Nov. 06 2022

DNSSEC Chain implementation

DANCE WG

Internet made in France

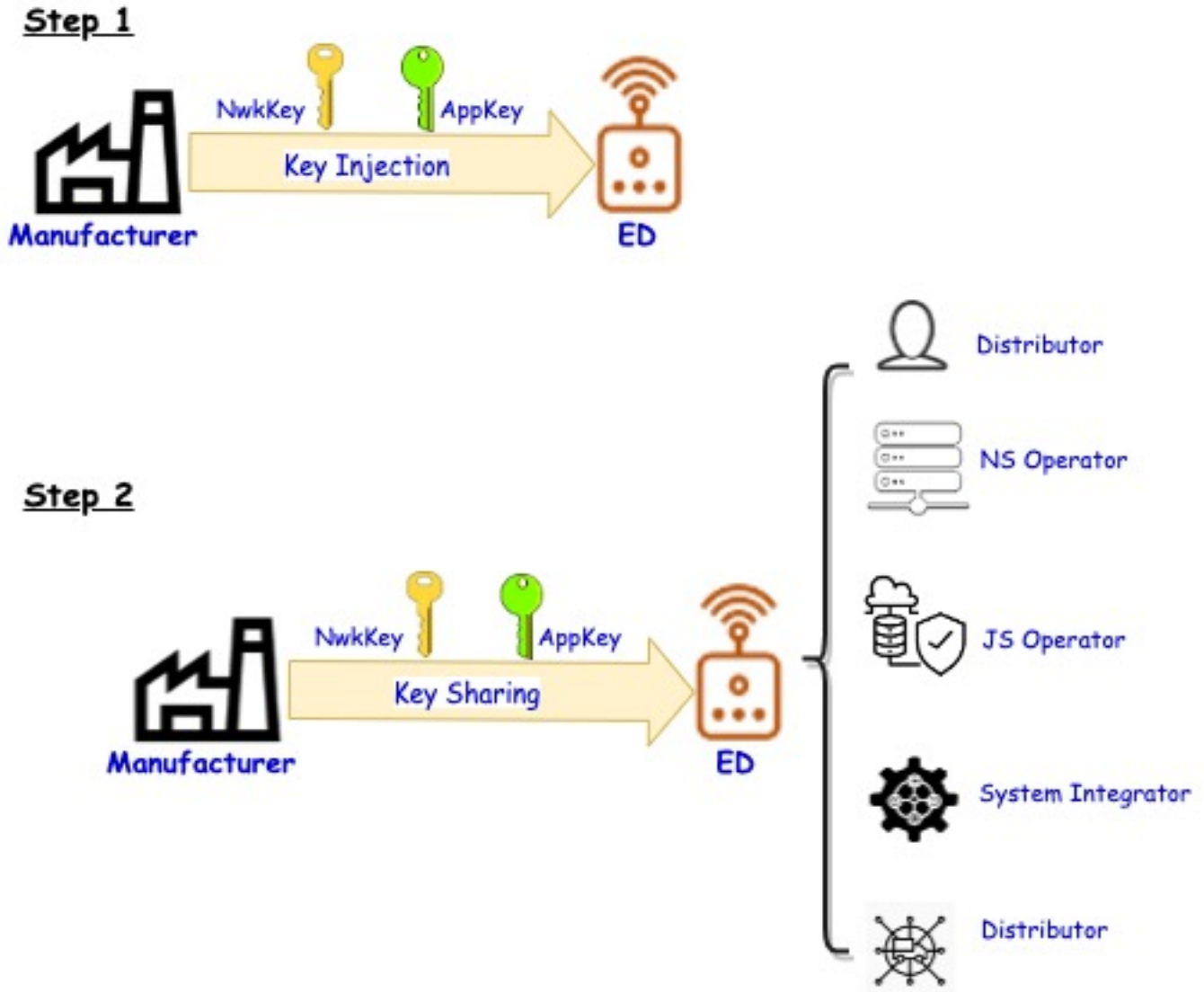
Presented at IETF Hackathon @London(2022)

afnic | Labs

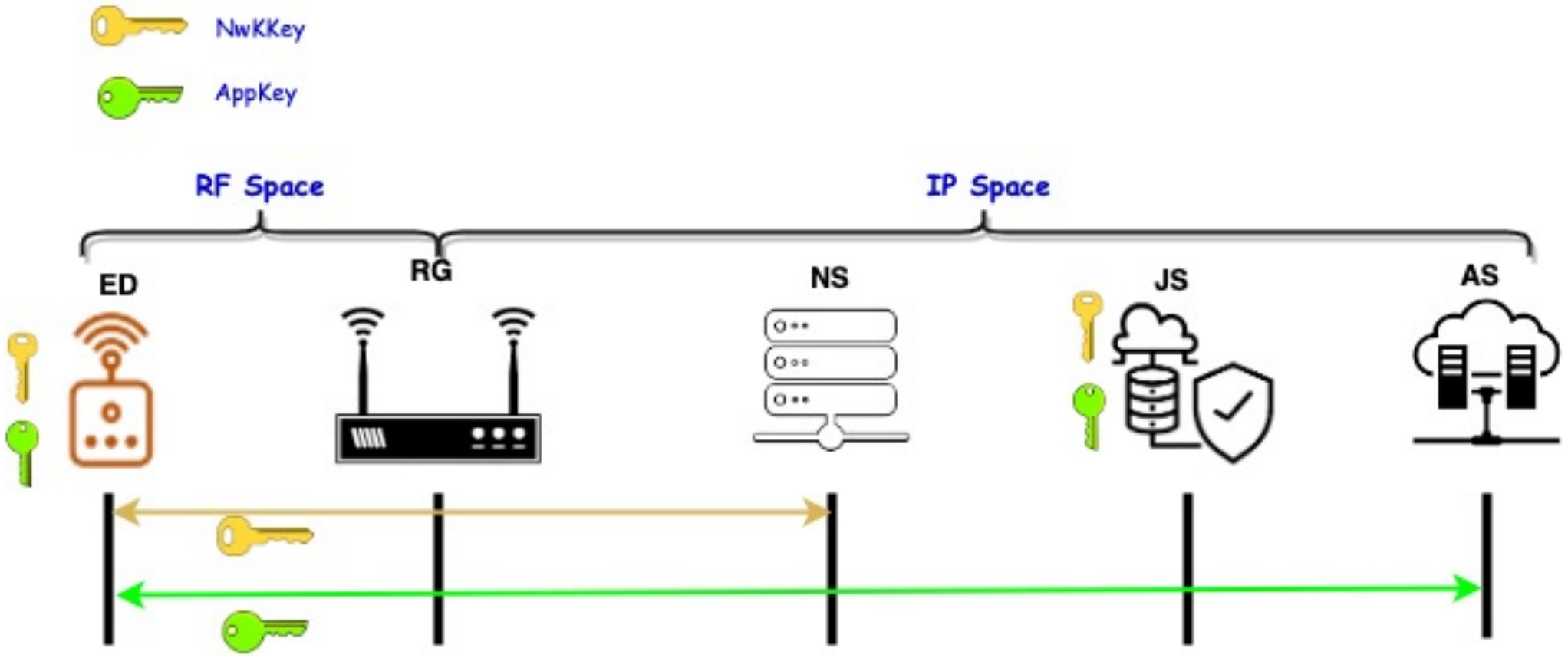
Agenda

- About Afnic

Key Sharing Challenge in IoT

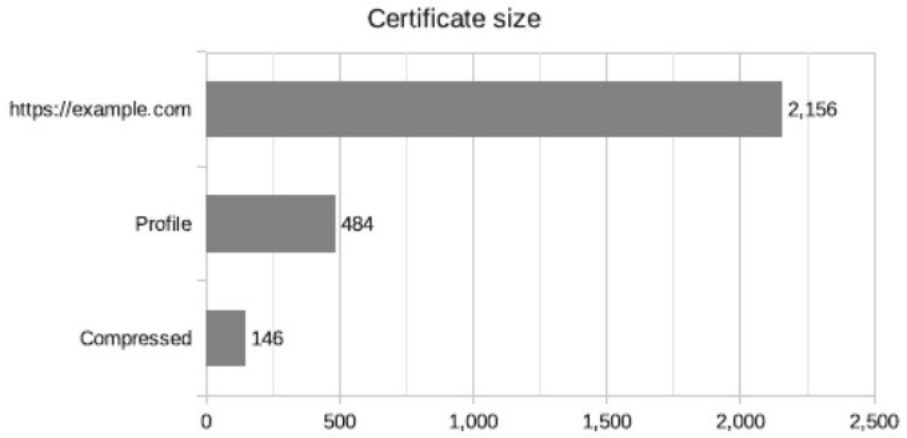


IoT Use case - LoRaWAN Key Distribution



X.509 Certificates cannot be directly employed in the LoRa RF space

F. Forsby et al.



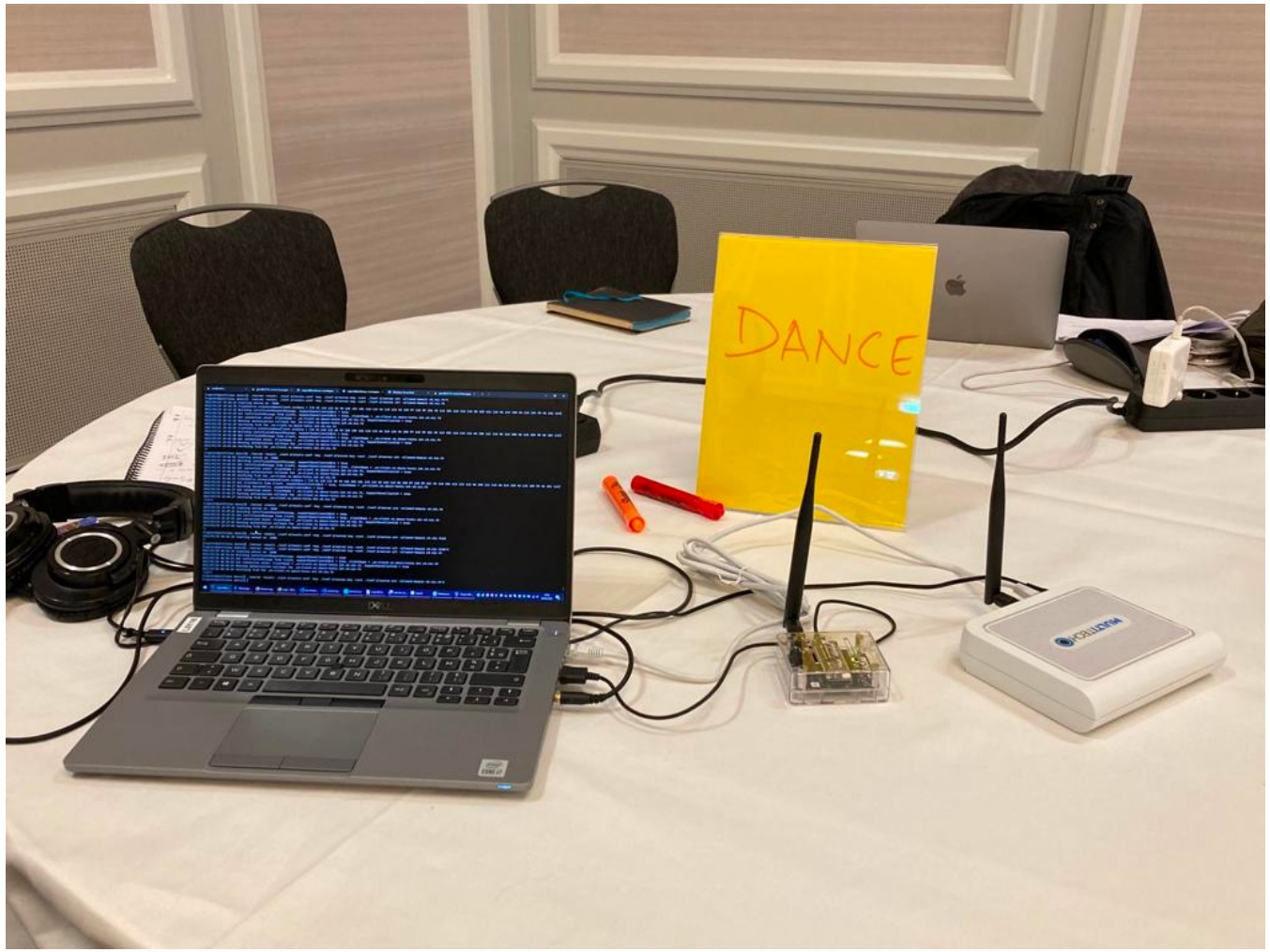
Data Rate (DR)	Spreading Factor (SF)	Channel Frequency	Uplink or Downlink	Bitrate (Bits/Sec)	Maximum User Payload Size (Bytes)
0	SF10	125 kHz	Uplink	980	11
1	SF9	125 kHz	Uplink	1,760	53
2	SF8	125 kHz	Uplink	3,125	125
3	SF7	125 kHz	Uplink	5,470	242
4	SF8	500 kHz	Uplink	12,500	242
5 – 7					
8	SF12	500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

Drafts that we worked on

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

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

Deploying the Updates in an IoT use-case - LoRaWAN



Existing work

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

- What has been done during the IETF 113 Hackathon?
  - Environment for testing TLS Client/Server authentication
  - 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
  - Fallback to authentication using SAN when dane_clientid is not sent
  - Possibility of whitelisting & authorization rules for which dane_clientid to accept

Work done during IETF 115 Hackathon

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