Nov. 11 2022

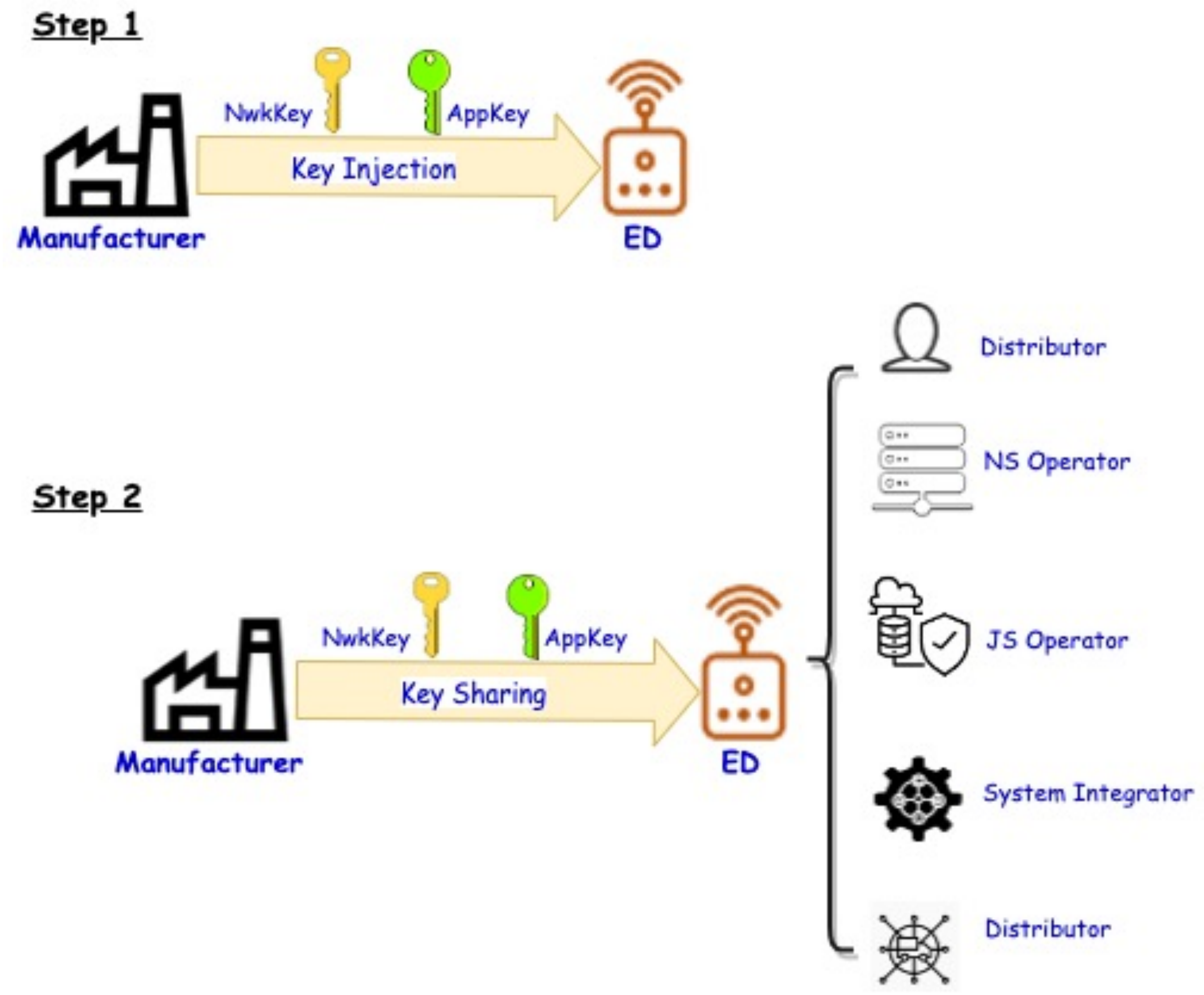
afnic
Internet
made in France

LoRaWAN Use case update

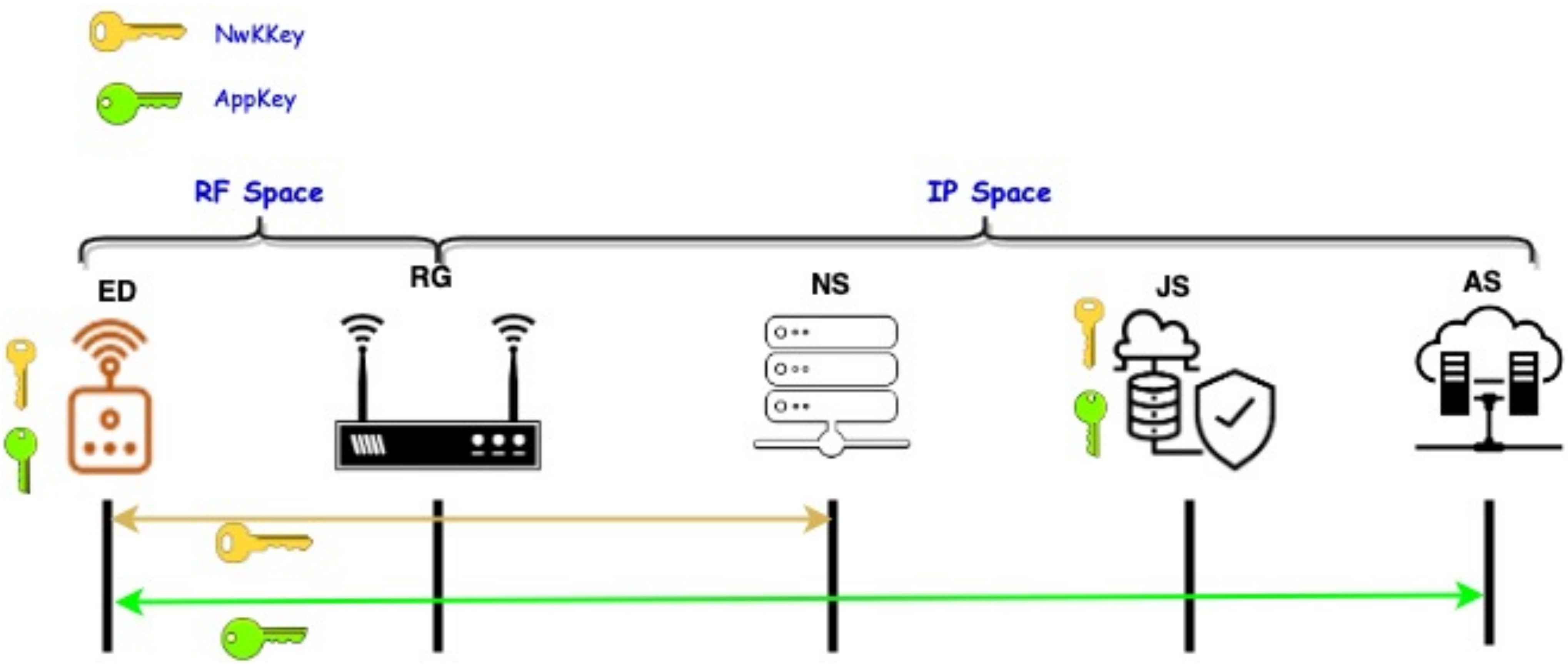
DANCE WG

Presented at IETF DANCE WG @London(2022)

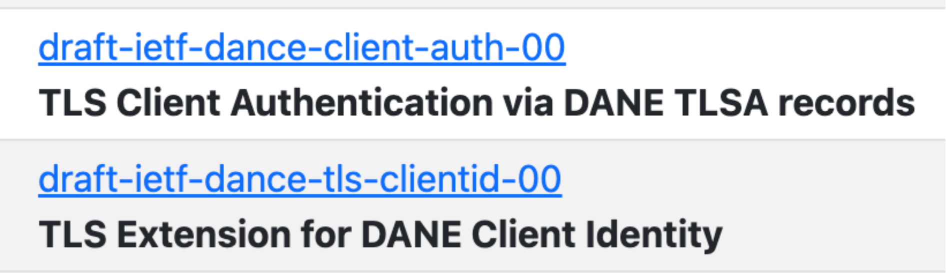
Key Sharing Challenge in IoT



IoT Use case - LoRaWAN Key Distribution



Using DANE indication Client/Server Authentication – Federated CA's

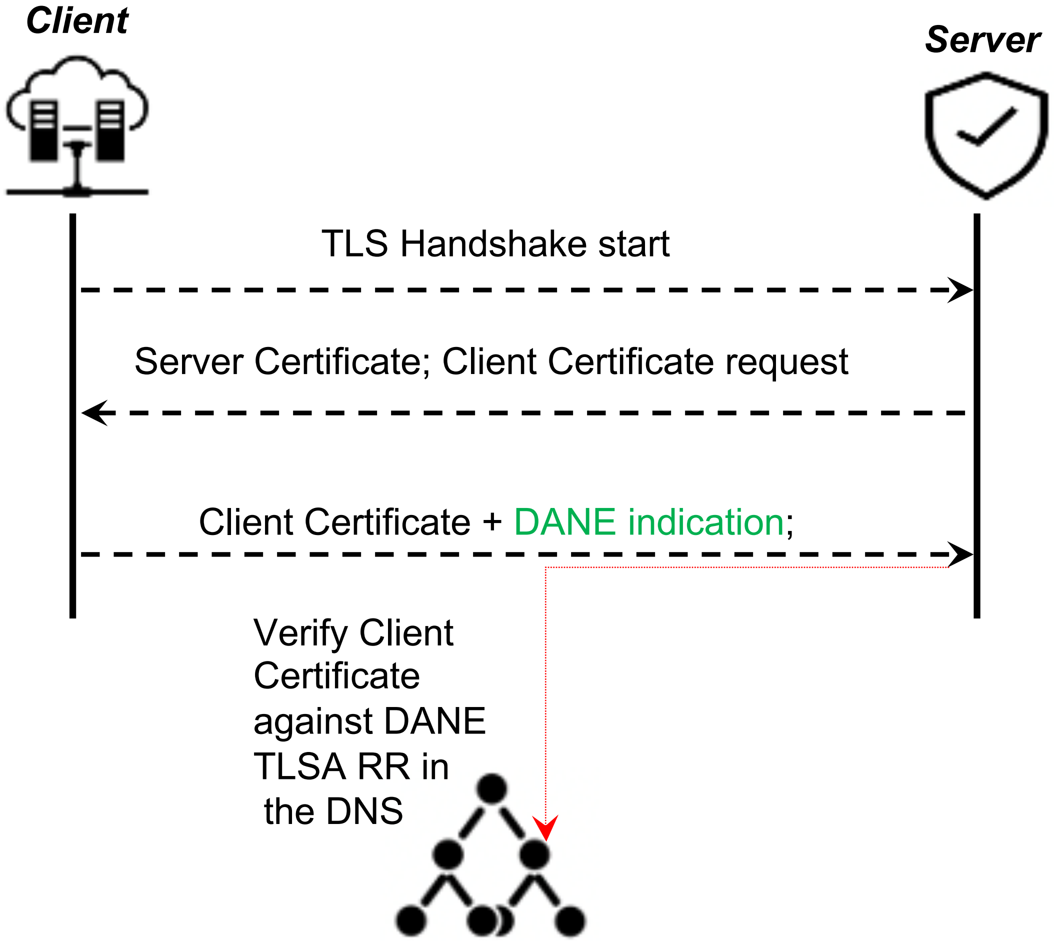


draft-ietf-dance-client-auth-00

TLS Client Authentication via DANE TLSA records

draft-ietf-dance-tls-clientid-00

TLS Extension for DANE Client Identity



Client

Server

TLS Handshake start

Server Certificate; Client Certificate request

Client Certificate + DANE indication;

Verify Client Certificate against DANE TLSA RR in the DNS

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

Work done

- Existing Implementation
  - go library for DANE TLSA authentication (Author: Shumon Huque)
- Environment for testing TLS Client/Server authentication
- Client ID draft
  - 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
- Client Cert draft
  - Adding the dane_clientid support (Both for TLS 1.2 & TLS 1.3)
  - Extending TLS 1.2 & TLS 1.3 library to use the new value dane_clientid extension

Work done during IETF 115 Hackathon

- AAA Server authentication for the IoT device using DNSSEC authentication Chain