LoRa DNS Service

AMM – Berlin Technical Committee #25
Sandoche Balakrichenan, Benoît Ampeau (Afnic)



ANTI TRUST STATEMENT

Anti-trust -- Bylaws Section 12.2: Support for Antitrust Laws:

“The Alliance unequivocally supports the policy of competition served by the antitrust laws and uncompromisingly intends to comply with such laws. Each Member further acknowledges that it may compete with the others in various lines of business and that it is therefore imperative that they and their representatives act in a manner which does not violate any applicable state, federal or international antitrust laws or regulations. It shall be the responsibility of every Member of the Alliance to be guided by this policy of compliance with the antitrust laws in all of the Alliance’s activities. It shall be the special responsibility of the Alliance’s Officers and Committee and Work Group chairpersons to ensure that this policy is known and to actively promote adherence to this policy in the course of activities pursued under their leadership.”

Agenda

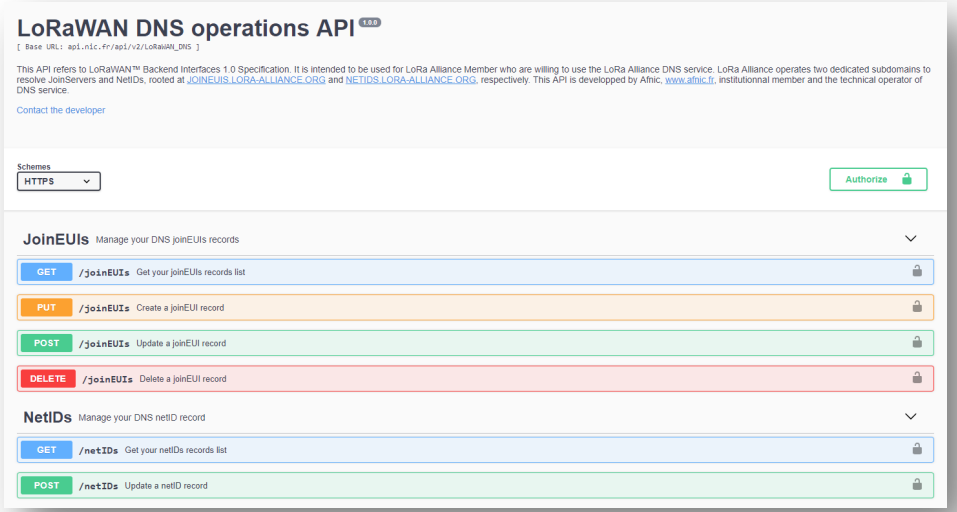
- DNS API quick overview
- Standardizing Securing Join Server interfaces based on DNS
  - Problem statement
  - Proposed solution
- LoRa DNS Service

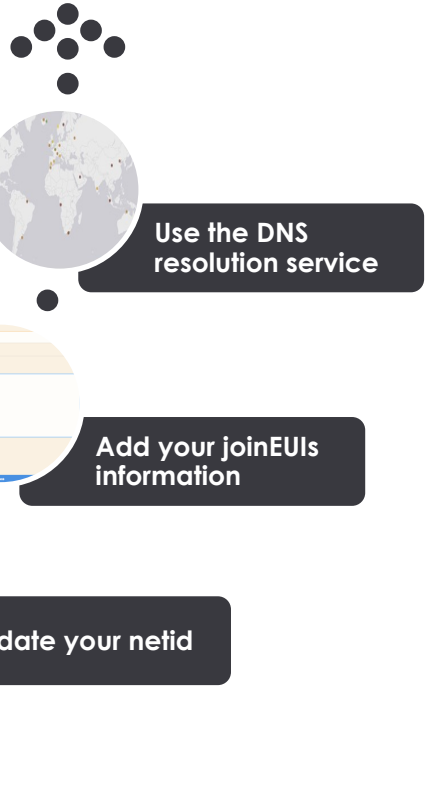
DNS API Service

- To test Roaming and OTAA
- Ease of use with examples
- Secured with an API key for each member
- A member cannot edit another member data in the DNS zone
- All information are stored in a database with a backup
- Currently available without any SLA

.

Device Onboarding process using DNS API





Any feedback welcome

Background

- Backend Interfaces define **messages** on the presentation and application layer
  - HTTP request/response bodies, encoding, etc
- Backend Interfaces 1.1 define **lookup** of networks and join servers through DNS, i.e. the network layer
  - Afnic contributed a test environment
- What is missing is the transport and session layer: how to **access** services in a secure way?

Copied from the "The Things Network" presentation at TC #24

Problem

- It is currently assumed that there is out-of-band configuration:
  - JS-side: registration of NS (by NetID) and AS (by AS-ID)
  - NS/AS-side: registration of JS (by JoinEUI)
  - This can involve TLS client/server certs, IP addresses, QoS, SLA
- There will hopefully be thousands of NS, AS and JS instances, so out-of-band configuration may run in manageability issues
- JS only needs to verify:
  - Whether the NS that performs the join is the NS configured for the device
  - Whether the AS that wants the AppSKey is the AS configured for the device

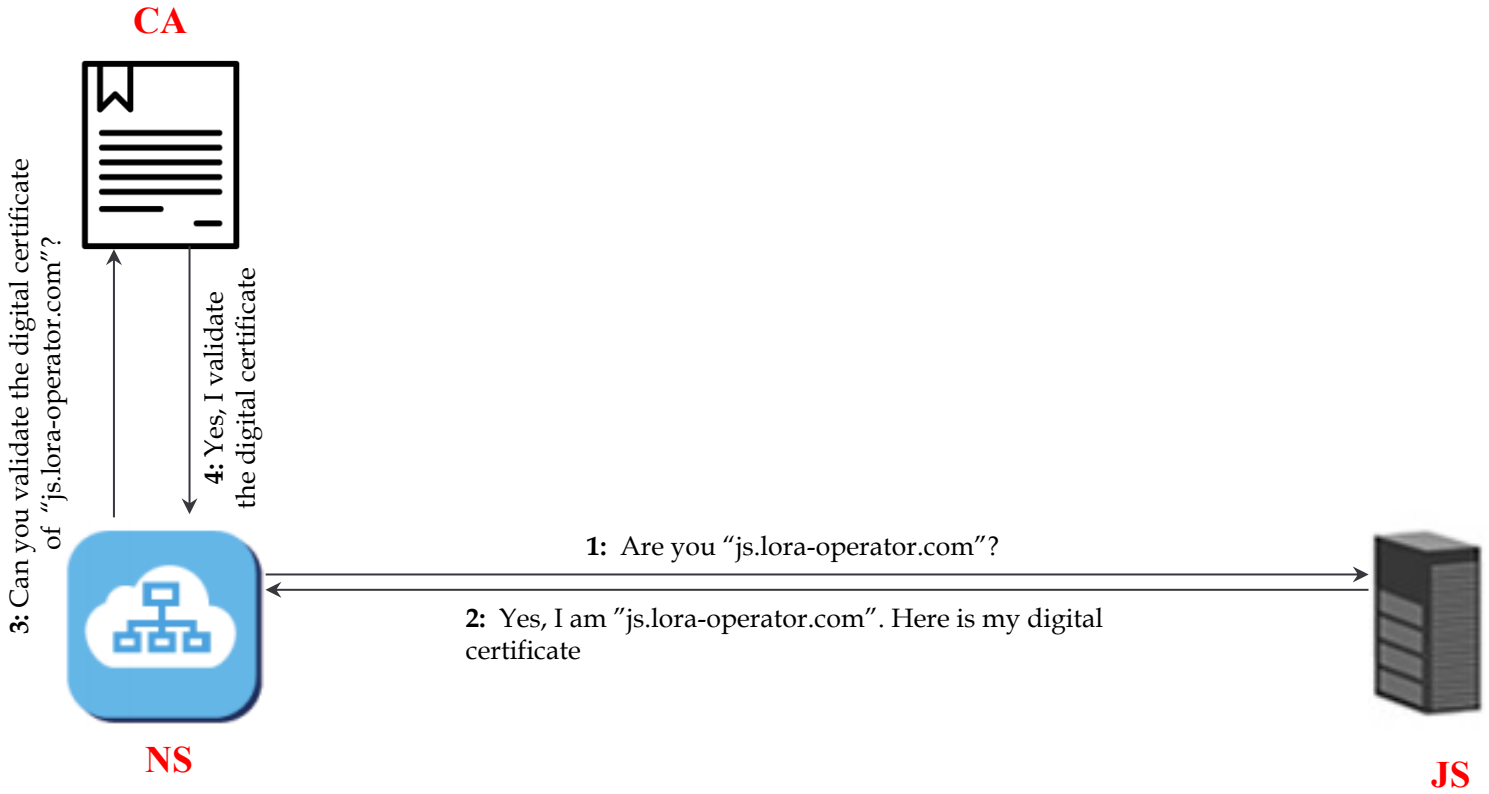
Copied from the "The Things Network" presentation at TC #24

Join Server Lookup and Authentication

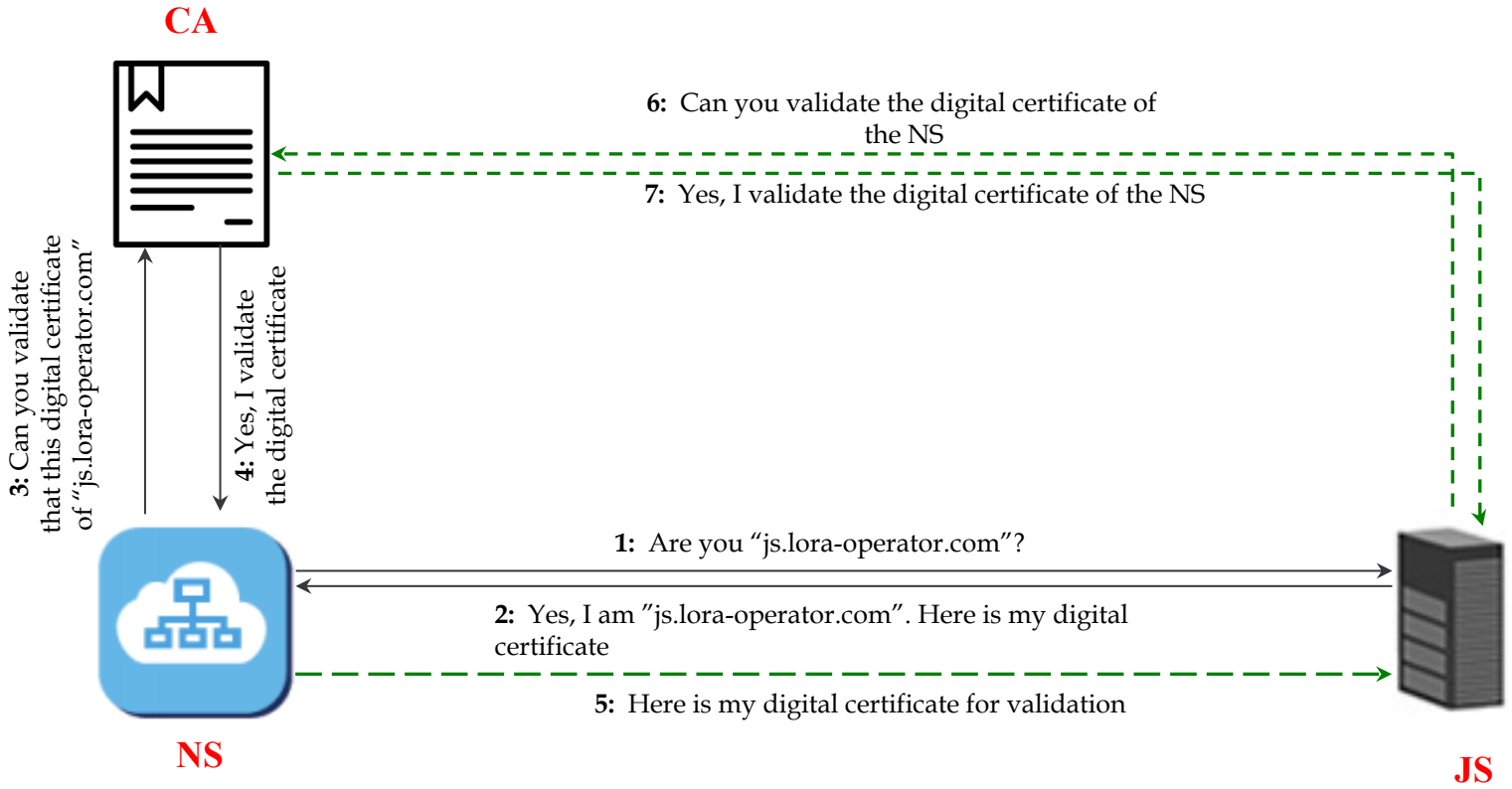
- DNS lookup by <join-eui>.joineuis.lora-alliance.org (A or CNAME)
- Proposing using Transport Layer Security (TLS)
- Requires trusted certificate chain
  - When using A record (i.e. https://<join-eui>.joineuis.lora-alliance.org):
    - 1: LoRa Alliance signed certificates, i.e. needs Certification Authority (CA) operated by the LoRa Alliance. Desired? Feasible?
    - 2: Use DANE/TLSA to put JS certificate fingerprint in DNS
  - When using CNAME (i.e. js.operator.com.), use any JS certificate. Easiest approach

Copied from the "The Things Network" presentation at TC #24

JS look up authentication (NS Validating the JS)



JS look up authentication (JS Validating to the NS)



Goal

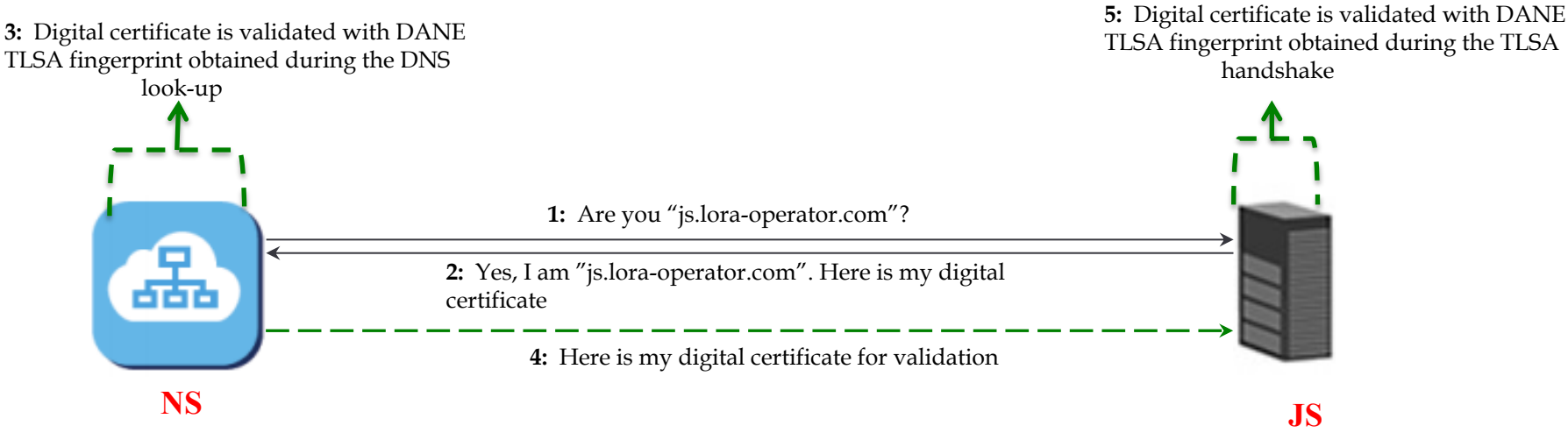
- TR for NS-JS which does not need any out of band configuration and works with only DNS look up
- Should work without a dedicated CA
  - Vulnerabilities in the CA (Comodo attack)

DANE TLSA Resource Record (RFC 7671)

- Step 1 : Create the public/private key for the domain (e.g: **js.lora-operator.com**)
- Step 2 : Generate the TLSA RR (**js.lora-operator.com. IN TLSA 3 0 1 e781577c0eabb6701a0caf287e48ceebd3ba64b81792ef49705f0f5e1070331b**) and add it to the DNS zone
- Sign the zone using DNSSEC

The above process could be automated and done in two or three clicks

NS-JS validation using DANE

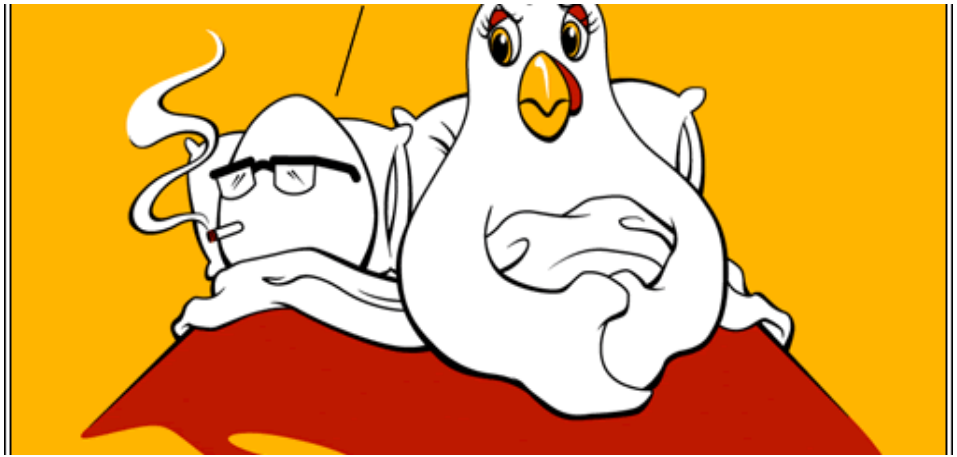


draft-huque-dane-client-cert-03 (IETF draft)

LoRaWAN DNS service

Member type	Member Name
Public Operator	Objenious
Private Operator	Mirakonta
Community Operator	Things Network
Equipment manufacturer	Kerlink

Other works based on DNS (e.g. JoinEUI reconfiguration CR)



Thanks for your attention

Any questions ?