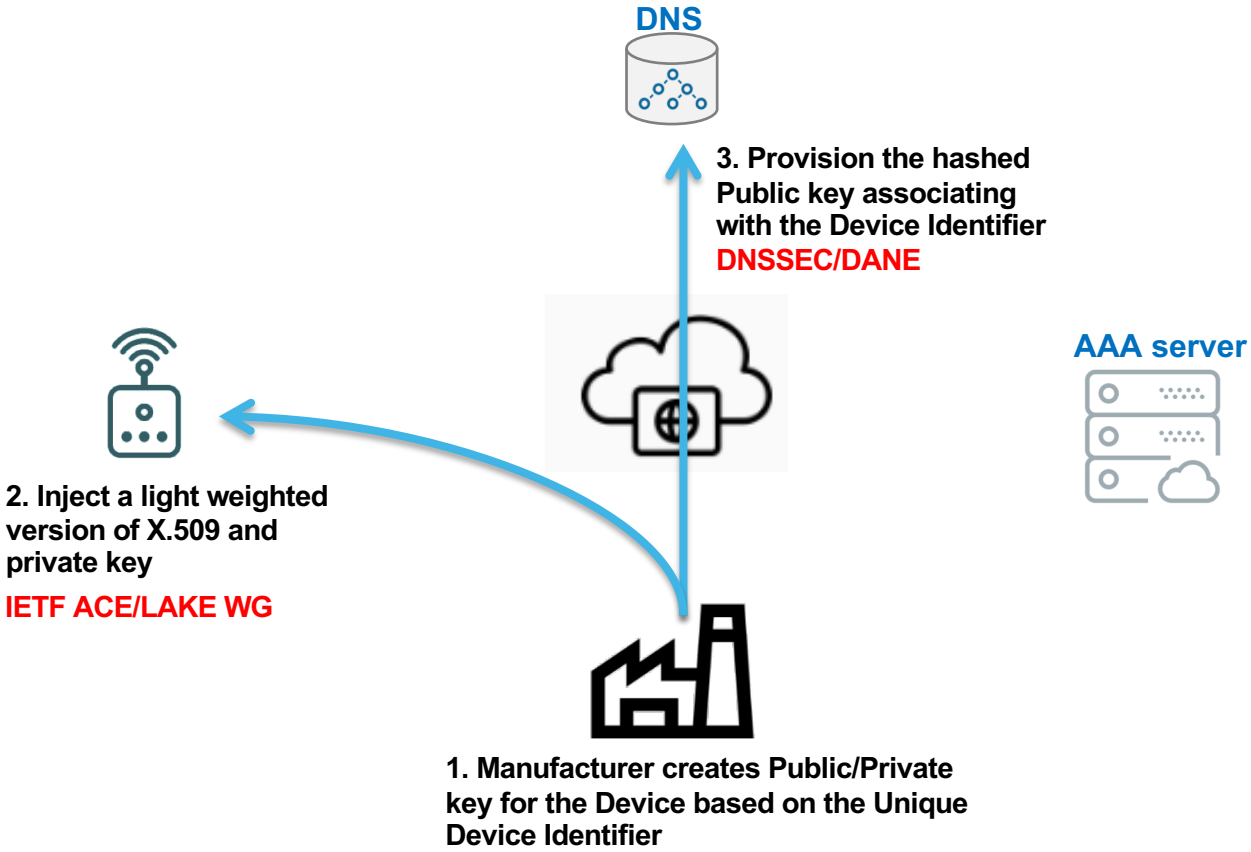
Printed behind the device

Sent via mail

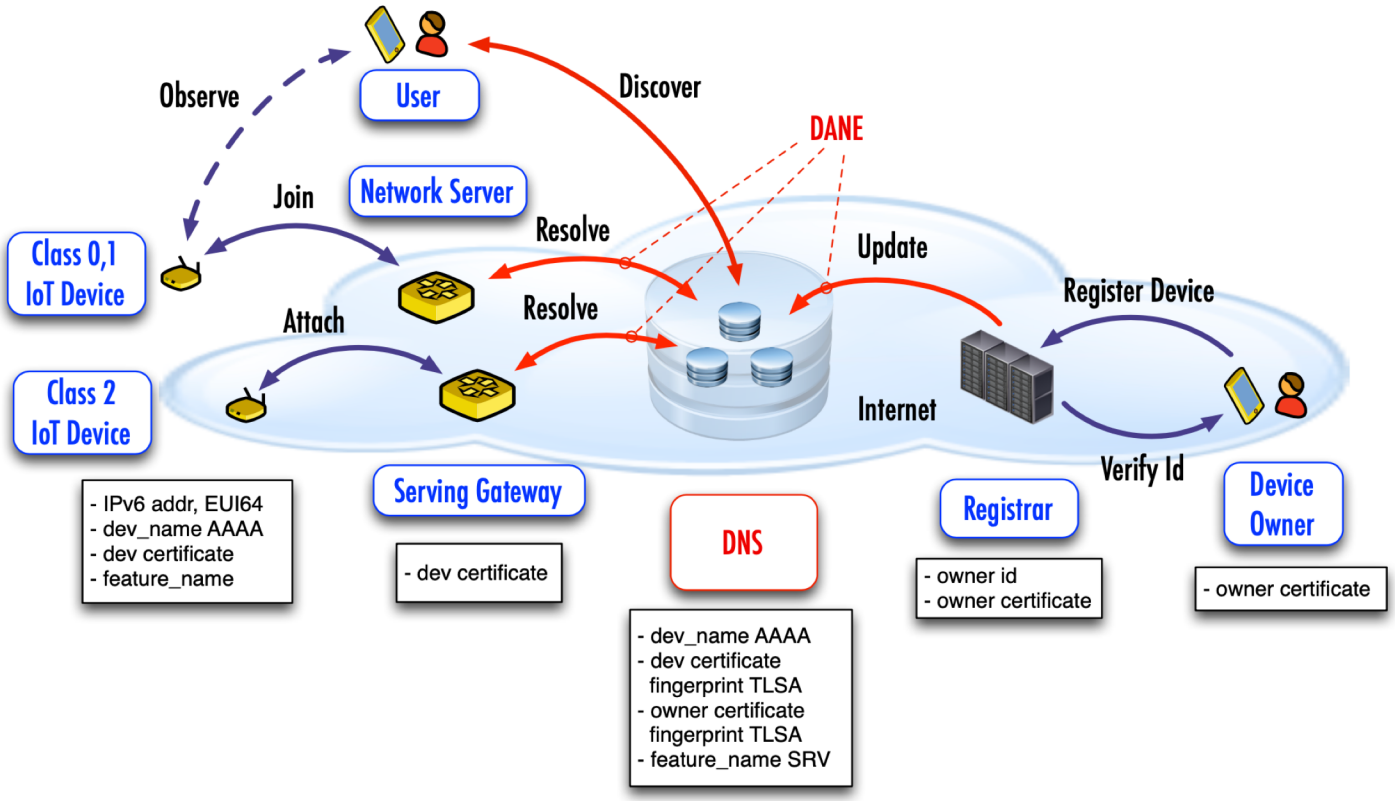
Operational Solution

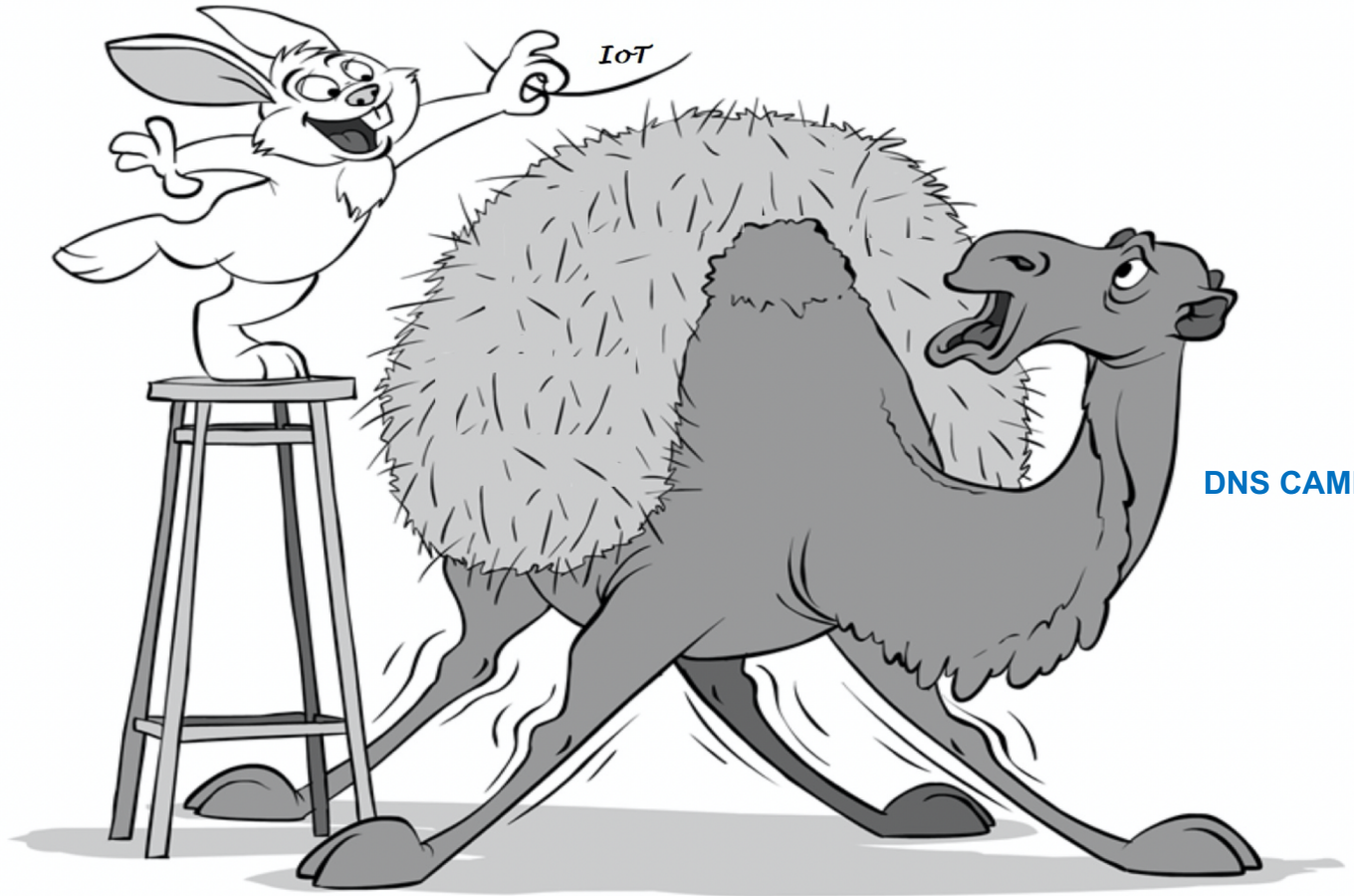
- Using Internet Style CA based solutions
- Issues in using CA certificates – Cost/Size
- For Cost – Self Signed Certificates
- For Size – ECDH, New IETF Standards (e.g: LAKE)

Vision – Using DNS infrastructure as the PKI for IoT



DiNS Project





DNS CAMEL

Future Directions

- Service Discovery – IETF DNS-SD
- Privacy – Oblivious DNS, DoH
- Open Roaming in IoT
- IoT Device Bootstrapping with DNS – BRSKI, MUD

Sandoche.balakrichenan@afnic.fr