

DRIP End-to-End Implementation

DNS / DNSSEC



AFNIC French Network Information Center



Instituto Tecnológico de Aeronáutica

The Team



**Nathan
Le Sausse**

AFNIC



**Sandoche
Balakrichenan**

AFNIC



**Lourenço Alves
Pereira Jr**

ITA



**Flavio
Souza**

ITA



João Paulo

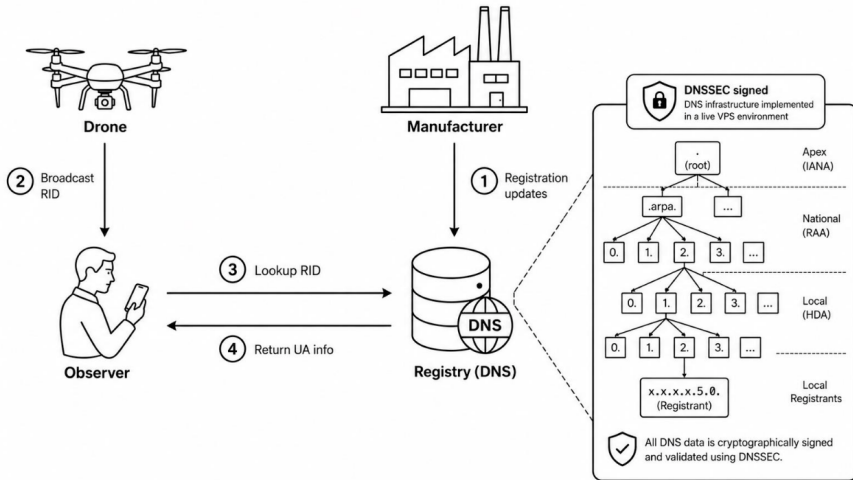
ITA



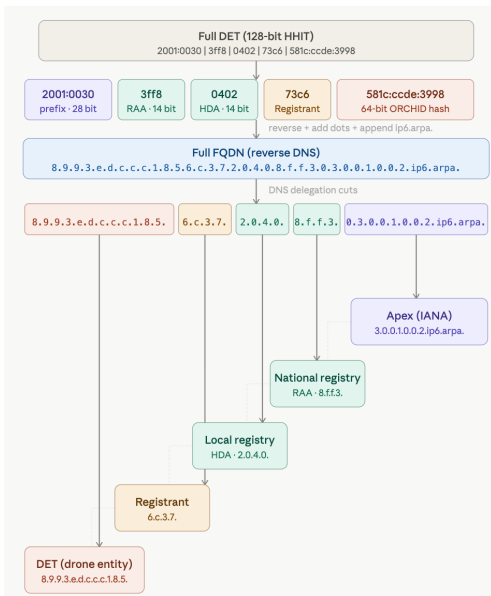
**André Elias
Melo**

ITA

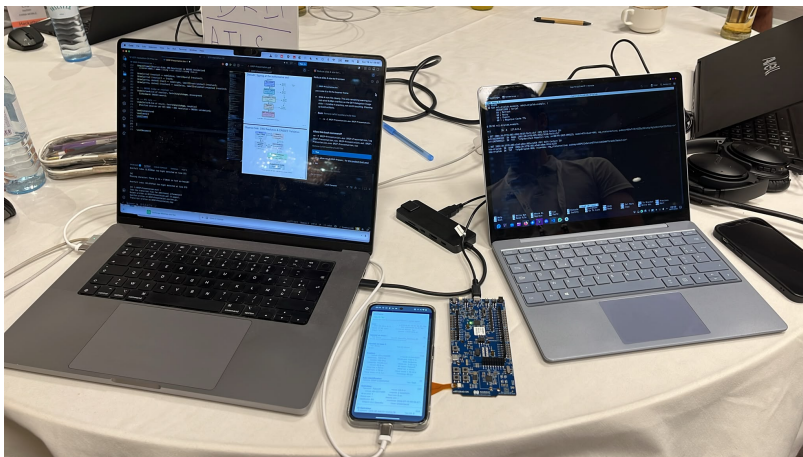
DRIP Functional Architecture with DNS resolution



DET Delegation as specified in RFC 9886



Experimental Setup



Contributions

Observer Code - Mobile App

RFC 9374 conformance replaced incorrect cSHAKE customisation string "HHIT" with the 16-byte Context ID, fixing DET derivation across all three components.

DNSSEC chain repaired inserted DS records at every delegation point (ORCHID → RAA → HDA), enabling full chain-of-trust validation for the first time.

Real DNSSEC validation replaced stub resolver with `ValidatingResolver` (dnsjava 3.6.0) anchored on lab trust anchors; forged responses now return `SERVFAIL`.

Aggregated trust verdict new *Trusted / Partial / Unverified* card combining both verification paths (broadcast Link + DNS registry).

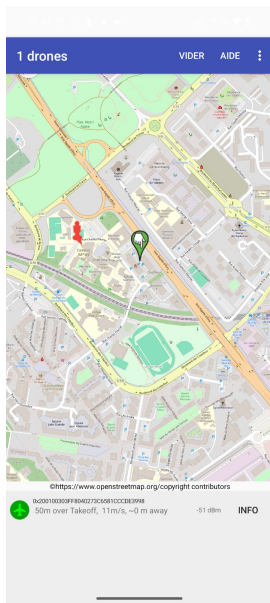
Drone Transmitter (nRF52840)

HDA endorsement replaced self-signed Link with a true hierarchical endorsement (RFC 9575): the HDA signs the drone's DET + public key, anchoring identity in the trust hierarchy.

AUTH reassembly bounded attacker-controlled indices and lengths in `combineAuthentication` are now clamped; malformed BLE frames can no longer crash the observer.

HHIT Suite ID corrected (RFC 9374) DET was advertising Suite 2 (ECDSA/SHA-384) instead of Suite 5 (EdDSA/cSHAKE128); mismatch detected by audit, fixed in the DNS provisioning script and new DET regenerated.

Drone as viewed from the observer App



DRIP Observer App - without DNSSEC Validation

09:41

Confiance

—

Lien

v.22026-07-19 09:41:02.802

RSSI -41 dBm, BT4

MAC CE:FA:0D:4A:D7:65

Débuté 00:28 ago

Dernière fois 00:00 ago

Mag & 102 ms

Distance ~1031416 m

Identité de base 1

24

Type None

Type d'ID Specific_Session_ID

ID UAS 0x200100303FFB04027306581CCCCDE3998

Identité de base 2

0

Type None

Type d'ID None

ID UAS

Position

46

Latitude 48.6248000

Longitude 2.4449000

Altitude pres. 150.0 m

Altitude géod. 150.0 m

Direction 180 deg

Statut Airborne

Vitesse hori. 10.50 m/s

Vitesse vert. 1.00 m/s

Hauteur 50.0 m

Réf. hauteur Takeoff

Précis* hori. < 10 m

Précis* vert. < 10 m

Précis* baro. < 10 m

Précis* vitesse < 10 m/s

Précis* temps <= 0.1 s

Horodatage 00:30

Auto-identification

20

Opération DRIP CASSIOPEE

Type Text

Opérateur

48

Type post* TakeOff

Altitude 35.0 m

Latitude 48.6251000

Longitude 2.4422000

Nb de zones 1

Rayon zone 0 m

Plafond zone —

Plancher zone —

Classification EU

Horodatage 2026-07-19 09:39:31.1

Catégorie EU_Specific

Classe Undeclared

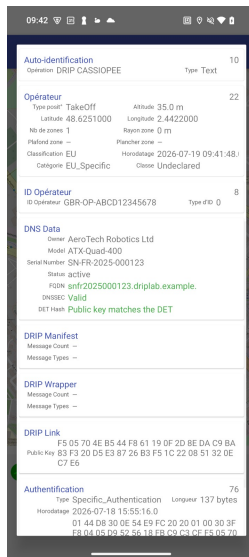
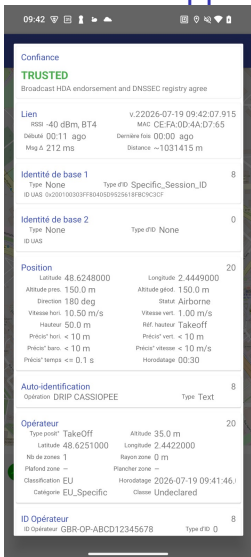
ID Opérateur

24

ID Opérateur GBR-OP-ABCD12345678

Type d'ID 0

DRIP Observer App With DNSSEC Validation



Trust verdict & drone telemetry

Left: TRUSTED HDA endorsement

DNS data, DNSSEC validation & DRIP Link

Right: DNSSEC Valid + Public key matches the DET