IETF 112 DANCE

EAP-TLS use case

Topics

Challenges with TLS client identity and EAP-TLS

DANE client identity and EAP-TLS

Q&A

Challenges with EAP-TLS supplicant authentication

Expensive

Current best practice dictates the use of a single private PKI

- This requires the organization to build/buy/maintain a private PKI
- PKI onboarding is a time-consuming activity
- This is a steep expense for small organizations

Interoperability barriers

A device needing to access multiple organizational networks needs multiple IDs

- Guest access for non-org (contract) workers is complicated to implement

Using DANE for EAP-TLS supplicant ID

One device identity, represented in DNS

- Configure supplicant access lists using DNS names
- Revocation at the speed of TTL

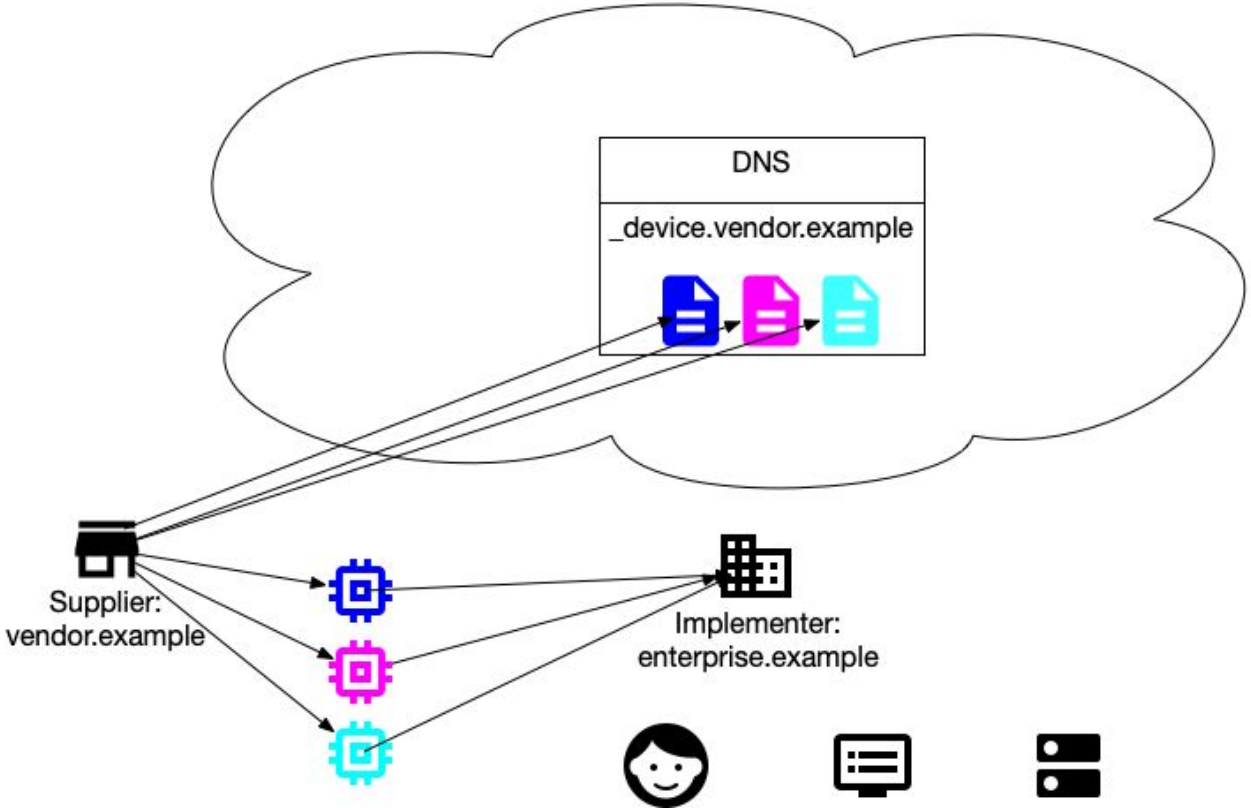
Useful identity may be provided by manufacturer or 3rd party

- No need for small organizations to operate private PKI
- No PKI onboarding time cost

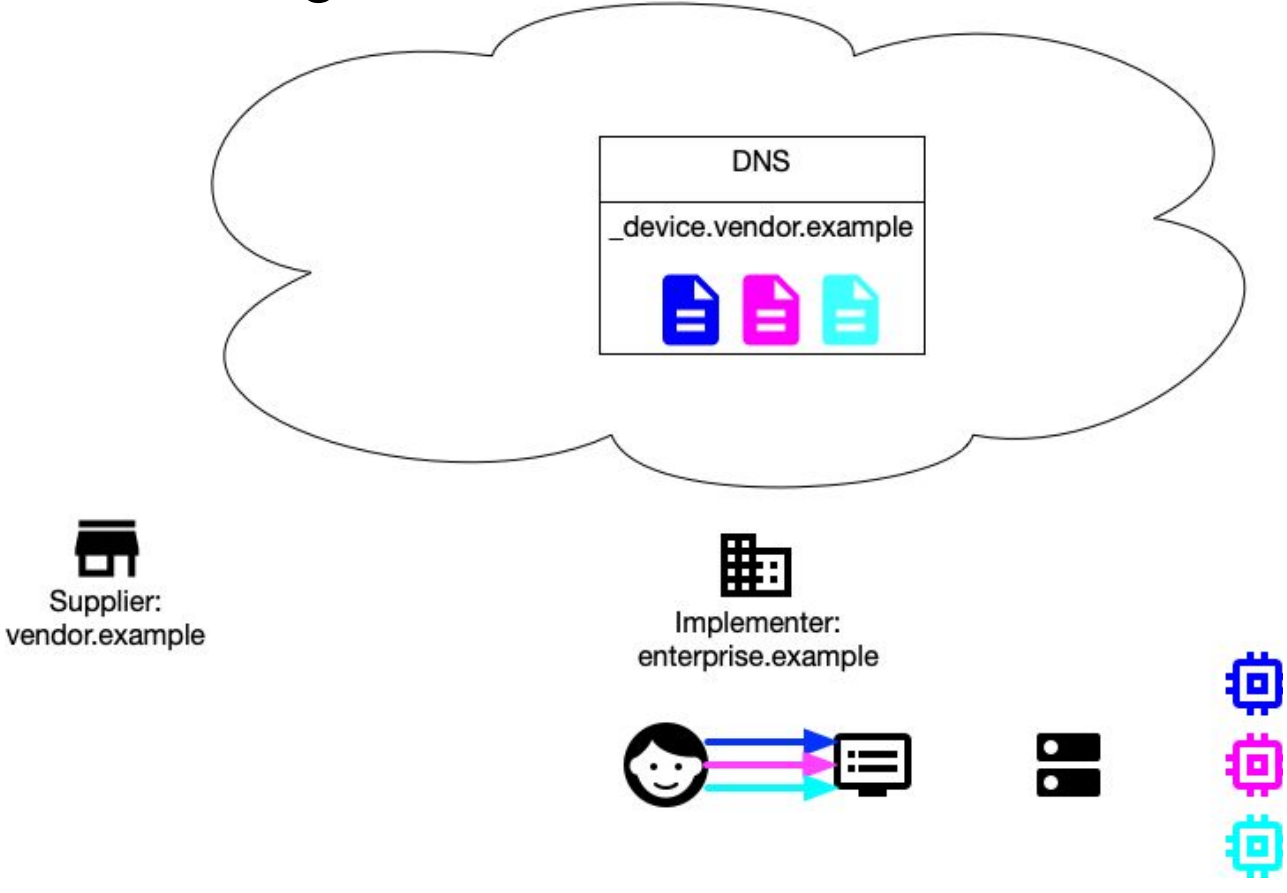
Use case: Network access for leased devices

1. Supplier (vendor.example) provisions devices with DANE IDs
2. Supplier ships devices to consumer/implementer
3. Implementer configures device network access
    a. Add device DANE ID to network ACL
    b. Configure device with network name (WiFi SSID)
    c. Configure EAP-TLS server auth (install CA cert)
4. Network bootstrapping complete

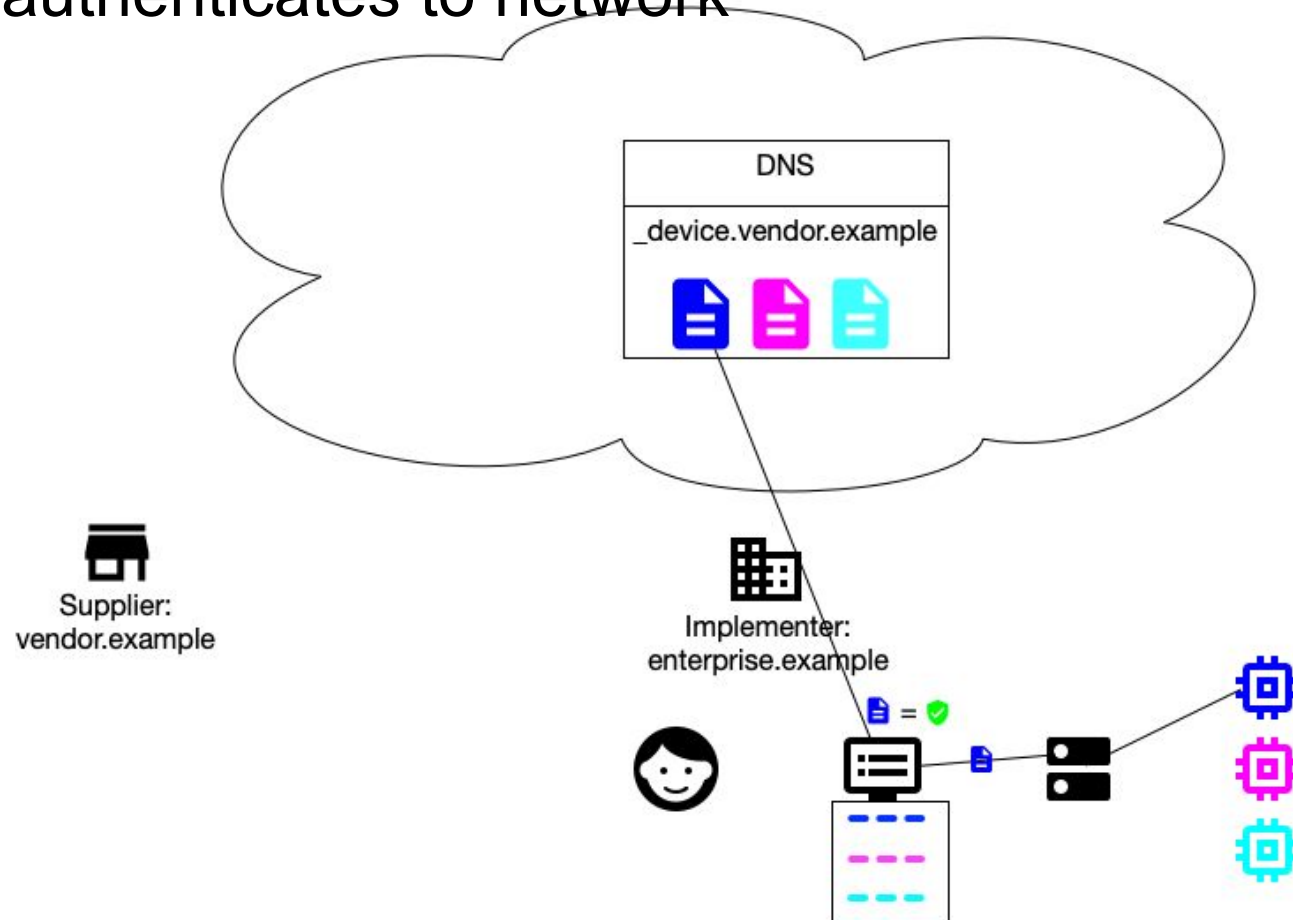
Supplier-issued identity bootstrapping



Implementer configures network access



Device authenticates to network



Q&A