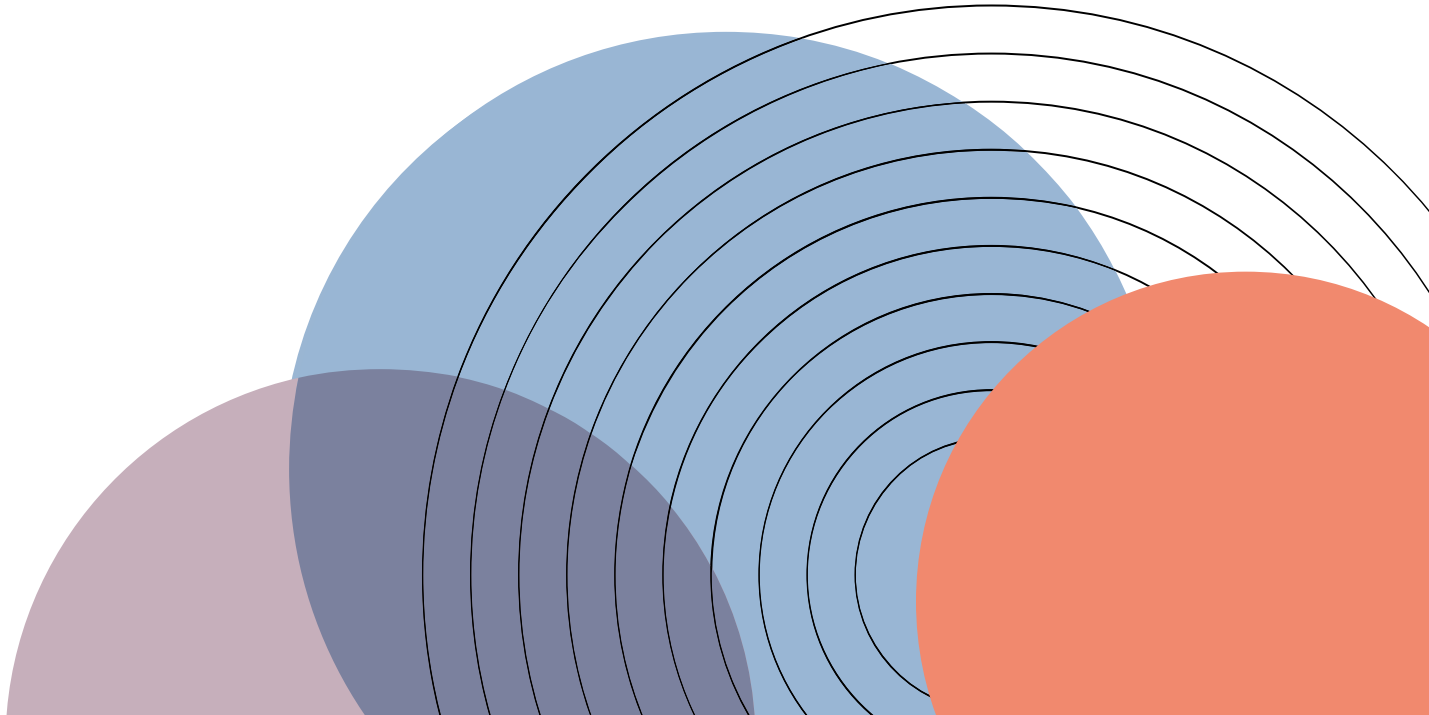
20 mars 2022

afnic
Internet
made in France

IETF 113 Hackathon – DANCE WG



Drafts that we worked on

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

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

Dane-client-cert draft

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

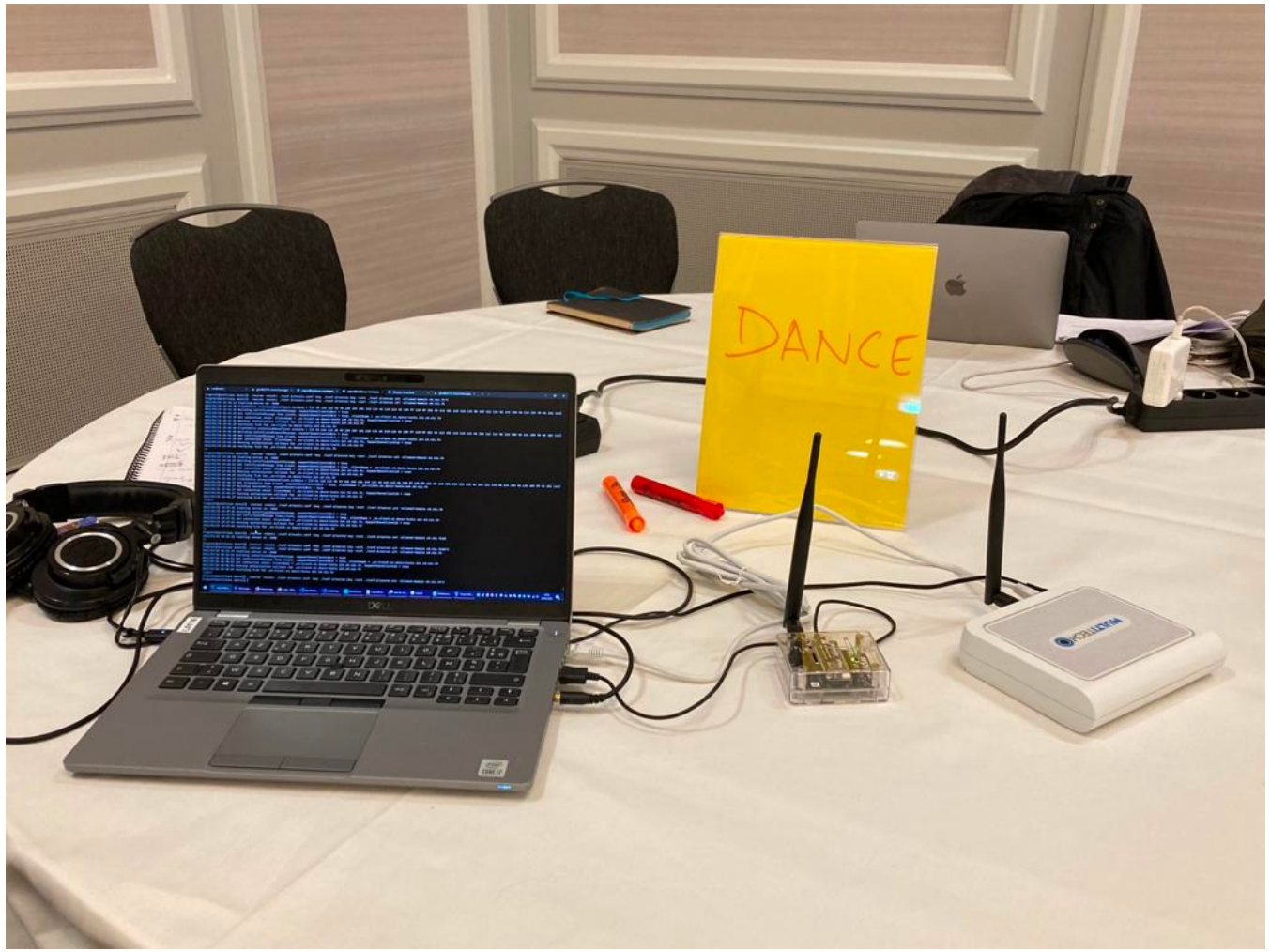
- What has been done during the Hackathon?
  - Environment for testing TLS Client/Server authentication
  - Authentication based on dane_clientid (Both for TLS 1.2 & TLS 1.3)
  - Fallback to authentication using SAN when dane_clientid is not sent (empty ext data)
  - Support for allow-lists & authorization 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

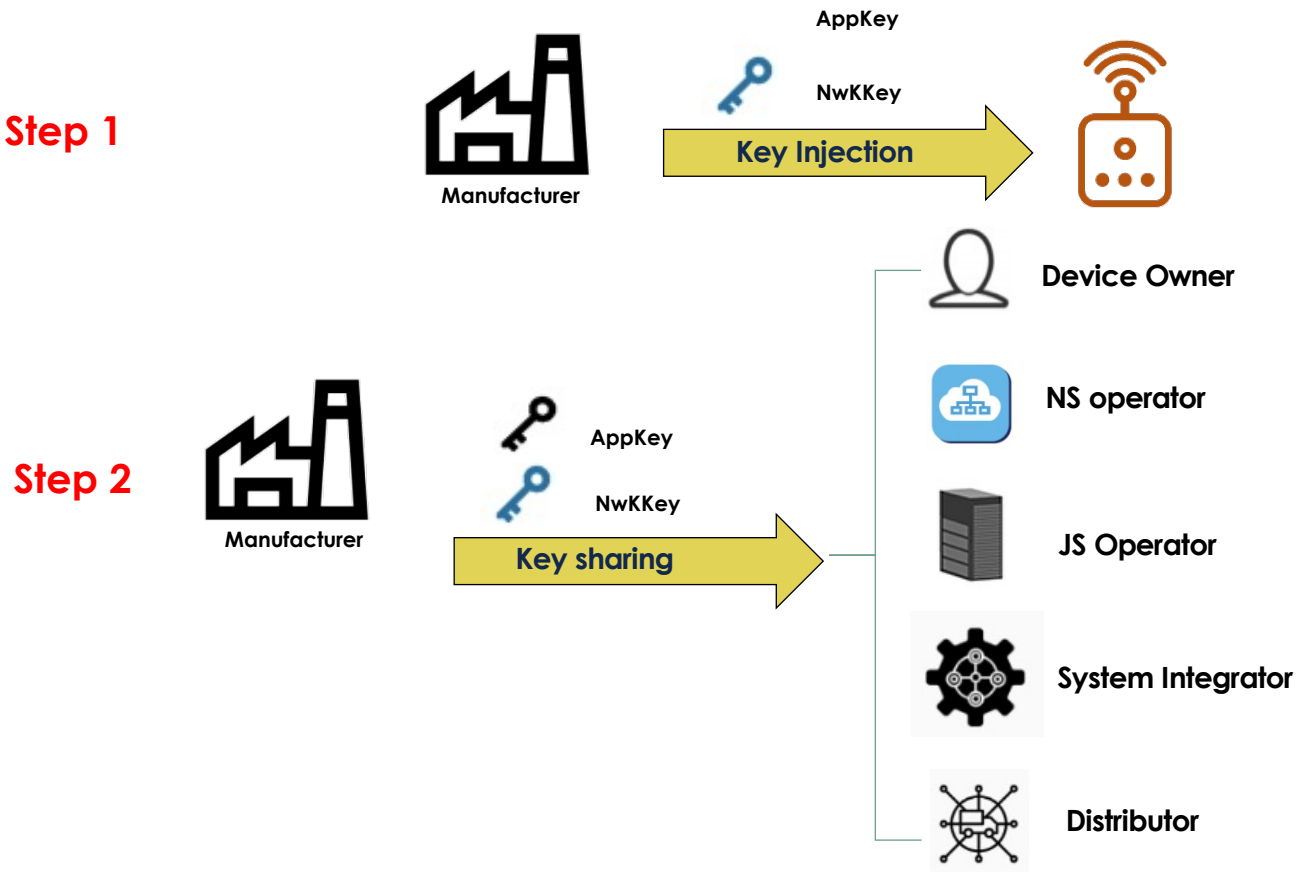
- Adding the dane_clientid support for TLS 1.2 & TLS 1.3 handshake

Deploying the Updates in an IoT use-case - LoRaWAN



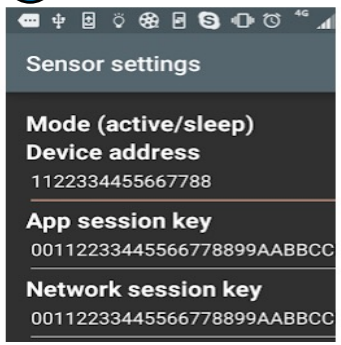
Brief LoRaWAN Background

Key Sharing Challenges in LoRaWAN



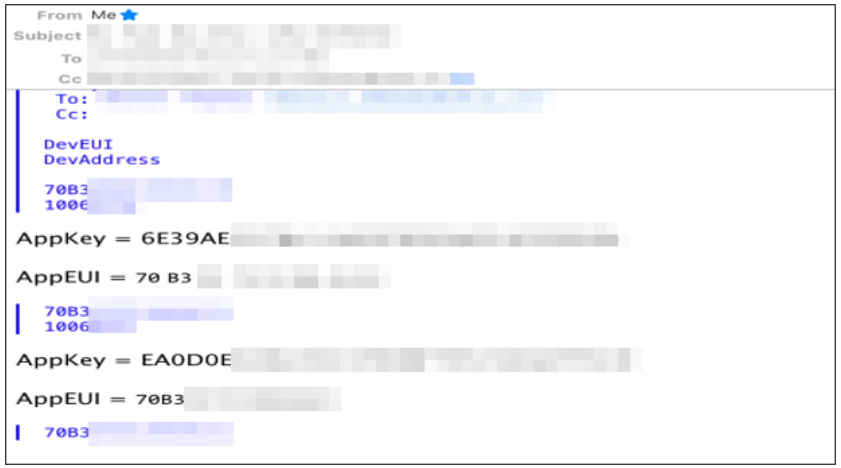
How the Keys are shared between different Stakeholders?

1 Accessible via NFC
On mobile phones

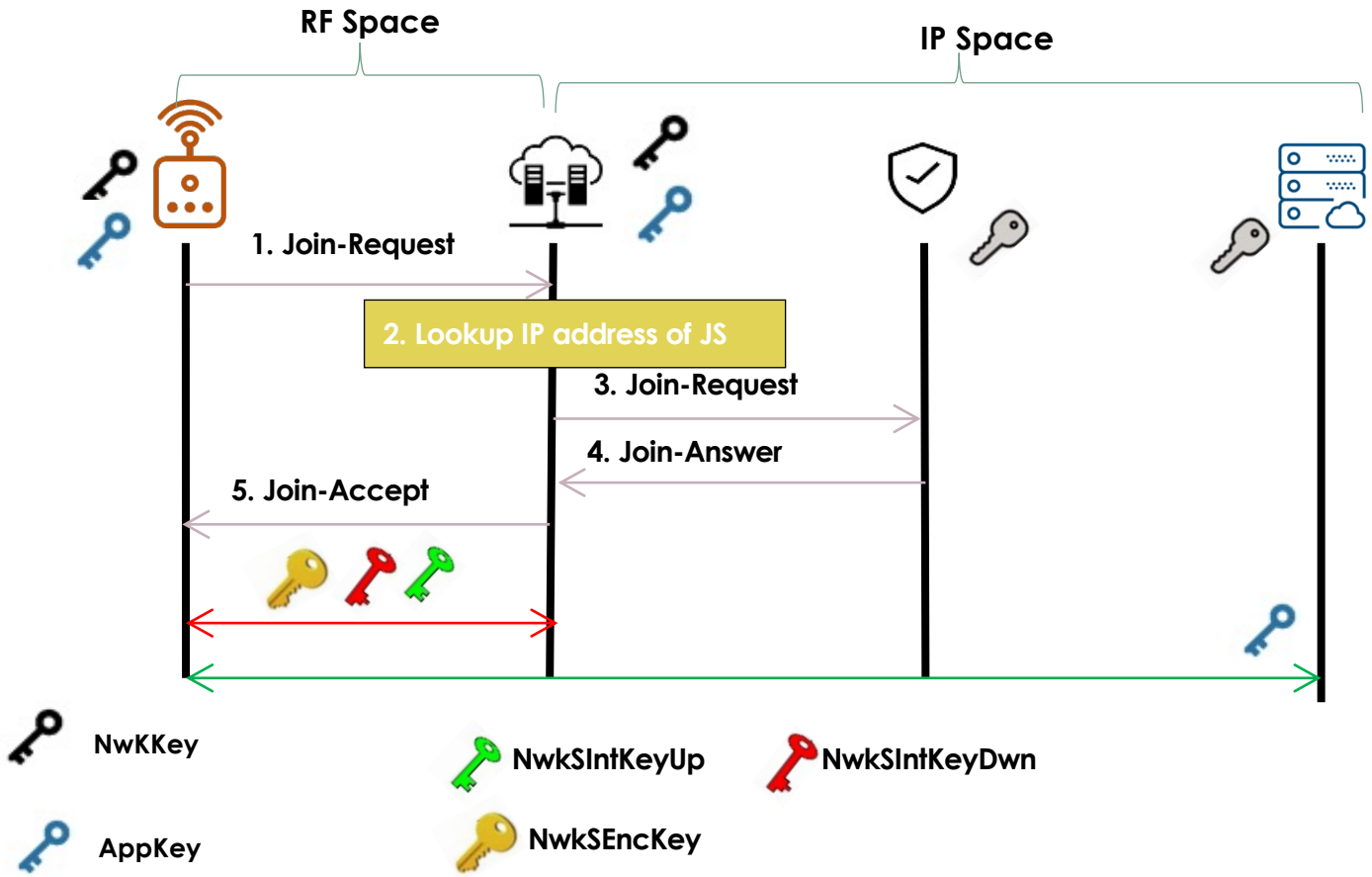


2 Printed behind the ED

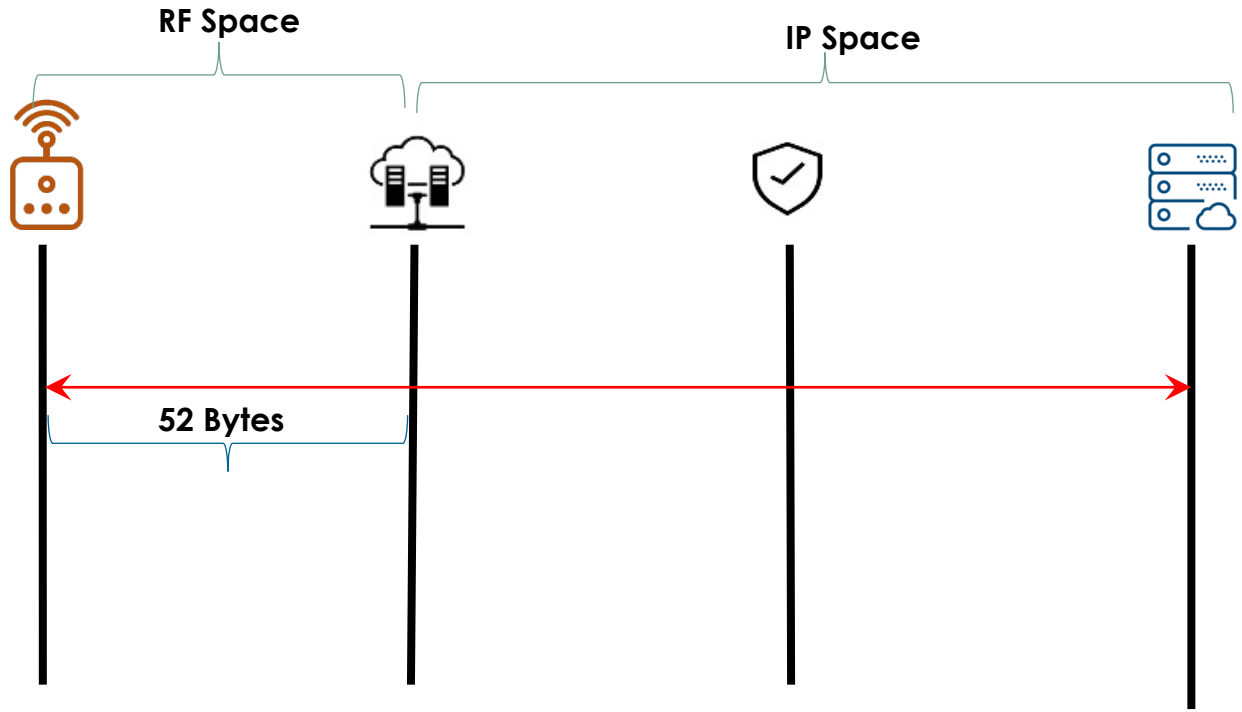
3 Sent via mail



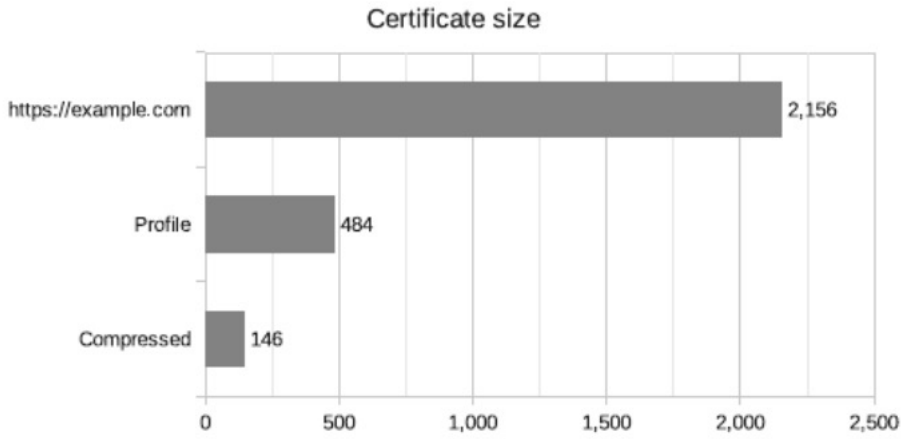
ED Onboarding using PSK (Symmetric Keys)



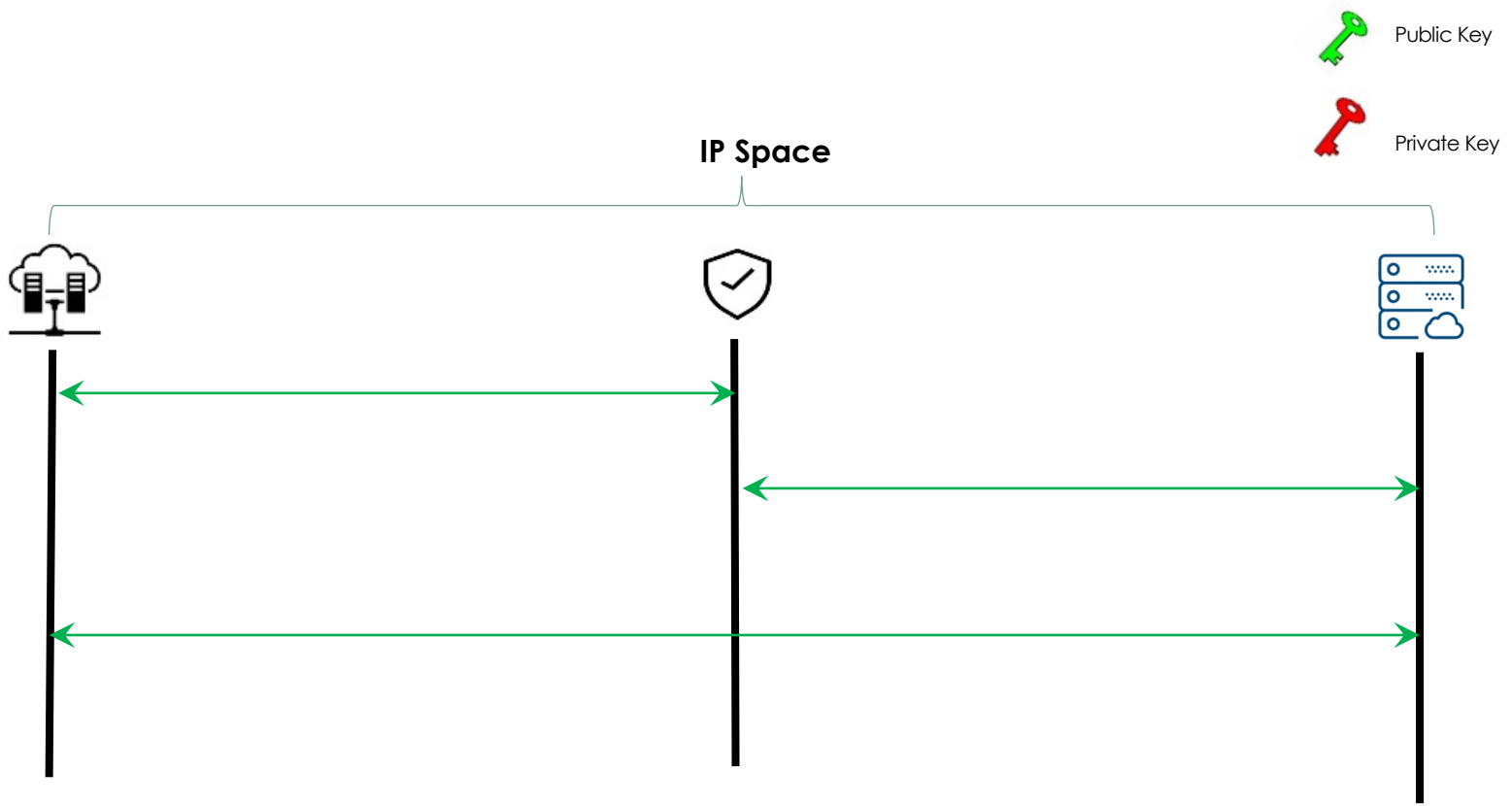
Currently End-To-End security is not possible using asymmetric keys



F. Forsby et al.



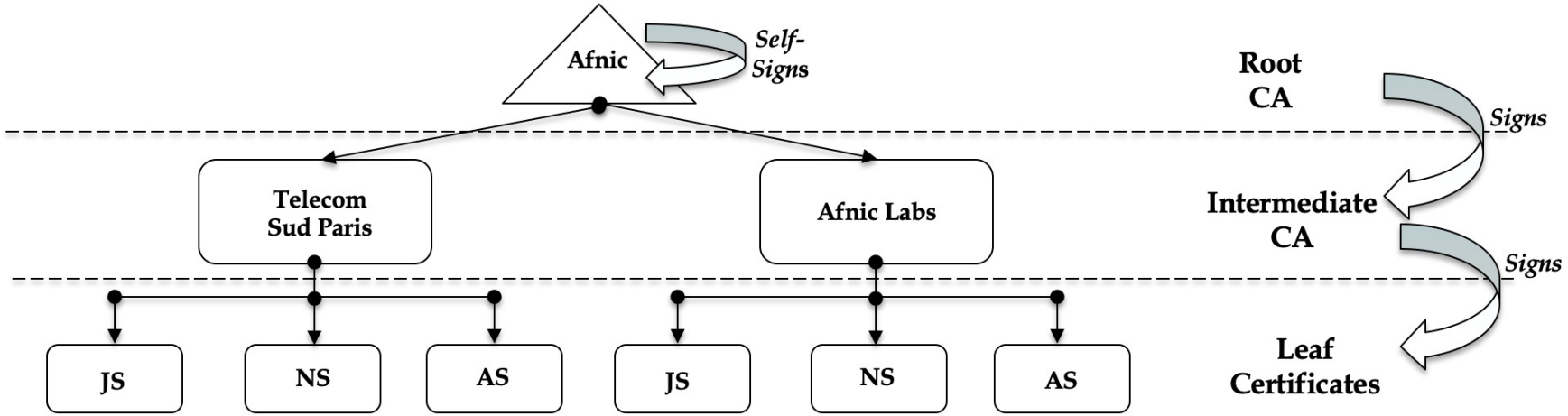
Focus is on Mutual Authentication in the LoRaWAN IP Space



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

Currently – Trust is Siloed

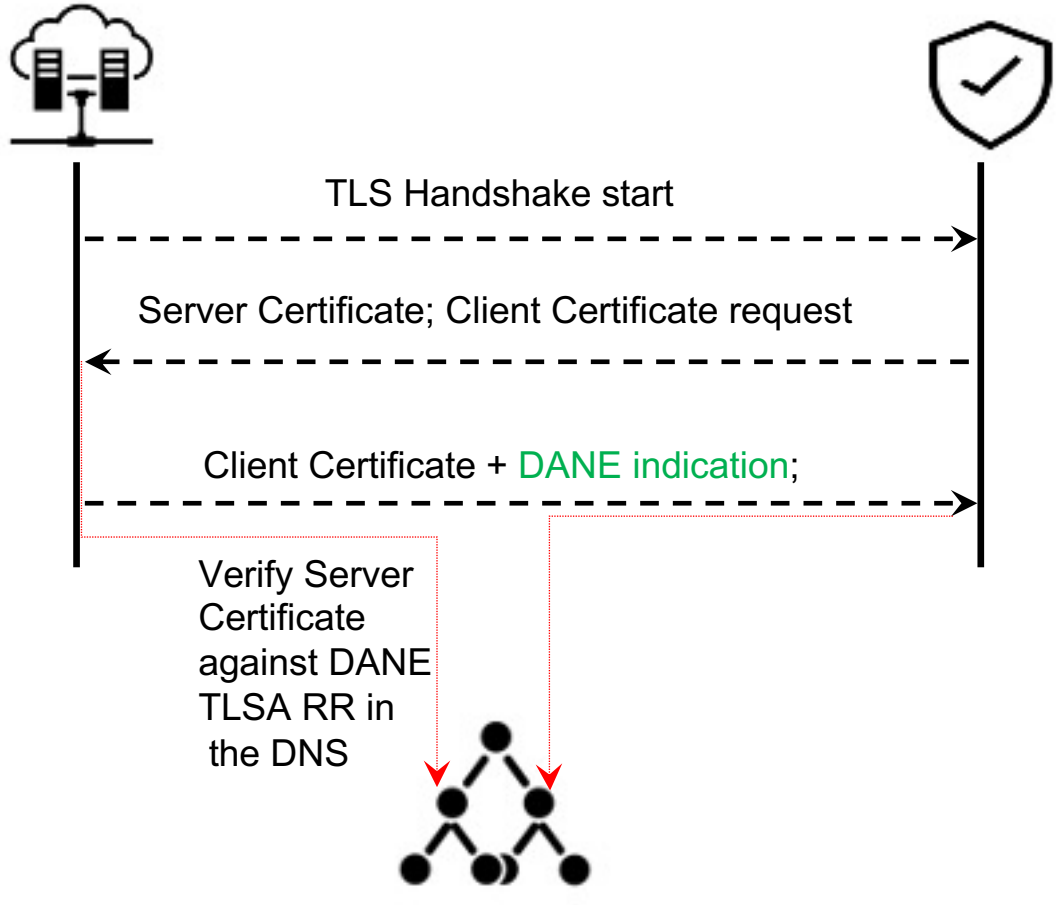


iotreg.net

netids.iotreg.net	joineuis.iotreg.net
XXX.netids.iotreg.net IN AAAA	Z.Y.X.joineuis.iotreg.net IN AAAA

DANE Client authentication with TLS 1.2 & TLS 1.3

- *DANE Client ID has made it possible to mutually authenticate between different private PKI's*



iotreg.net

netids.iotreg.net

XXX.netids.iotreg.net IN AAAA
_ns-client.XXX.netids.iotreg.net IN TLSA

joineuis.iotreg.net

Z.Y.X.joineuis.iotreg.net IN AAAA
_443._tcp.Z.Y.X.joineuis.iotreg.net IN TLSA