

afnic
Internet
made in France

DNS OARC 47 - 10/11/2026

Operationalizing the DNS for Drone Identity with DRIP

– *Sandoche BALAKRICHENAN*

The DNS Camel



Source: https://www.ietf.org/blog/herding-dns-camel/

Aircraft Identification & Verification

Identity Assignment

ICAO (international)
24-bit address blocks to States
France: `380000–3BFFFF`

address block

DGAC (national, France)
Keeps the aircraft register; assigns addresses from the French block

registration

Aircraft identity
Registration **F-GABC** (legal)
ICAO address **39ABCD** (technical)
Flight ID **AFR123** (operator)

Identity verification

1. **Flight plan** – airline files **AFR123**, Paris–Marseille
2. **Surveillance** – Mode S / ADS-B broadcasts **39ABCD** and **AFR123**
3. **Correlation** – track matched to the flight plan: callsign, position, transponder code
4. **Display** – the aircraft appears as **AFR123** on the controller's screen

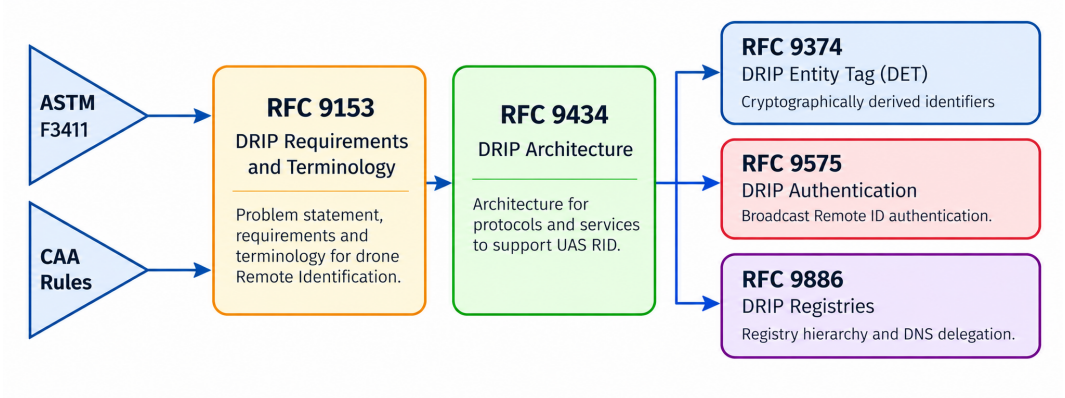
Identity verification relies on **correlation and operational procedures – not on cryptographic authentication**.

Motivation for Drone Identification

- ICAO 24-bit aircraft addresses provide only 2^{24} ($\sim$16.7 million) possible identifiers, making them unsuitable for large-scale UAS identification.
- Observers may not have access to traditional aviation infrastructure.
- Identification must work across national and administrative boundaries.
- Broadcasting an identifier does not guarantee its authenticity.

References: ICAO, UAS Traffic Management (UTM) Framework; RFC 9153, *DRIP Requirements and Terminology*; IETF DRIP Working Group Charter (2020).

DRIP Standardization Framework



ICAO defines governance | IETF defines the technical protocols

DRIP Entity Tag: Structure and Construction

Structure: 128 bits

- **Prefix:** 28 bits (`2001:30::/28`)
- **HID:** 28 bits
  RAA (14) + HDA (14)
- **Suite ID:** 8 bits
- **Hash:** 64 bits

Construction

1. Select prefix, hierarchy and suite.
   RAA 16376, HDA 10, Suite 5 ⇒ `2001:003f:fe00:0a05`
2. Encode the public key as `HOST_ID`.
   Ed25519 key `c92e2f9d…e8e877fa` (32 bytes)
3. Compute the hash (cSHAKE128, Suite 5).
   cSHAKE128(upper 64 bits ‖ key) ⇒ `130824699a4bc6b2`
4. Combine the four fields.
   `2001:3f:fe00:a05:1308:2469:9a4b:c6b2`

`2001:003f:fe00:0a05:1308:2469:9a4b:c6b2`

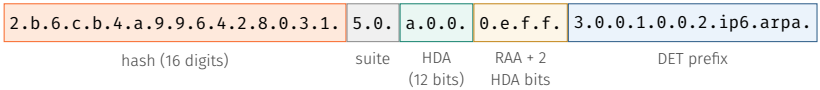


DET Delegation as specified in RFC 9886

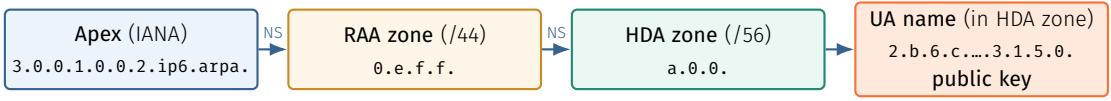
1. DET (128 bits) `2001:3f:fe00:a05:1308:2469:9a4b:c6b2`



2. Reverse the hex digits, append `ip6.arpa`



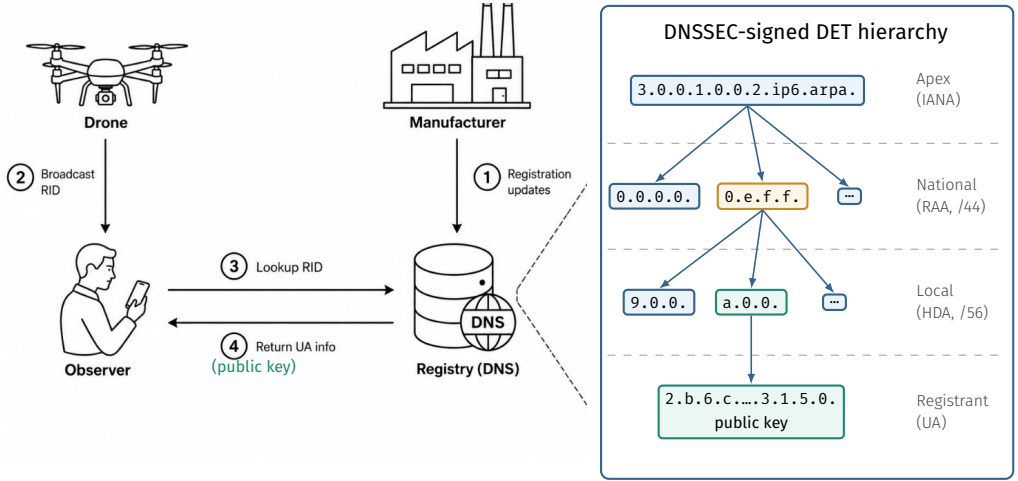
3. Zone cuts on hex-digit boundaries



The RAA "borrows" the top 2 bits of the HDA so that each zone cut falls on a hex-digit boundary.

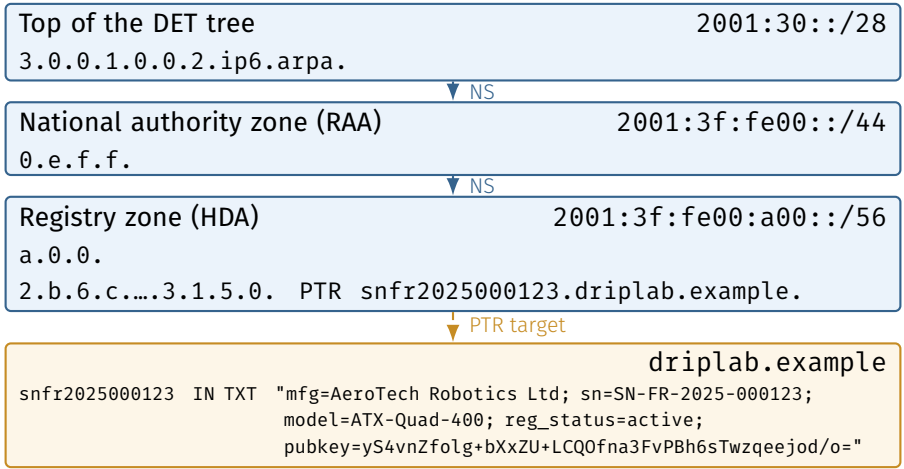
Source: RFC 9886, Section 3 and Appendix A (example DET: RAA 16376, HDA 10).

DRIP Functional Architecture with DNS resolution

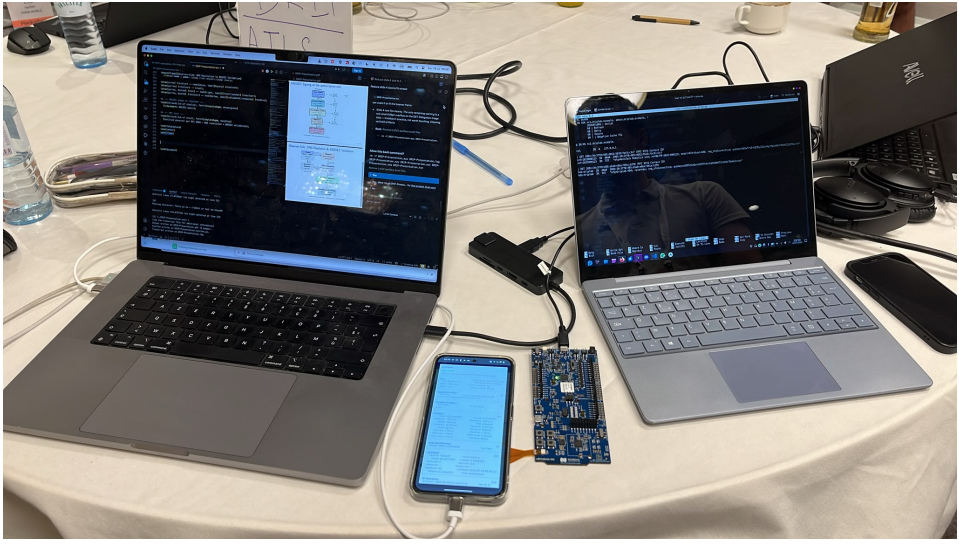


Source: DNS hierarchy and record types as specified in RFC 9886, Section 3 and Appendix A.

PoC - DNS Zone Configurations in a VPS



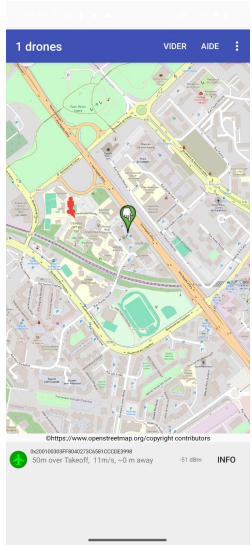
Experimental Setup durign the IETF 126 Hackathon



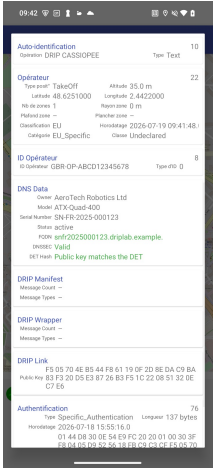
How the Observer Verifies a DET

1. The Nordic nRF52840 broadcasts its DET over Bluetooth
   `2001:30:3ff8:405:d952:5618:fbc9:c3cf`
2. Reverse the 32 hex digits and append **`ip6.arpa`**
   `f.c.3.c.9.c.b.f.8.1.6.5.2.5.9.d.5.0.4.0.8.f.f.3.0.3.0.0.1.0.0.2.ip6.arpa`
3. **Walk the hierarchy** – ORCHID → RAA → HDA zone
4. **PTR** from the HDA zone – gives the drone's domain name
   `<DET name>  PTR  snfr2025000123.driplab.example.`
5. **TXT** from the forward zone (**`driplab.example`**) – gives the drone's public key
   `snfr2025000123.driplab.example.  TXT  "…; pubkey=9QVwTrVE+GEZ…IOx+Y="`
6. **Hash check** – cSHAKE128(first 64 bits of DET ‖ public key) $\stackrel{?}{=}$ last 64 bits of DET
   `d9525618fbc9c3cf  =  d9525618fbc9c3cf`

Drone as viewed from the observer App



DRIP Observer App — With DNSSEC Validation



DNS data, DNSSEC validation & DRIP Link – DNSSEC valid + public key matches the DET

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

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.

An Informal Consortium Working on DRIP



Afnic – France



ITA (Instituto Tecnológico de Aeronáutica) – Brazil



Linköping University – Sweden



Bear Metal (bearmetal.eu) – Estonia