The path from an Internet registry to an IoT registry based on DNS

Sandoche BALAKRICHENAN
Hypothesis

**Requirement:** Operational feasibility
How we are planning to achieve this vision?

DONE
WINGS
Widening interoperability for networking Global supply Chains

PoC
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
Provisioning => Establishing the route

“A name indicates what we seek. An address indicates where it is. A route indicates how we get there.”

—Jon Postel, RFC 791

LoRaWAN Backend Interfaces specification
LoRaWAN Architecture basic vs Roaming
## Prior Configuration Parameters for Roaming

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Net-ID</td>
</tr>
<tr>
<td>Roaming Policy</td>
</tr>
<tr>
<td>Peer’s channel plan</td>
</tr>
<tr>
<td>Peer’s fNS URL</td>
</tr>
<tr>
<td>Peer’s sNS URL</td>
</tr>
<tr>
<td>Peer’s NS IP address</td>
</tr>
<tr>
<td>Peer JS URL</td>
</tr>
<tr>
<td>Peer JS IP Address</td>
</tr>
<tr>
<td>Peer JS Http Credentials</td>
</tr>
</tbody>
</table>
Roaming with minimum prior configurations – DNS Resolution

ED

RG

fNS

sNS

DNS

JS

Get IP address of the JS
IP address of the JS
Get sNS Identifier
NetID of sNS
Get IP address of sNS
ProfileReq
ProfileAns
JR
JR
JR
JAccept
Packet uplink
Packet downlink
Packet uplink
Packet downlink
Packet uplink
Packet downlink
JAccept
Packet uplink
Packet downlink
Packet uplink
Packet downlink
Adding Security – Certificate Provisioning – IoTRoam PoC

Call for collaboration - https://github.com/AFNIC/IoTRoam-Tutorial
Adding Security – Certificate Validation

DNS

Afnic Labs NS

Combined Trust Chain
- Server Certificate
- Intermediate Certificate

Telecom Sud Paris JS

Telecom Sud Paris JS authenticated Afnic NS

IP address resolution
IoTRoam Platform

Diagram showing the connection process involving MQTT Broker, LoRa Network Server, DNS Server, and TSP - JS. The process includes mutual authentication using combined certificates and DNS resolution for NS Intermediate & CA Cert.
Using DANE Client Authentication (Ongoing work)

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

1. TLS Handshake start
2. Server Certificate + DANE indication; Client Certificate request
3. Client Certificate + DANE indication;
   - Verify Server Certificate against DANE TLSA RR in the DNS
   - Verify Client Certificate against DANE TLSA RR in the DNS
Compressing X.509 certificates for constrained LoRaWAN use-case (Ongoing work)

- Maximum frame size as low as 51 bytes
- LoRaWAN uses 128-bit AES pre-shared symmetric keys

Source: F. Frosby et al.

- LAKE IETF WG, LPWAN IETF WG
Privacy Challenges & Solutions envisioned

- Protecting the IoT device identity – *Ephemeral & Application Identifiers*

- Protecting the metadata – *Content Object Security* (Content disclosure attributed to designated receivers)

- How to handle Object Security in decentralized manner? – *DNS based PKI*

- Standardised crypto library framework – *Deployment on RIOT OS*

- Architecture validation - *IoTROam*
sandoche.balakrichenan@afnic.fr