20 mars 2022

afnic

Internet
made in France

IETF 113 Hackathon – DANCE WG

Drafts that we were working on

- draft-huque-tls-dane-clientid-06

- draft-huque-dane-client-cert-08

Dane-client-cert draft

- Existing Implementation
    - go library for DANE TLSA authentication (Author: Shumon Huque)

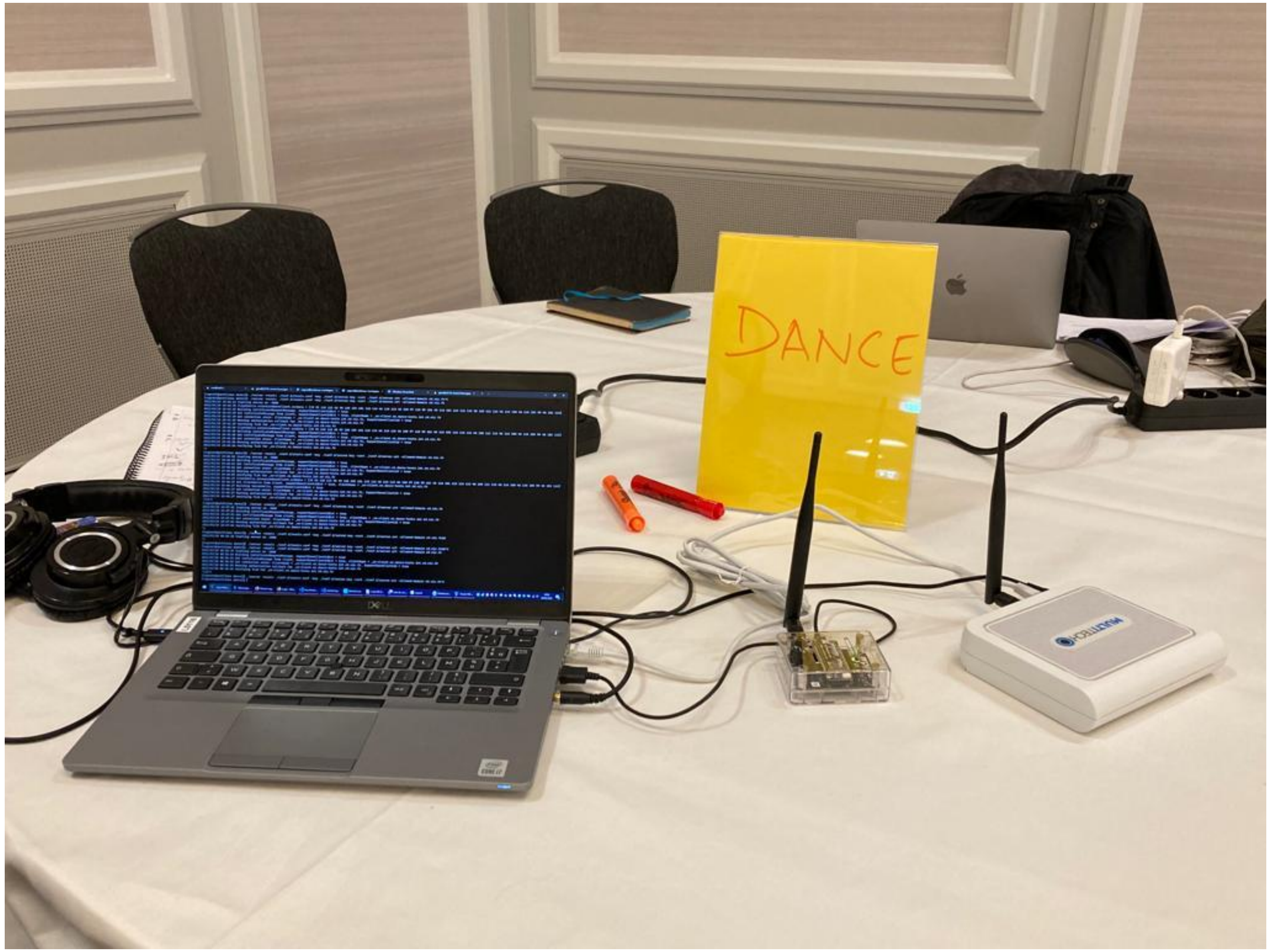
- What has been done during the Hackathon?
    - Environment for testing TLS Client/Server authentication
    - Authentication based on dane_clientid (Both for TLS 1.2 & TLS 1.3)
    - Fallback to authentication using SAN when dane_clientid is not sent
    - Possibility of whitelisting & authorization rules for which dane_clientid to accept

Dane-clientid draft

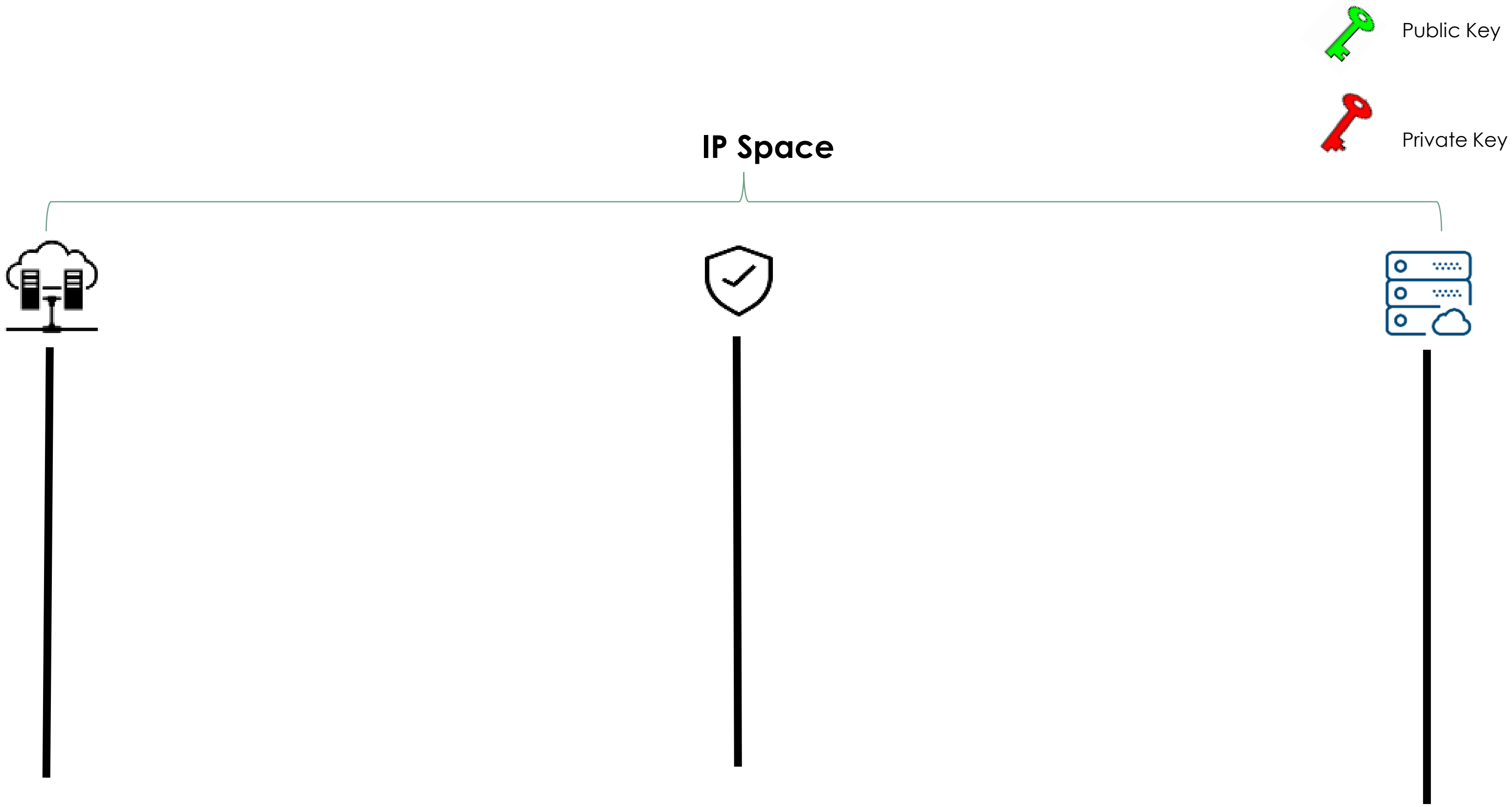
- Extending TLS 1.2 & TLS 1.3 library to use the new value dane_clientid extension

- Adding the dane_clientid support for TLS 1.2 & TLS 1.3 handshake

Deploying the Updates in an IoT use-case - LoRaWAN



Mutual Authentication in the LoRaWAN IP Space



🟩 Public Key

🟥 Private Key

IP Space

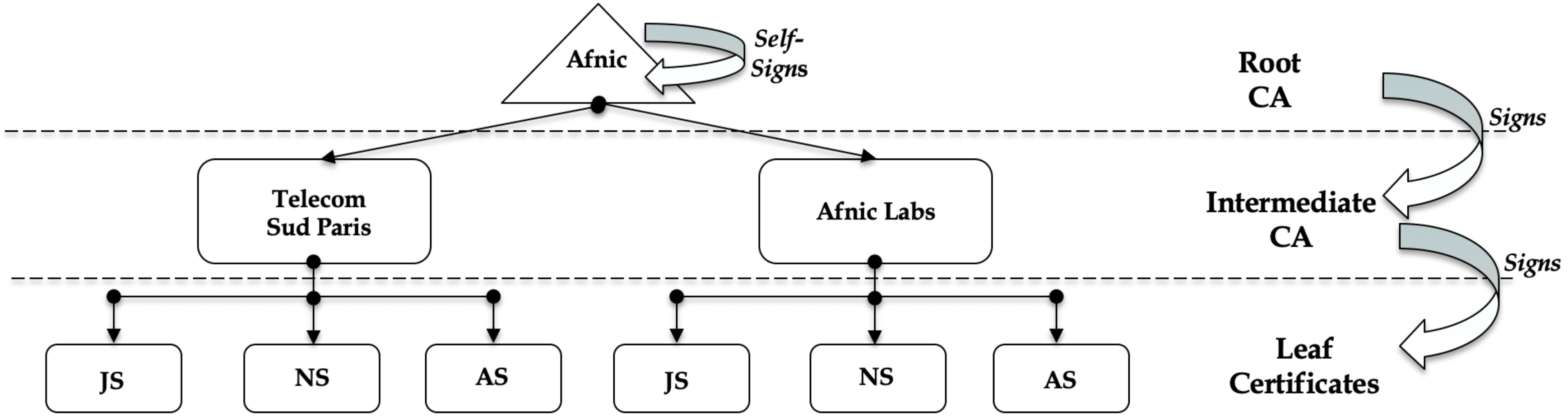
Issues with the Web PKI

- CA bundle not available in most cases

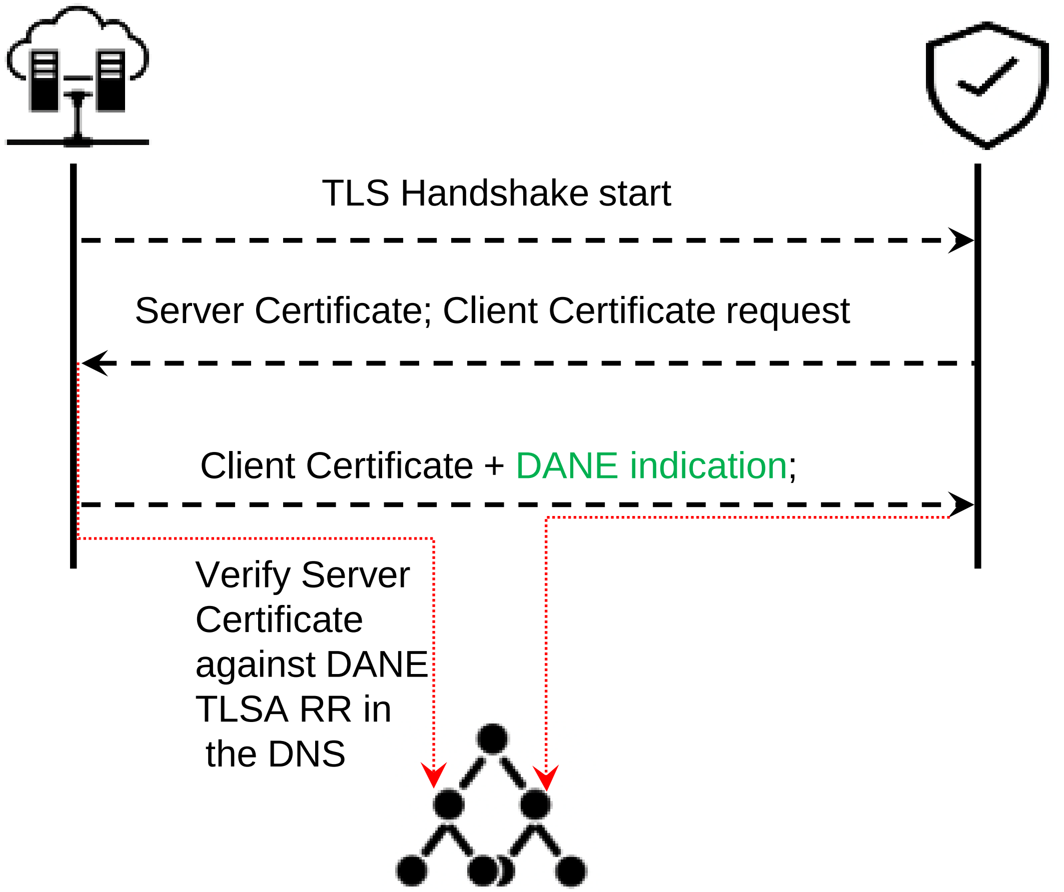
- Web PKI CA adds Cost –> Possible Solution: *Self-Signed*

- Private PKI – Since the trust is based on a single Root CA

Web PKI – Self Signed Certificate Provisioning



DANE Client authentication with TLS 1.2 & TLS 1.3



TLS Handshake start

Server Certificate; Client Certificate request

Client Certificate + DANE indication;

Verify Server Certificate against DANE TLSA RR in the DNS