Oct. 11 2023

Zero Trust - DNS-based Identity and access management

afnic
Internet
made in France

Sandoche BALAKRICHENAN

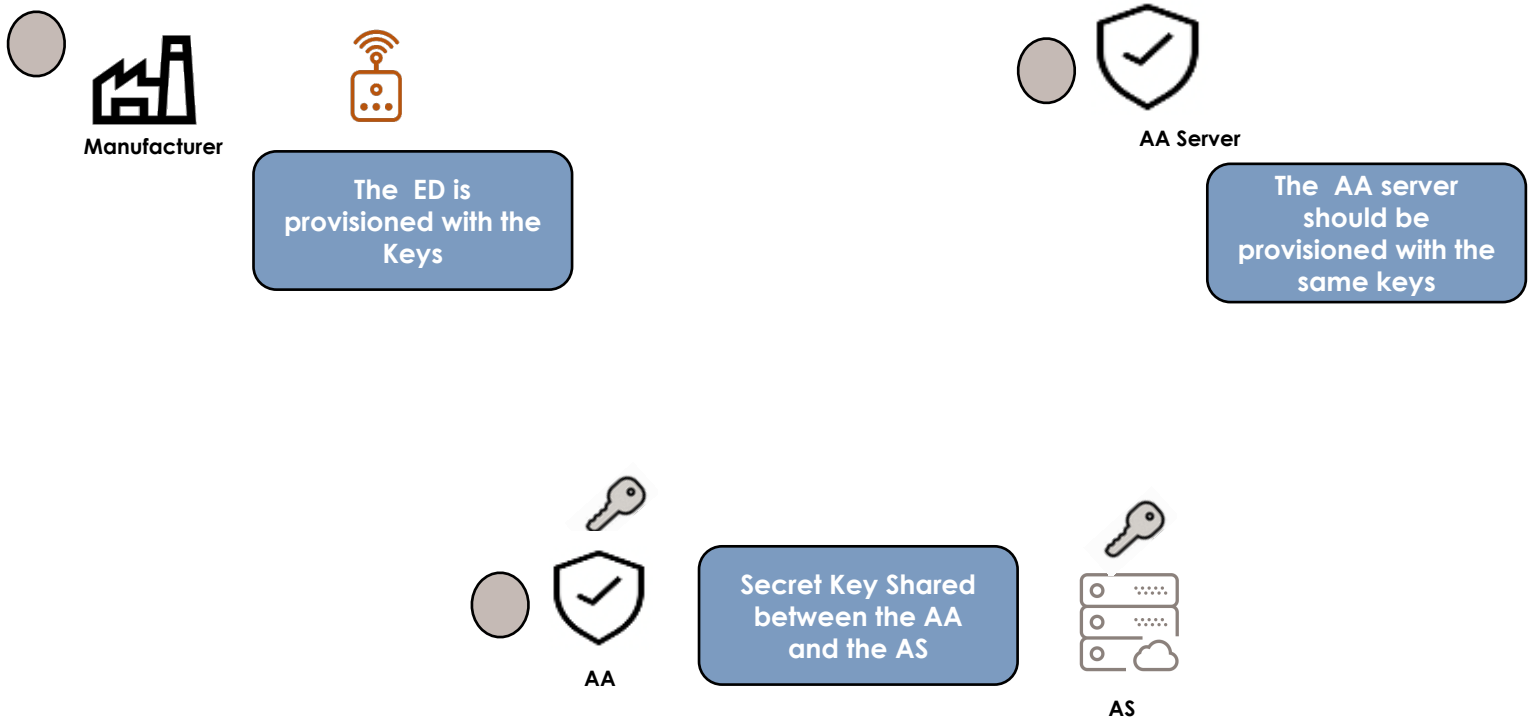
afnic | Labs

Zero trust definition

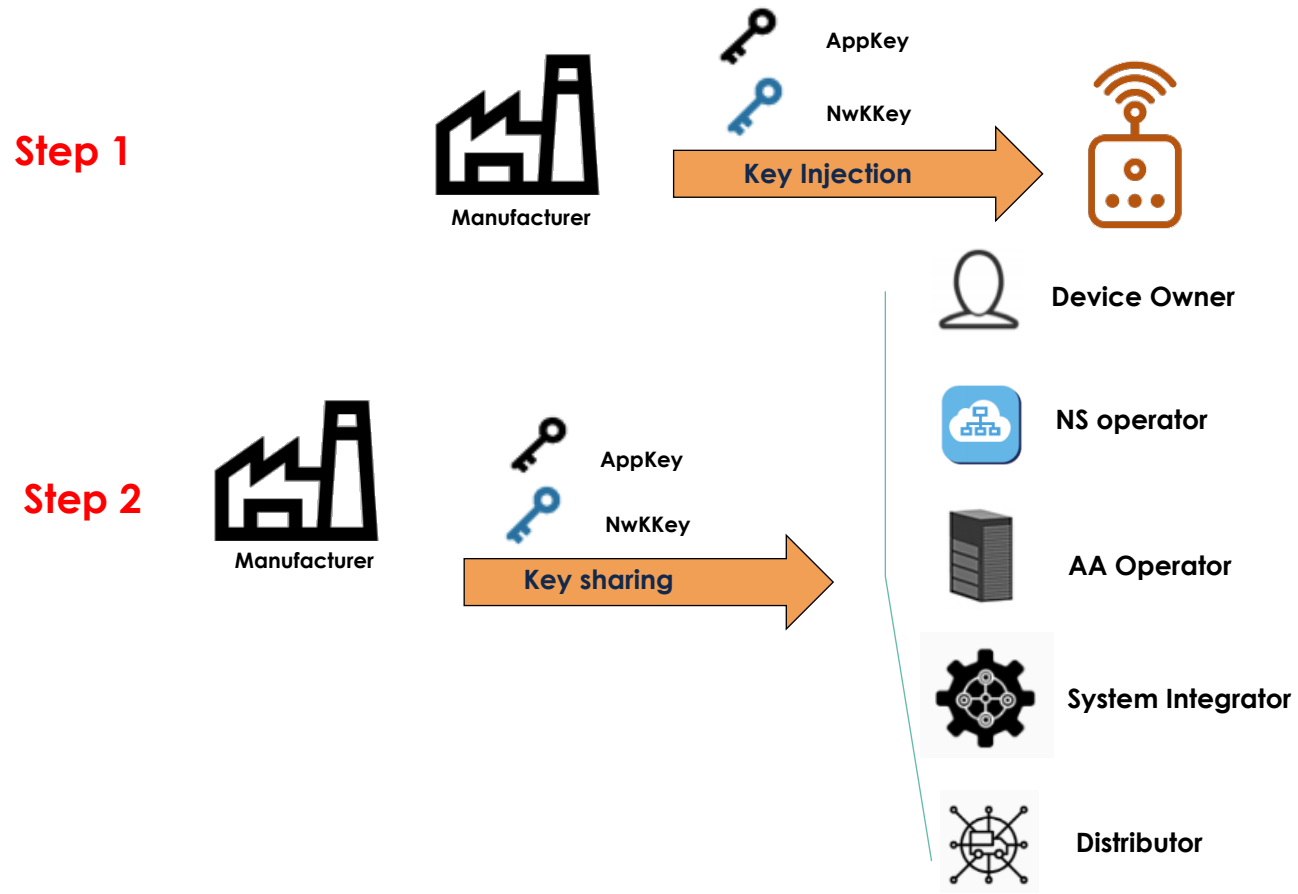
- NIST SP 800-207 – Zero Trust Architecture

ID management system: This is responsible for creating, storing, and managing enterprise user accounts and identity records (e.g., lightweight directory access protocol (LDAP) server). This system contains the necessary subject information (e.g., name, email address, certificates) and other enterprise characteristics such as role, access attributes, and assigned assets. This system often utilizes other systems (such as a PKI) for artifacts associated with user accounts. This system may be part of a larger federated community and may include nonenterprise employees or links to nonenterprise assets for collaboration.

Key Sharing Journey-map in IoT

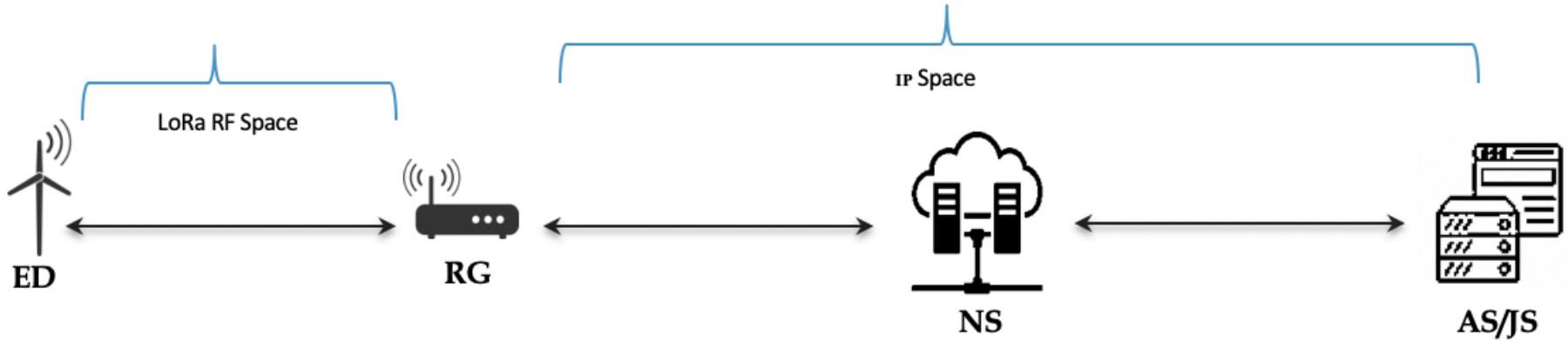


Challenge (e.g. LoRaWAN use-case)



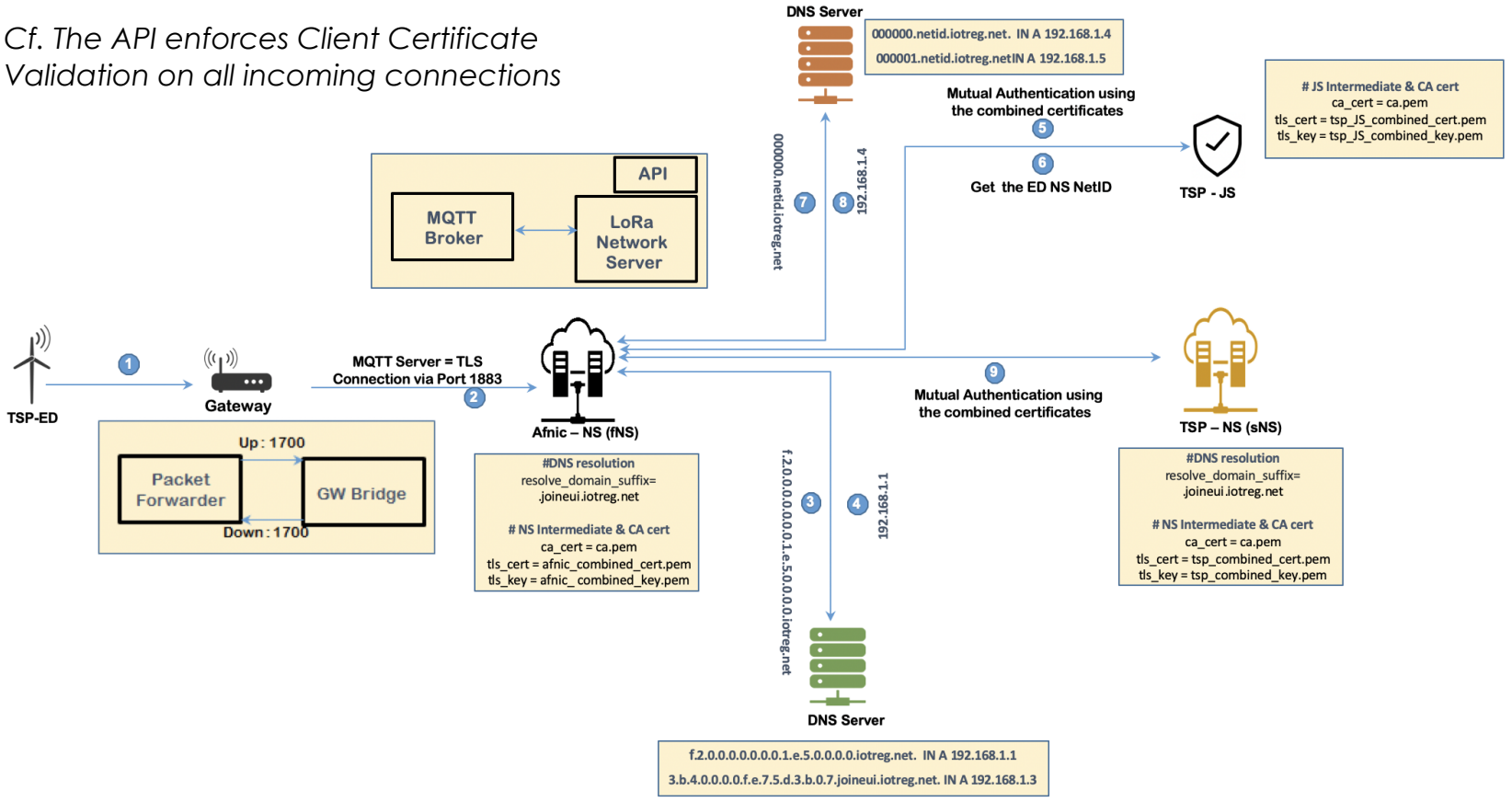
afnic | Labs

LoRaWAN



Mutual authentication using self-signed certificates

Cf. The API enforces Client Certificate Validation on all incoming connections



Issues with 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

DANE Primer

port, protocol, domain name

data (hex encoded) associated with the certificate or public key

```
_25._tcp.mail.example.com. IN TLSA (
                    3 1 1  d2abde240d7cd3ee6b4b28c54df034b9
                           7983a1d16e8a410e4561cb106618e971 )
```

Parameters: Usage, Selector, Matching-Type

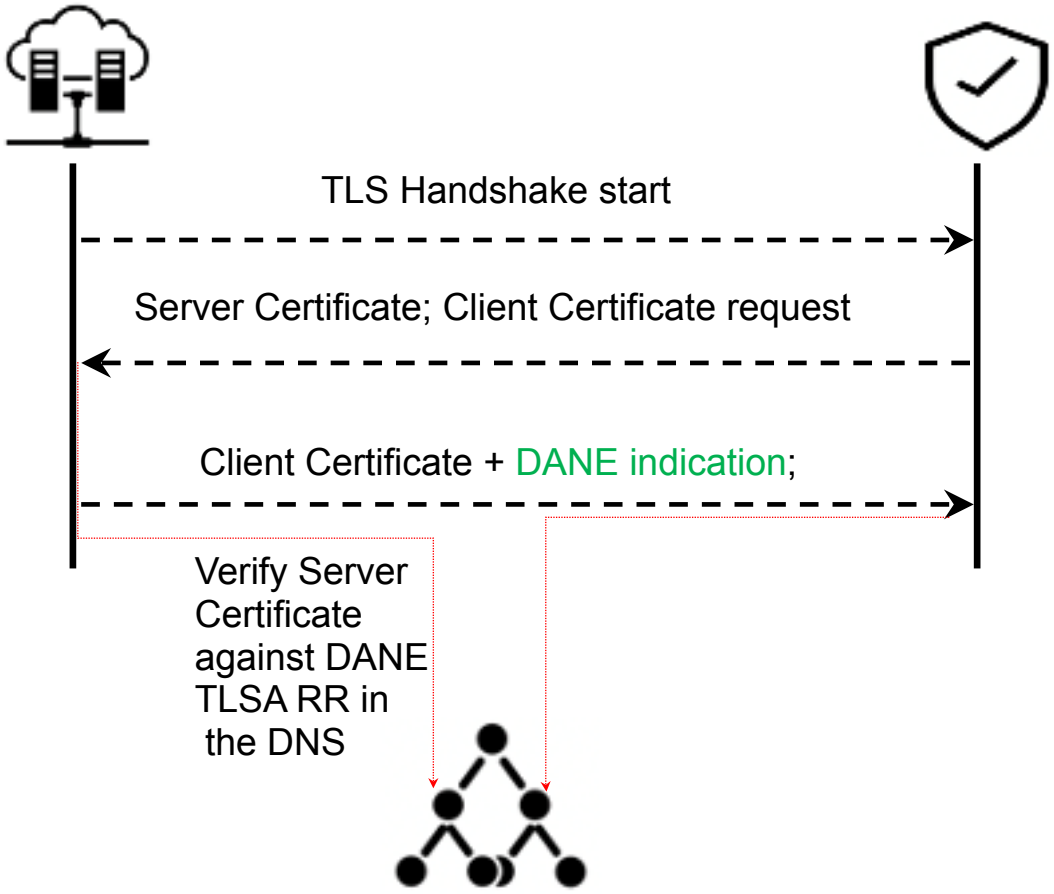
Usage 0: PKIX-CA: CA Constraint
Usage 1: PKIX-EE: Service Cert Constraint
Usage 2: DANE-TA: Trust Anchor Assertion
Usage 3: DANE-EE: Domain Issued Certificate

Selector 0: Full Certificate
Selector 1: Public Key (could be raw)

Matching-Type 0: Full Content
Matching-Type 1: SHA-256 Hash
Matching-Type 2: SHA-512 Hash

DANE record specifies the SHA256 hash of the subject public key of the certificate that should match the End-Entity certificate. Authenticated entirely in the DNS (no PKIX involved).

DANE Client authentication with TLS 1.3



Afnic's Vision for IoT using DNS

DONE

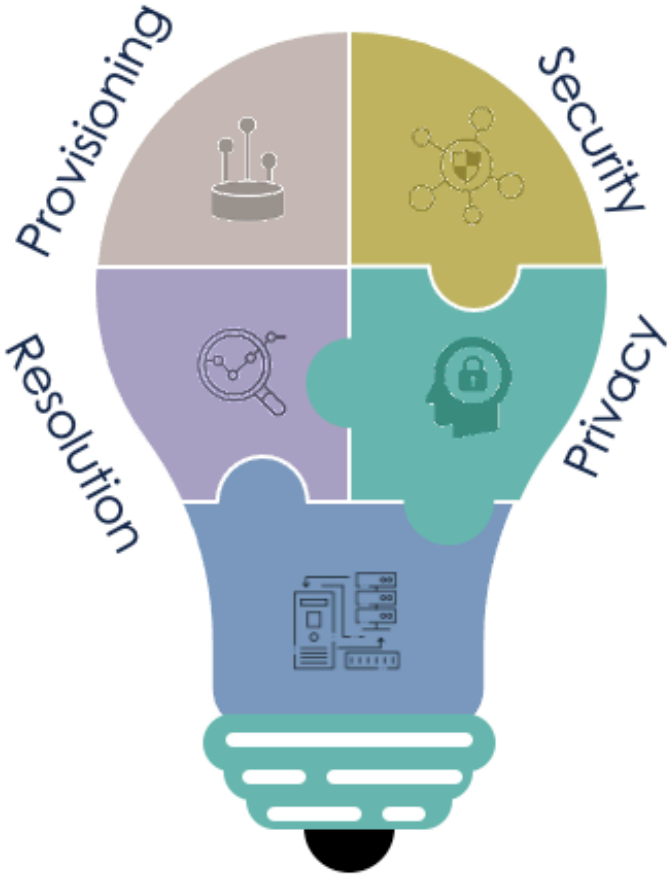
WINGS

Widening interoperability for networking Global supply Chains

DONE

LoRa Alliance

DNS Service



ONGOING

DINS*

DNS Naming and Services for Secure Seamless IoT

ONGOING

PIVOT*

Privacy-Integrated design and Validation in the constrained IoT