Asymmetric cryptography for LoRaWAN

Sandoche BALAKRICHENAN

Oct. 11 2022

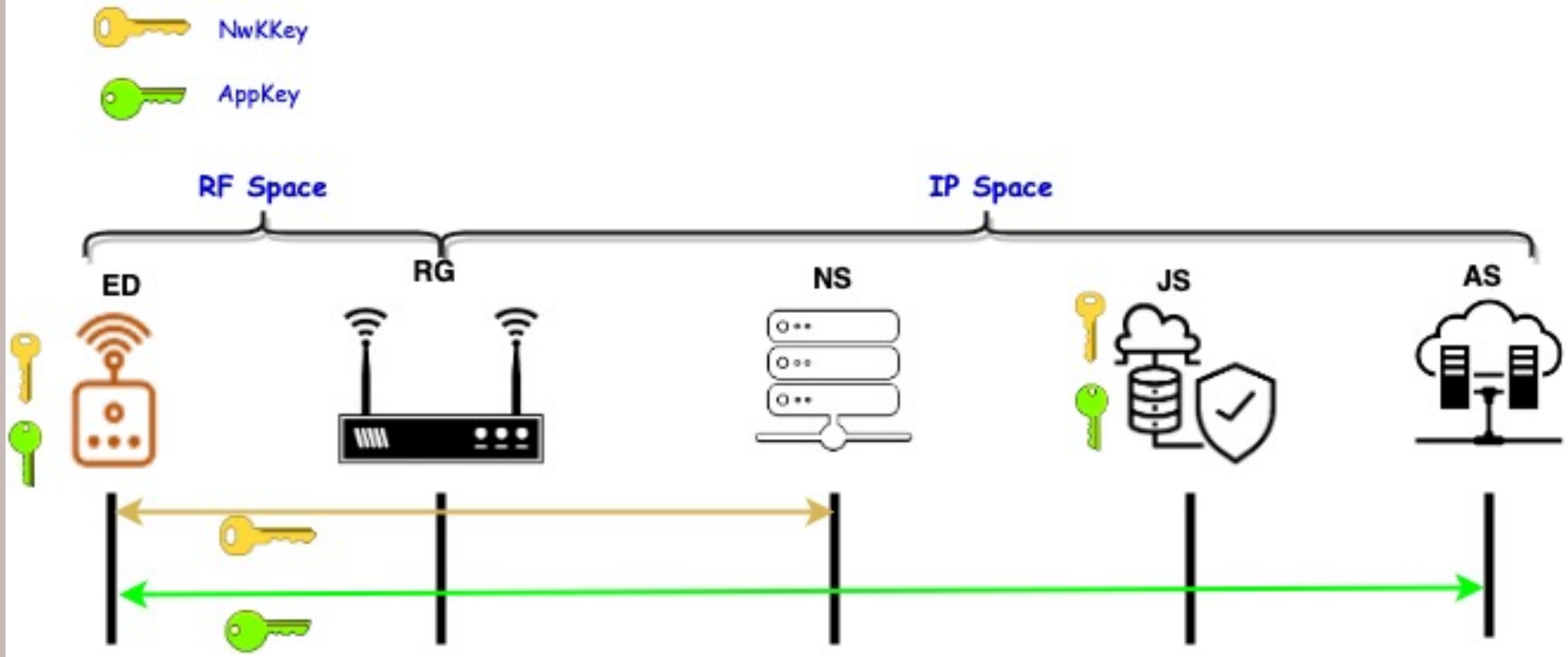
afnic
Internet
made in France

Presented at TC – SFO (2022)

Fundamental security properties that need to be supported in LoRaWAN

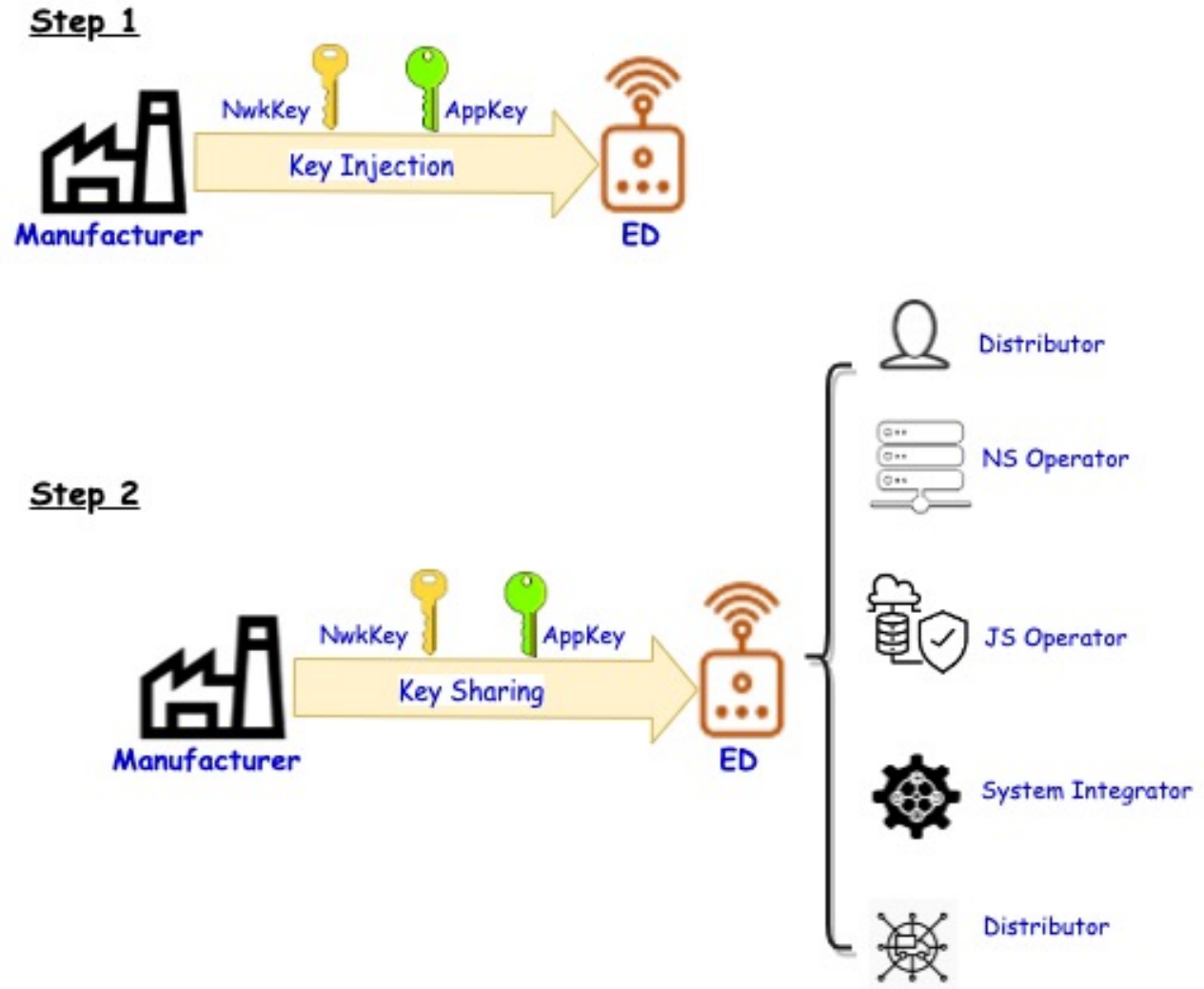
- Integrity protection
- Confidentiality
- Mutual Authentication
- Replay Protection

afnic | Labs Symmetric Cryptography & RF, IP Space



afnic | Labs

Key Sharing Dilemma in LoRaWAN



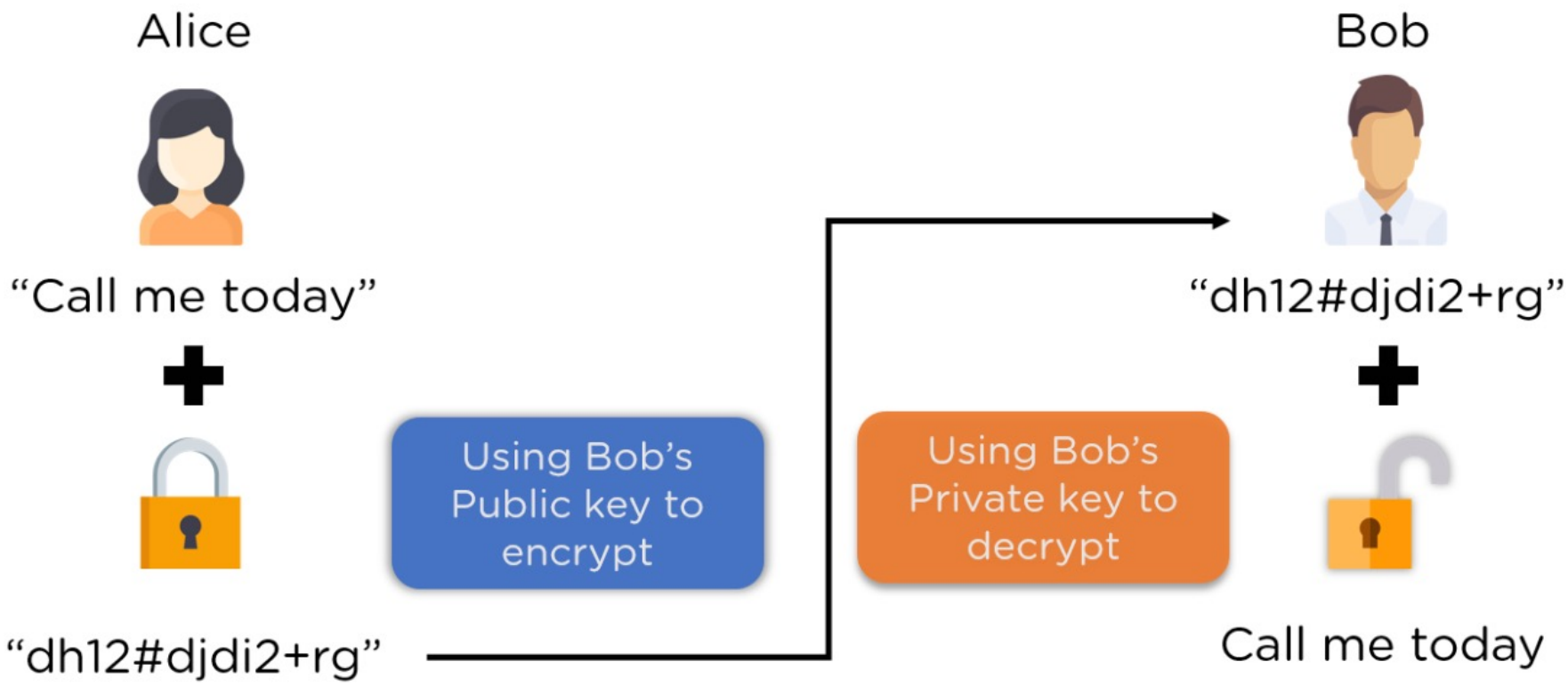
IP Space interfaces (Backend Network Elements)

- AS-JS
- JS-NS
- NS-NS

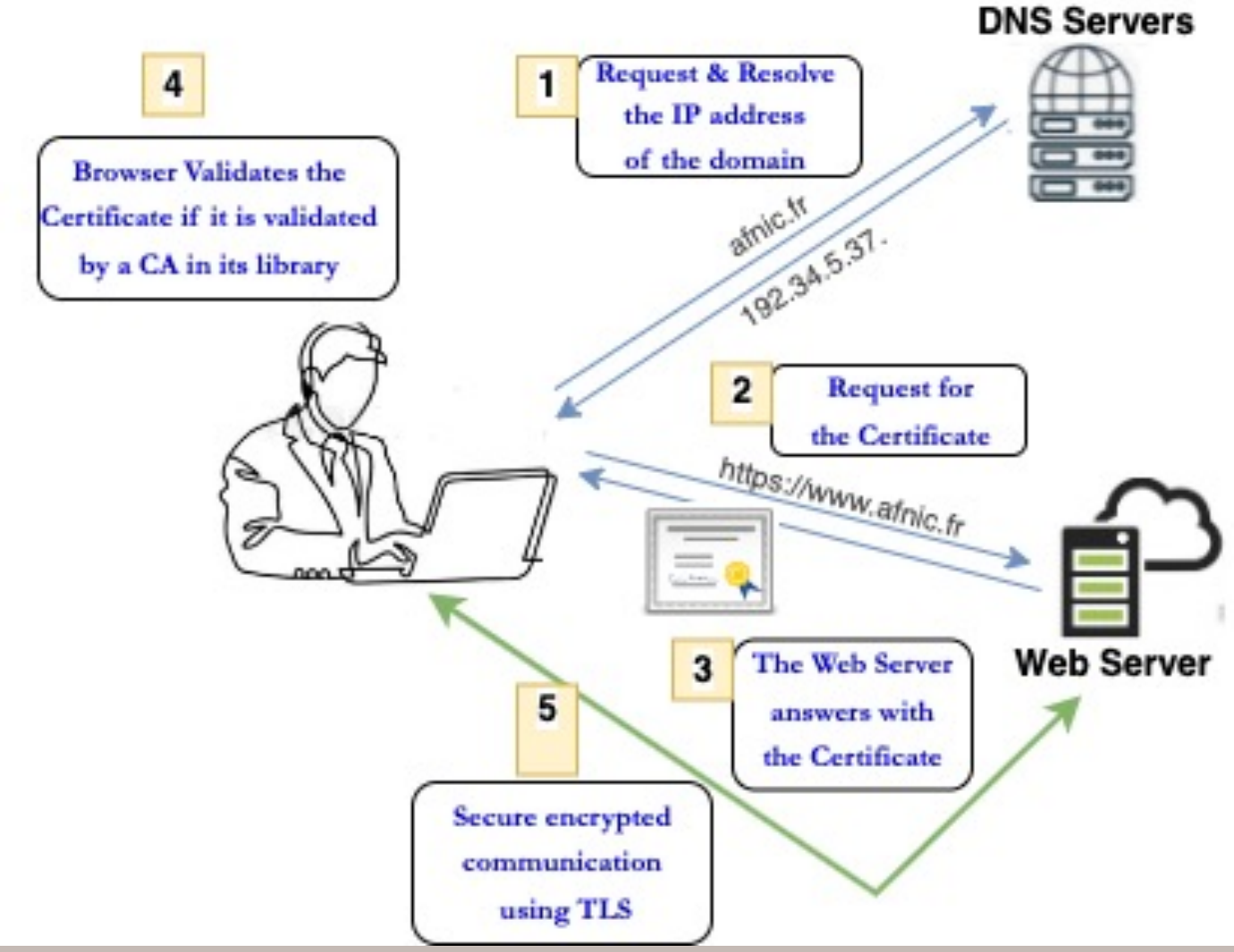
From Section 21 of the Backend Specifications:

> 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.)

Asymmetric Cryptography - primer



Securing Web communication – Asymmetric Cryptography

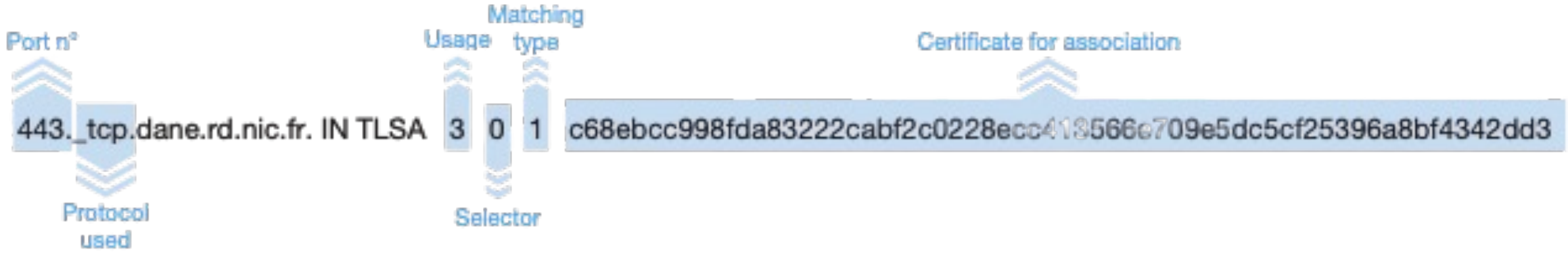


Using the web based *asymmetric cryptography (PKIX)* in IP space

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. Our Price: **$7.27**/yr.	Listed Price: $179.95/yr. Our Price: **$56.06**/yr.	Listed Price: $149.00/yr. Our Price: **$74.99**/yr.

DNS Based PKI using DNSSEC (RFC 4033, 4034 & 4035) & DANE (RFC 6698, 7671)



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

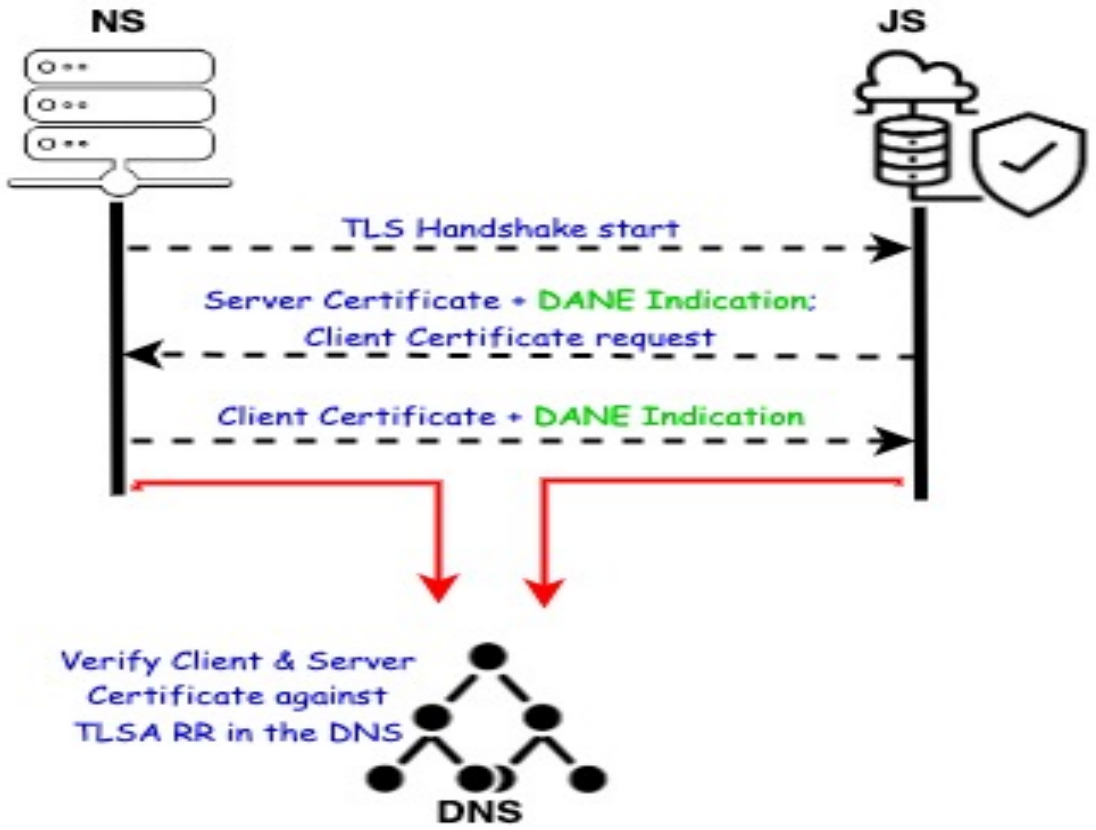
draft-ietf-dance-client-auth-00

TLS Client Authentication via DANE TLSA records

draft-ietf-dance-tls-clientid-00

TLS Extension for DANE Client Identity

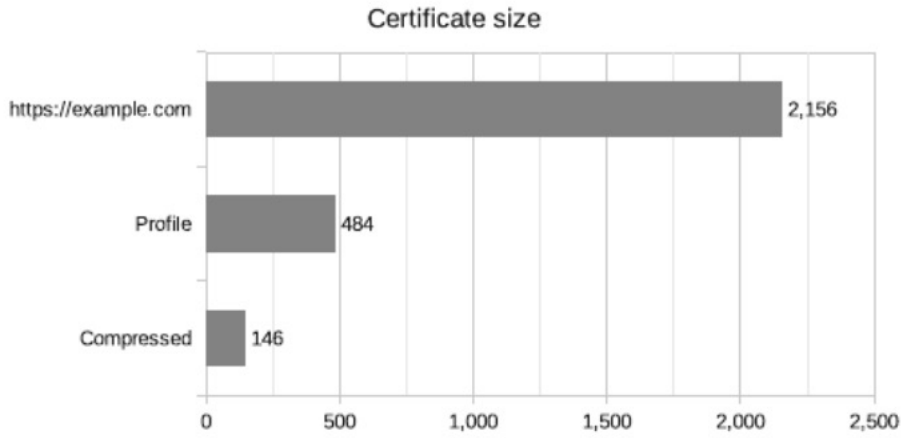
Afnic – First to implement and test the two IETF drafts during IETF 113 Hackathon



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

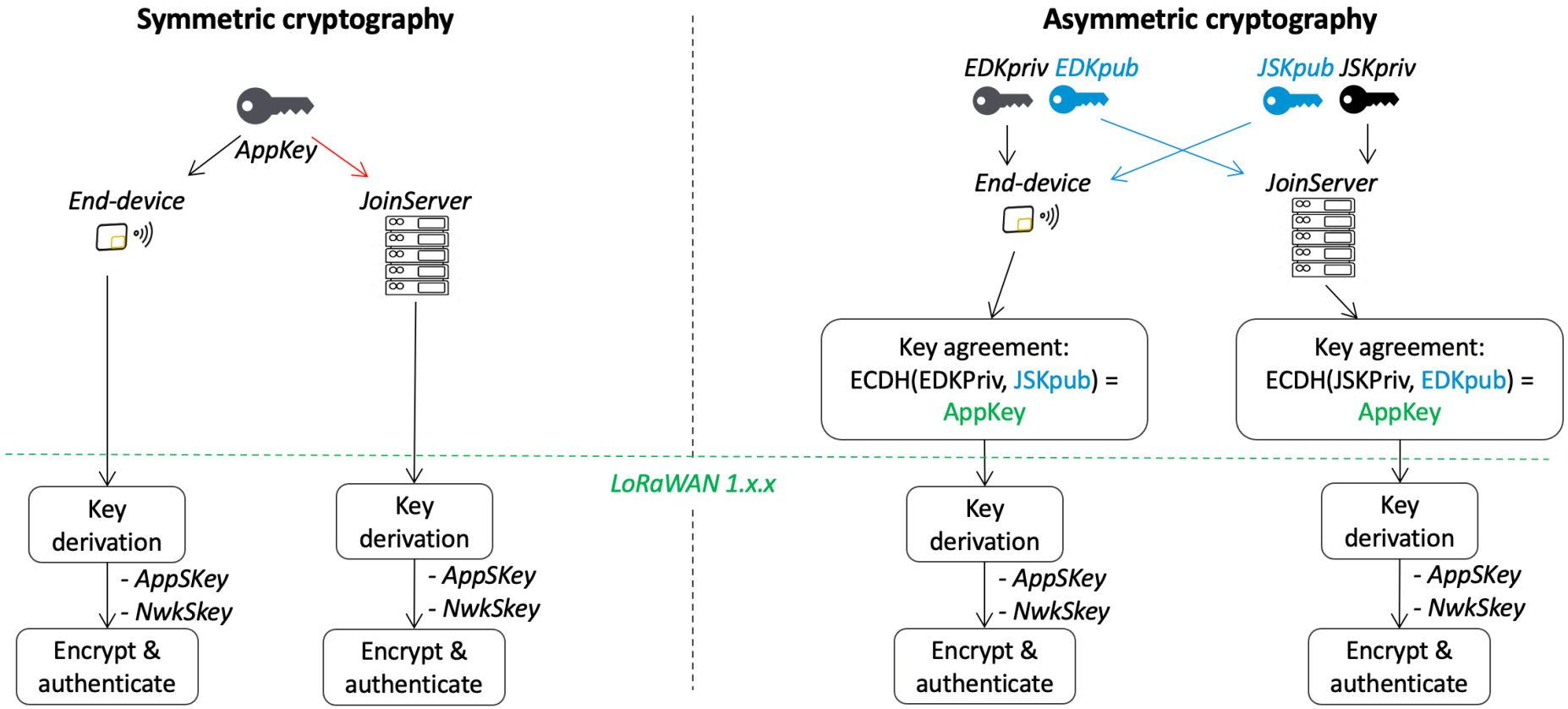
Web based X.509 digital certificates cannot be deployed directly in the RF space

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

An intermediate Solution..



Source: Kerlink

Implementation in the ED

```rust
fn main() {
    ecc::unset_rng();

    println!("Starting !");

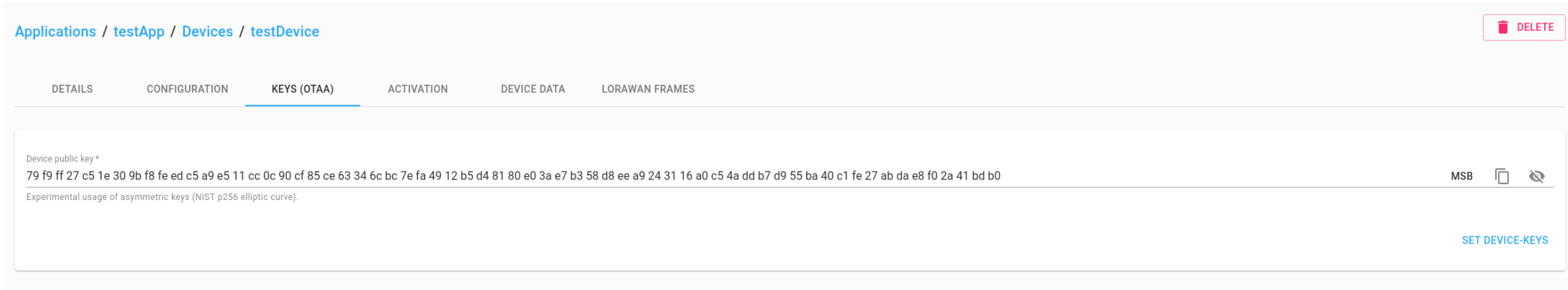
    let dev_sec = SecretKey::from_bytes(DEV_PRIV_KEY);
    let js_pub = log_unwrap!(PublicKey::from_uncompressed_bytes(JS_PUB_KEY), "Failed to load public key");

    let secret = log_unwrap!(dev_sec.shared_secret(&js_pub), "Could not compute shared secret");

    let secret_bytes = secret.as_bytes();
    println!("Computed shared secret, {:x?}", secret_bytes);
    let app_key = secret_bytes[0..16].try_into().unwrap();

    let mut lora = LoRa::from_global();
    lora.set_datarate(Datarate::LoRaMacDR5);
}
```

Implementation in JS (Chirpstack)



afnic | 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**

References

- **Afnic**
  - *https://github.com/AFNIC/Mutual-Authentication-via-DANE*
  - *https://gitlab.rd.nic.fr/tutoriels/The-DNS-to-Reinforce-the-PKIX*

- **External**
  - *IETF LPWAN (Low Power Wide Area Network) WG*
  - *IETF LAKE (Lightweight Authenticated Key Exchange) WG*