Using DNS for Secure/Seamless IoT

- Sandoche BALAKRICHENAN

DINR – 22 July 2020
Agenda

Identification & Resolution

Security

Future directions
Three Steps to resolve an Identifier in the Internet

1. Naming Conventions

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

2. Provisioning

3. Resolution

Identifiers
- www.afnic.fr
- labs@afnic.fr

Naming Service

Application

IETF is the SDO
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

<table>
<thead>
<tr>
<th>Naming Conventions</th>
<th>SDO</th>
<th>Naming Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>URI (e.g. Domain names)</td>
<td>IETF</td>
<td>DNS</td>
</tr>
<tr>
<td>EPC</td>
<td>GS1</td>
<td>ONS</td>
</tr>
<tr>
<td>OID</td>
<td>ITU and ISO/IEC</td>
<td>ORS</td>
</tr>
<tr>
<td>DOI</td>
<td>ISO</td>
<td>Handle</td>
</tr>
</tbody>
</table>
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

Device1
Gateway
MQTT Server = TLS Connection via Port 1883

LoRa Network Server

MQTT Broker

API

hNS

Packet Forwarder
GW Bridge

Up: 1700
Down: 1700

DNS Server

TLS Connection via Port 443

App/Join Server

# CN = "9.f.2.6.c.0.6.d.5.a.9.b.6.5.5.1.joineui.iotreg.net"
#tls_cert="join-api-server.pem"
#tls_key="join-api-server-key.pem"
Root keys for the device added via Web Interface

10.1.87.85

10.1.86.48
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

1. Manufacturer creates Public/Private key for the Device based on the Unique Device Identifier

2. Inject a light weighted version of X.509 and private key
   IETF ACE/LAKE WG

3. Provision the hashed Public key associating with the Device Identifier
   DNSSEC/DANE

AAA server
DiNS Project

Class 0,1 IoT Device
- IPv6 addr, EUI64
- dev_name AAAA
- dev certificate
- feature_name

Class 2 IoT Device

Network Server

User

Discover

Join

Resolve

Attach

DANE

Update

Internet

Register Device

Verify Id

Device Owner
- owner certificate

Registrar
- owner id
- owner certificate

DNS
- dev certificate
- dev_name AAAA
- dev certificate fingerprint TLSA
- owner certificate fingerprint TLSA
- feature_name SRV

Serving Gateway
DNS CAMEL
Future Directions

• Service Discovery – IETF DNS-SD

• Privacy – Oblivious DNS, DoH

• Open Roaming in IoT

• IoT Device Bootstrapping with DNS – BRSKI, MUD