RIOT SUMMIT 2026

Secure Provisioning and Enrollment of IoT Devices Using DNSSEC

Marc Sanchez

2026-09-03

EOTP : 22-CMAS-0021













1. Whoami 2
2. Context 4
3. DNS 7
4. DNSSEC 9
5. Protocol Workflow 11
6. Implementation 17
7. IoT-LAB 19
8. Conclusion 22

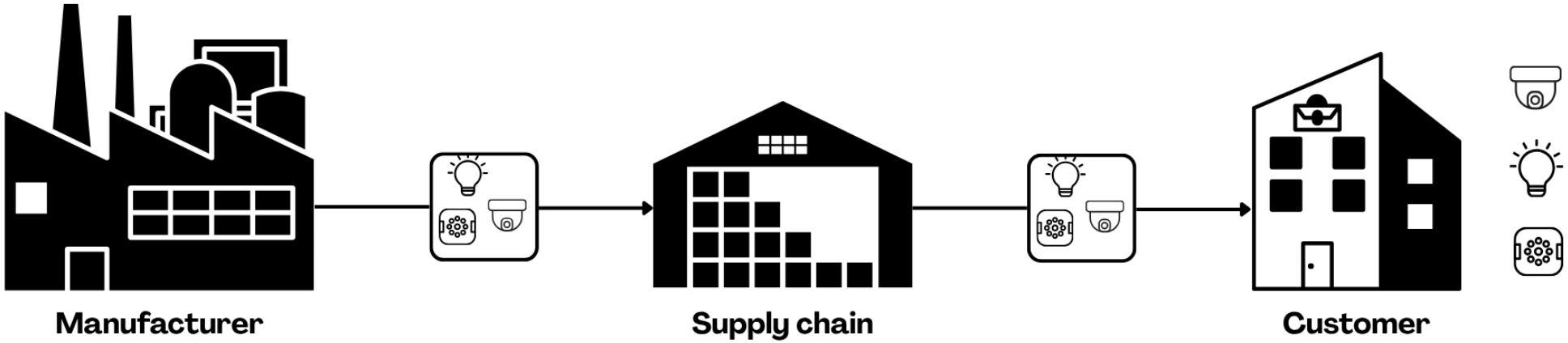
1. Whoami

Marc Sanchez

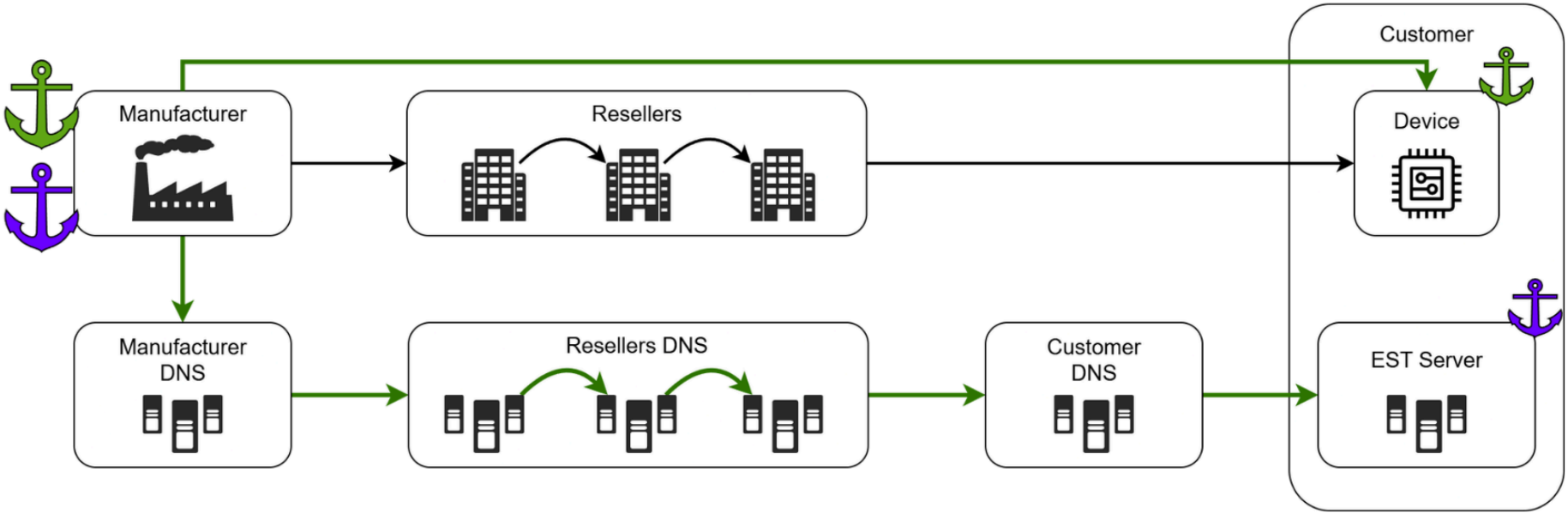
- **Cybersecurity Master's degree** (August 2025)
  - Ensimag - Université Grenoble-Alpes
- **1st year PhD Student** (October 2025)
  - Laboratoire d'Informatique de Grenoble (LiG)
  - Supervised by **Didier Donsez** & **Franck Rousseau**

2. Context

A DNSSEC-based protocol for zero-touch provisioning and enrollment of IoT devices

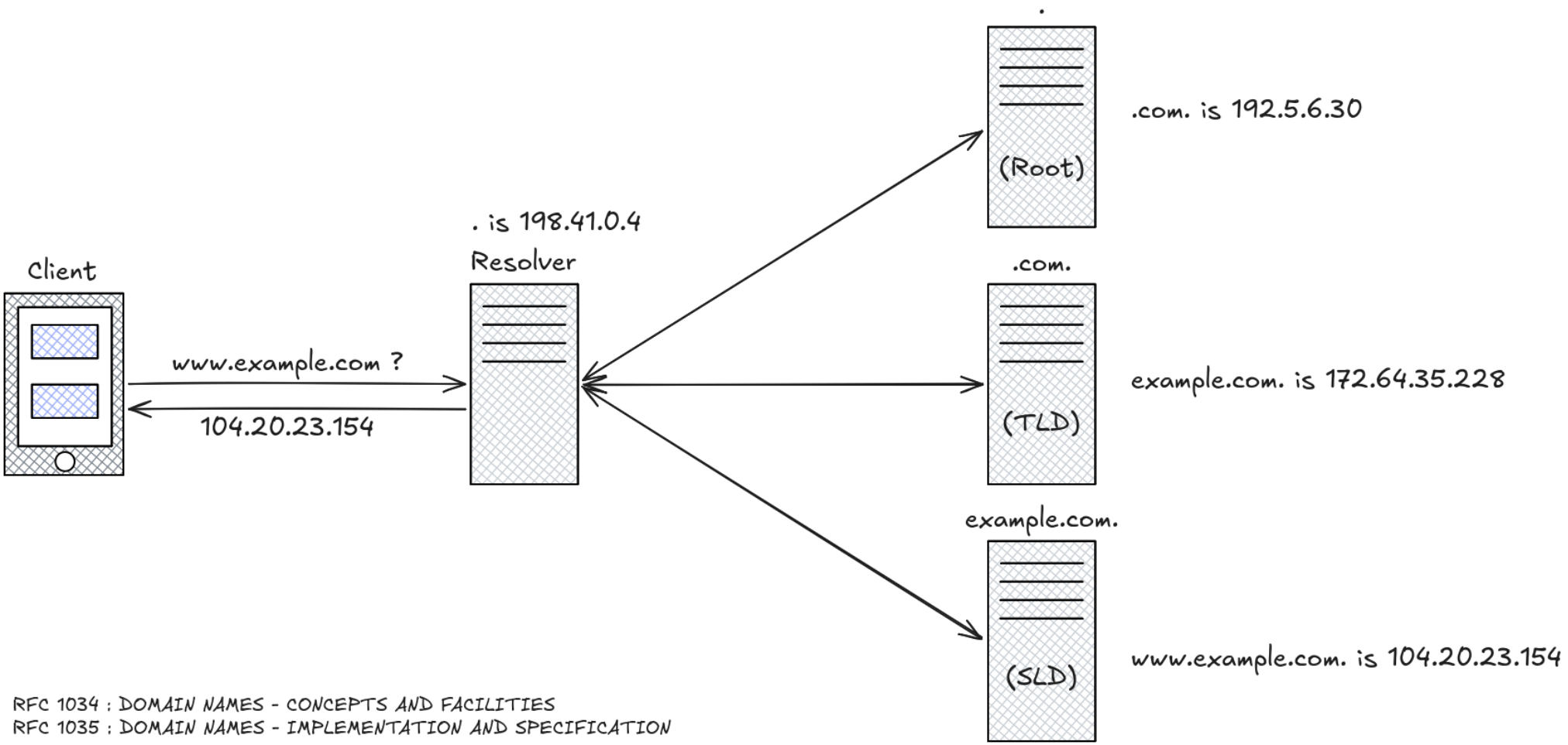


- **Manufacturer** : Makes the same devices for all clients
- **Supply chain** : Subject to compromise, replication
- **Customer** :
  - Restricted Environnement (VLANs, Firewalls, ...)
  - Wants to deploy tens of devices



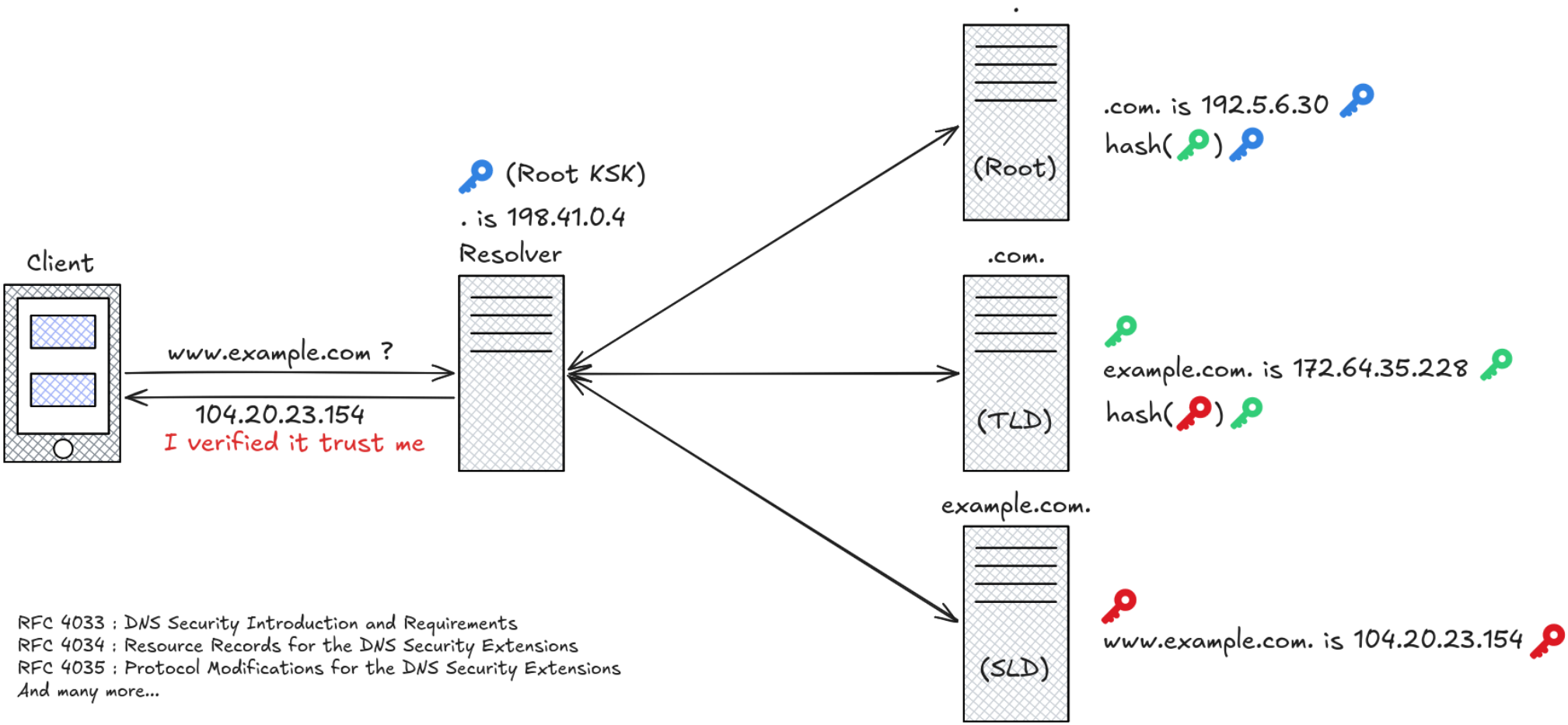
- **DevID** contains :
  - Manufacturer's certificate
  - Device KeyPair
  - Device certificate **(signed by the manufacturer)**
- **DNS** redirects the domain name of the device from the previous owner to the new owner's domain.

3. DNS



RFC 1034 : DOMAIN NAMES - CONCEPTS AND FACILITIES
RFC 1035 : DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

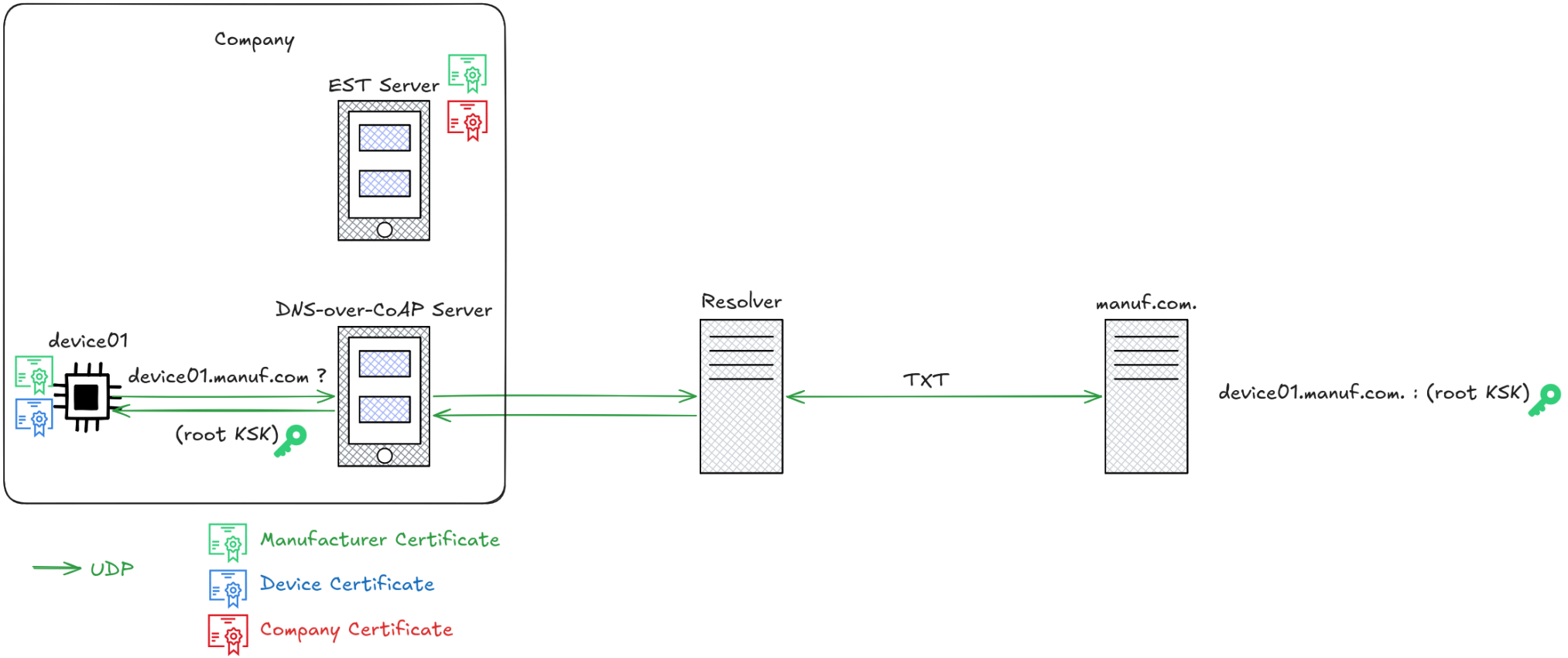
4. DNSSEC



RFC 4033 : DNS Security Introduction and Requirements
RFC 4034 : Resource Records for the DNS Security Extensions
RFC 4035 : Protocol Modifications for the DNS Security Extensions
And many more...

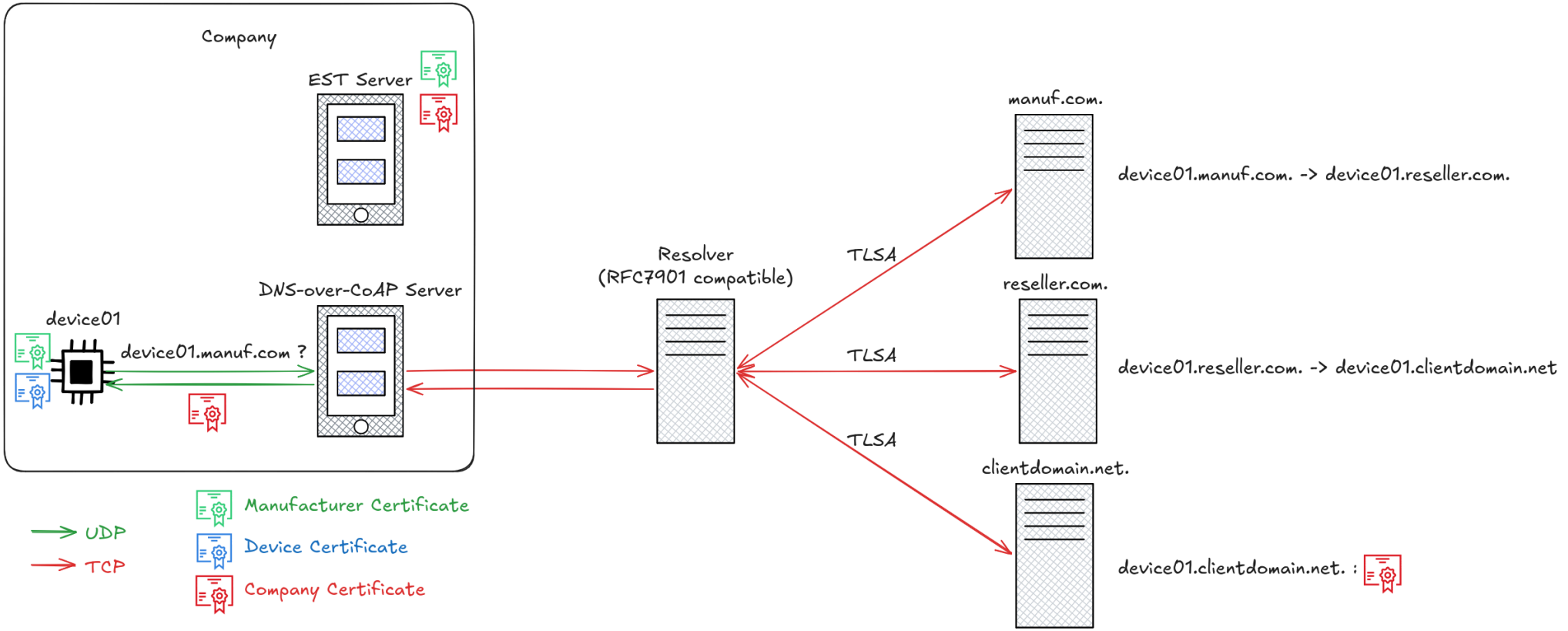
5. Protocol Workflow

Step 1 : Root KSK retrieving



RFC 9953 : DNS over CoAP (DoC)

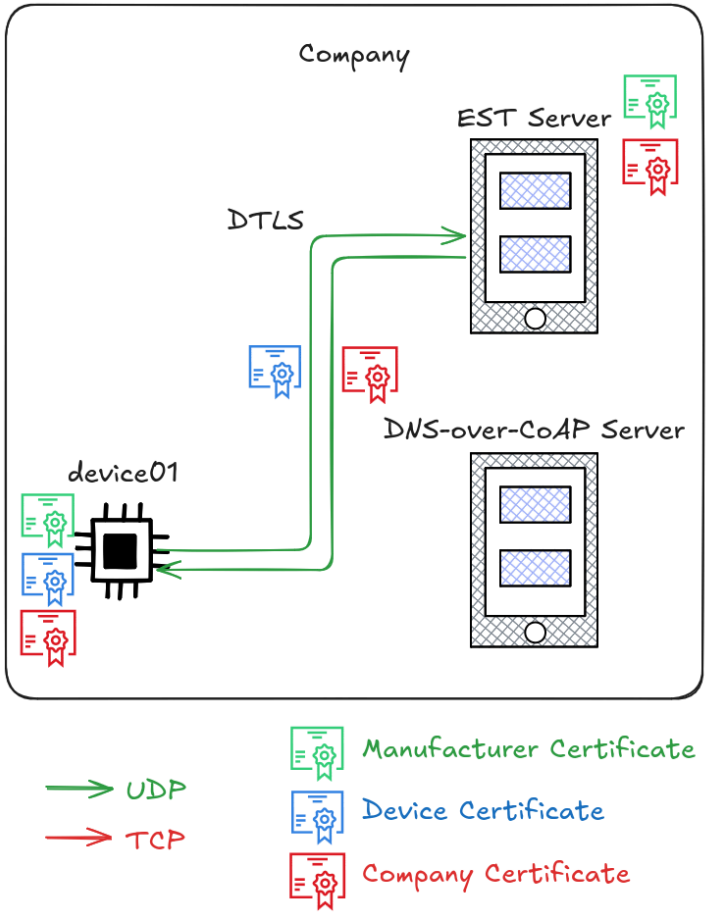
Step 2 : Company Certificate retrieving



RFC 9953 : DNS over CoAP (DoC)

RFC 7901 : CHAIN Query Requests in DNS
RFC 6698 : The DNS-Based Authentication of Named Entities (DANE) TLS Protocol: TLSA

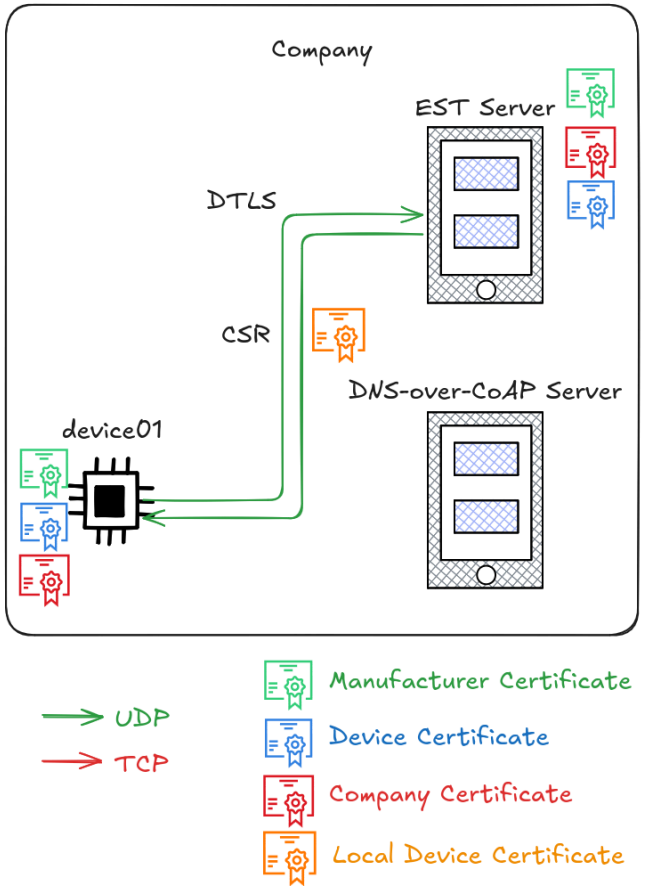
Step 3 : Mutual authentication via DTLS



RFC 9953 : DNS over CoAP (DoC)
RFC 7901 : CHAIN Query Requests in DNS
RFC 6698 : The DNS-Based Authentication of Named Entities (DANE) TLS Protocol: TLSA

RFC 7030 : Enrollment over Secure Transport
RFC 9148 : EST-coaps: EST with the Secure Constrained Application Protocol

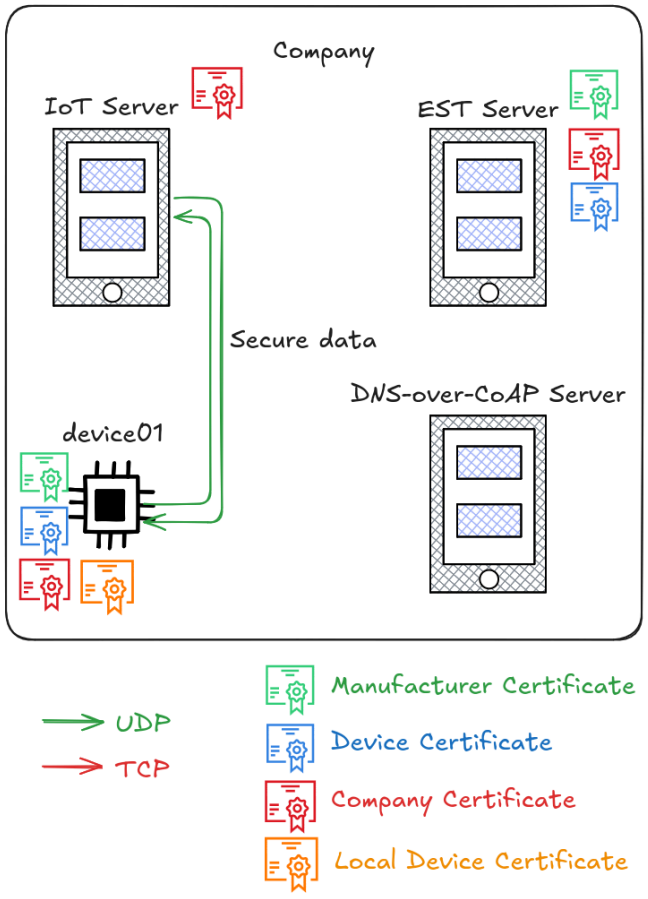
Step 4 : Device gets a Local Device IDentity



RFC 9953 : DNS over CoAP (DoC)
RFC 7901 : CHAIN Query Requests in DNS
RFC 6698 : The DNS-Based Authentication of Named Entities (DANE) TLS Protocol: TLSA
RFC 7030 : Enrollment over Secure Transport
RFC 9148 : EST-coaps: EST with the Secure Constrained Application Protocol

RFC 2986: PKCS #10: Certification Request Syntax Specification Version 1.7

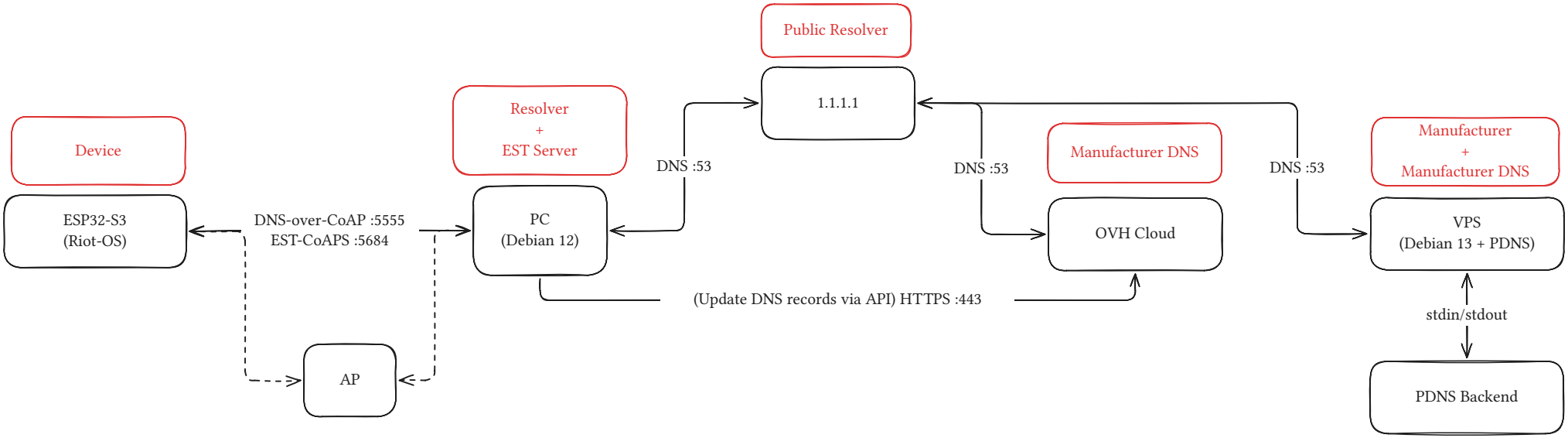
Step 5 : Device can operate securely



RFC 9953 : DNS over CoAP (DoC)
RFC 7901 : CHAIN Query Requests in DNS
RFC 6698 : The DNS-Based Authentication of Named Entities (DANE) TLS Protocol: TLSA
RFC 7030 : Enrollment over Secure Transport
RFC 9148 : EST-coaps: EST with the Secure Constrained Application Protocol
RFC 2986: PKCS #10: Certification Request Syntax Specification Version 1.7

6. Implementation

First Proof Of Concept to make tests, **hardly reproducible**
Tested on **ESP32-S3** running **Riot-OS**



7. IoT-LAB



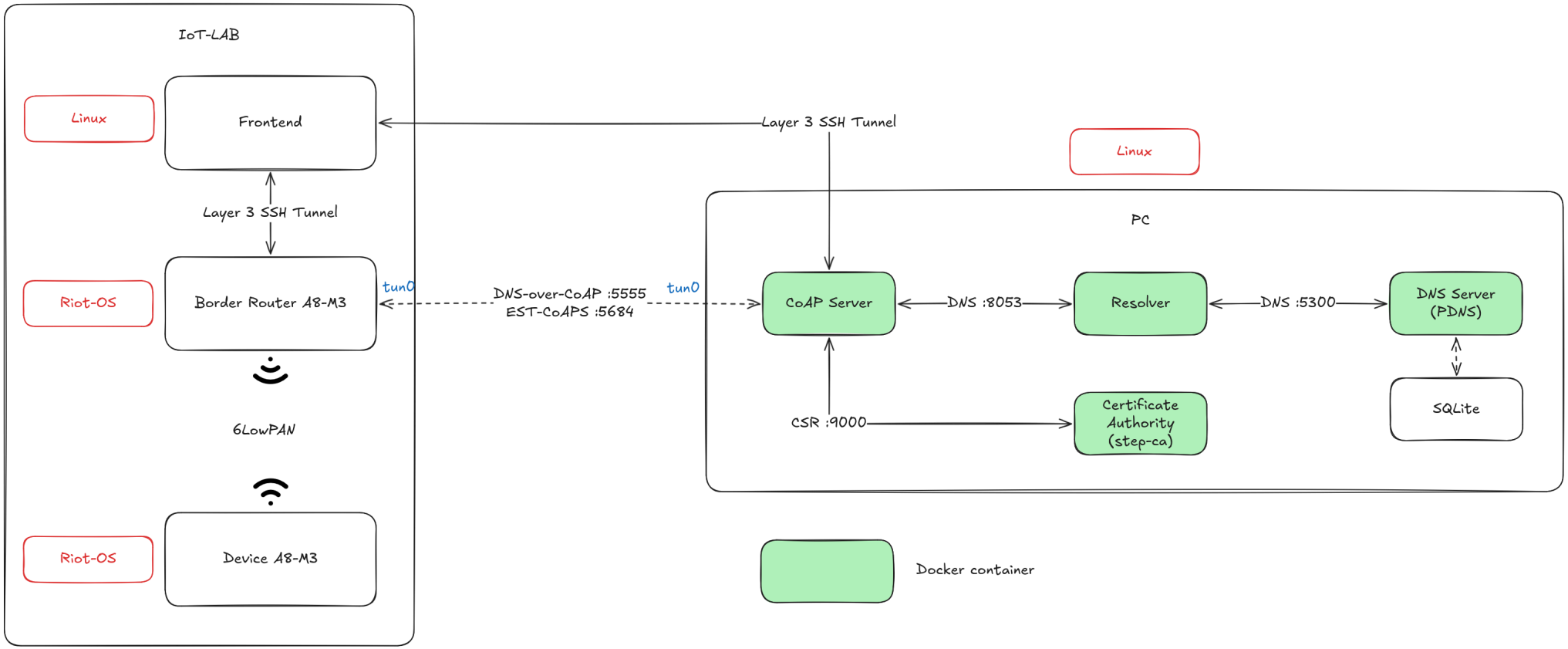
IoT-LAB : An infrastructure for experiment studies.

IoT-LAB provides testbeds in open access, suitable for testing networking with small wireless devices.

- **19** types of boards (supporting Riot-OS)
- Located in **Grenoble**, **Lille**, **Paris**, **Saclay**, **Strasbourg**, **Toulouse**

IoT-LAB and **Containers** allow **easy deployment and reproductibility**

Used **A8-M3 nodes** running **Riot-OS**



8. Conclusion

- 🥳 Proof-Of-Concept works
- ✅ RIOT-OS
  - Easy portability across boards and network stacks
  - Compatible with IoT-LAB boards
- ✅ ESP32-S3 : Xtensa LX7 dual-core (240 MHz) - 8MB RAM
  - Base board for tests
- ✅ STM32F103 : ARM Cortex M3 (72 MHz) - 64 KB of RAM
  - Used in IoT-LAB experiments
  - Minor changes and optimization
- 🚧 Futur works
  - Use IoT-LAB for measurements (energy, time)
  - Tests on other devices (ESP, nRF, STM, ...)
  - Publish paper


Thank you!
Any questions?