Oct. 22 2022

Internet made in France

PKI for IoT using the DNS infrastructure

Sandoche BALAKRICHENAN

Presented at DNS-OARC 39 @Belgrade(2022)

afnic Labs This proposal doesn't burden the DNS camel





afmic-

Labs Key sharing dilemma between the RF & IP space amic Step 1 NwkKey AppKey Key Injection Manufacturer ED Distributor 0.00 NS Operator 0.44 Step 2 配 AppKey NwkKey JS Operator Key Sharing ED Manufacturer System Integrator Distributor

afruc

afnic Labs Examples of how PSK's are shared?

Accessible via NF On mobile phones	C s	LoRaWAN device
Sensor settings Mode (active/sleep) Device address 1122334455667788		DevEUI: 0123456789ABCDEF AppEUI: FEFCBA9876543210 AppKey: 0101010101010101
App session key 00112233445566778899AABBCC Network session key	3 Sent via mail	LOT 201812
00112233445566778899AABBCC	Econo Ma Econo Ma Econo Rei Ewdr Rei Amie - offer #170010 To pieterstalioratactory.com E C.c. Report Amoeau spepoit amoeau@afnic.frs	
	DevEUI DevAddress 7083055E10060230 10060230	
	AppKey = 6E39AEC0794114E6F09F0A9E4F13B204 AppEUI = 70 B3 D5 7E F0 00 46 B3 231 231 AppKey = EA0D0ED4022GC37E09E7EF03446E75CD	
	AppEUI = 7002057550004502	

afruc

afnic Labs Key sharing dilemma within the IP space

• AS-JS

• JS-NS

• NS-NS

From Section 21 of the LoRaWAN Backend Specifications:

Network elements SHALL rely on a security solution that can provide mutual end-point authentication, integrity and replay protection, and confidentiality when communicating with each other. The choice of mechanism used for achieving these properties is left to the deployments (e.g., using IPsec VPN, HTTPS, physical security, etc.)



Using the web based asymmetric cryptography (PKIX) in Labs IP space

Issues	Solutions		
Cost	Self-Signed Certificates		
Label length	Self-Signed Certificates		
Non-Availability of CA trust-store	DNS-Based PKI		

	Comodo PositiveSSL	Comodo InstantSSL Premium	Comodo PositiveSSL EV
Pricing	Listed Price: \$49.00/yr.	Listed Price: \$179.95/yr.	Listed Price: \$149.00/yr.
	Our Price: \$7.27 /yr.	Our Price: \$56.06 /yr.	Our Price: \$74.99 /yr.

afnic

afruc

DNS Provisioning



afnic



= = = - -> Encrypted communication thanks to PKI based on self-signed certificates

Issue in using Self-signed certificates





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

Afnic –implemented and tested the two IETF drafts during IETF 113 Hackathon



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

An ideal scenario for E2E Security



key for the Device based on the Unique Device Identifier



ofnic | Labs Web based X.509 digital certificates cannot be deployed directly in the RF space

F. Forsby et al.



Data Rate (DR)	Spreading Factor (SF)	Channel Frequency	Uplink or Downlink	Bitrate (Bits/Sec)	Maximum User Payload Size (Bytes)
0	SF10	125 kHz	Uplink	980	11
1	SF9	125 kHz	Uplink	1,760	53
2	SF8	125 kHz	Uplink	3,125	125
3	SF7	125 kHz	Uplink	5,470	242
4	SF8	500 kHz	Uplink	12,500	242
5-7					
8	SF12	500 kHz	Downlink	980	53
9	SF11	500 kHz	Downlink	1,760	129
10	SF10	500 kHz	Downlink	3,125	242
11	SF9	500 kHz	Downlink	5,470	242
12	SF8	500 kHz	Downlink	12,500	242
13	SF8	500 kHz	Downlink	21,900	242

afric Labs Issues being 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

afnic Labs References

- Afnic
 - <u>https://github.com/AFNIC/Mutual-Authentication-via-DANE</u>
 - <u>https://gitlab.rd.nic.fr/tutoriels/The-DNS-to-Reinforce-the-PKIX</u>
- External
 - IETF LPWAN (Low Power Wide Area Network) WG
 - IETF LAKE (Lightweight Authenticated Key Exchange) WG

