# Secure Remote Drone ID: Implementation and Experiment Updates

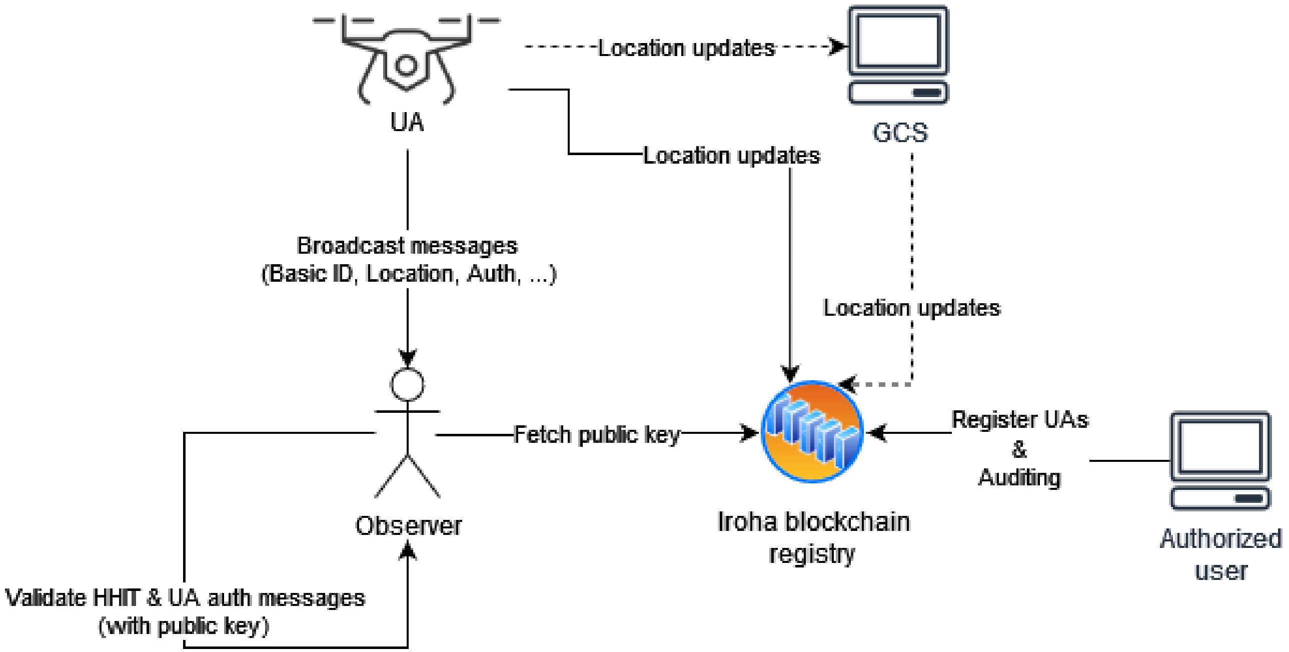
28th March 2023

IETF 116

Andrei Gurtov

LINKÖPING UNIVERSITY

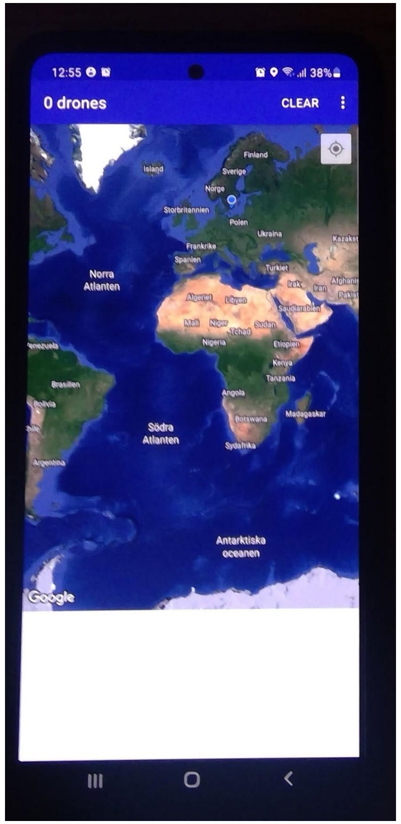
# DRIP Experimental Testbed

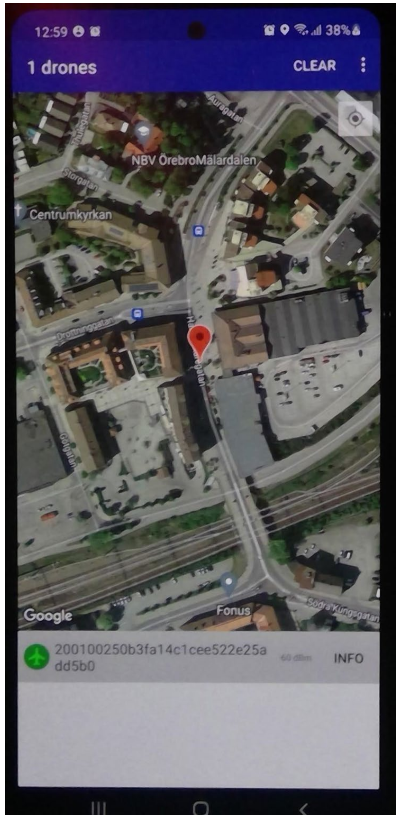


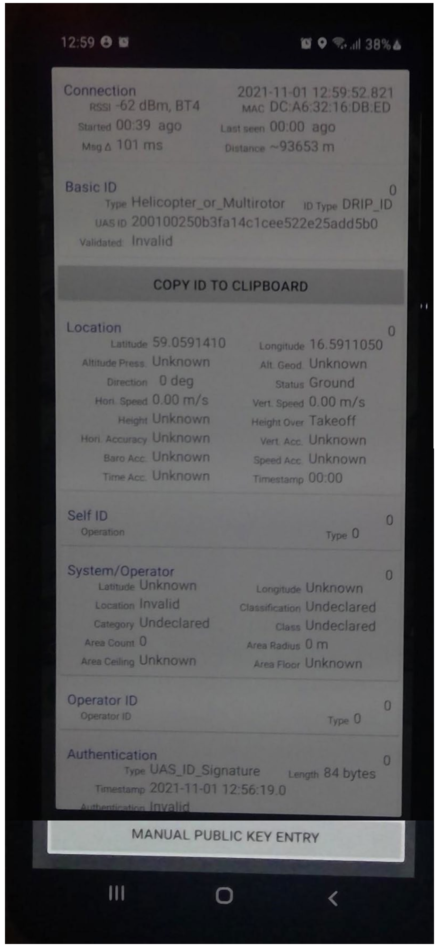
- Observers receive Direct RID messages, and perform lookups on registry
- UAs and GCSs send location updates to registry
- Admin registers new accounts (drone/operators)
- UAs do not participate in the blockchain

# Observer application

- OpendroneID as a base
- Google API with maps required separate developer key
  - Hard to provide .apk packages
- Now published as Google Play App with OpenstreetMaps
  - A few tens of downloads
  - [https://play.google.com/store/apps/details?id=org.securedroneid.android](https://play.google.com/store/apps/details?id=org.securedroneid.android)
  - iPhone next?







12:59 38%

Connection 2021-11-01 12:59:52.821
RSSI -62 dBm, BT4 MAC DC:A6:32:16:DB:ED
Started 00:39 ago Last seen 00:00 ago
Msg Δ 101 ms Distance ~93653 m

Basic ID 0
Type Helicopter_or_Multirotor ID Type DRIP_ID
UAS ID 200100250b3fa14c1cee522e25add5b0
Validated: Invalid

COPY ID TO CLIPBOARD

Location 0
Latitude 59.0591410 Longitude 16.5911050
Altitude Press. Unknown Alt. Geod. Unknown
Direction 0 deg Status Ground
Hori. Speed 0.00 m/s Vert. Speed 0.00 m/s
Height Unknown Height Over Takeoff
Hori. Accuracy Unknown Vert. Acc. Unknown
Baro Acc. Unknown Speed Acc. Unknown
Time Acc. Unknown Timestamp 00:00

Self ID 0
Operation Type 0

System/Operator 0
Latitude Unknown Longitude Unknown
Location Invalid Classification Undeclared
Category Undeclared Class Undeclared
Area Count 0 Area Radius 0 m
Area Ceiling Unknown Area Floor Unknown

Operator ID 0
Operator ID Type 0

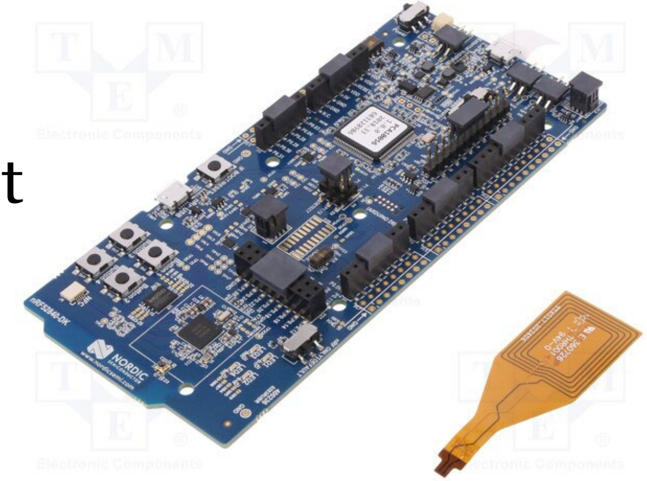
Authentication 0
Type UAS_ID_Signature Length 84 bytes
Timestamp 2021-11-01 12:56:19.0
Authentication Invalid

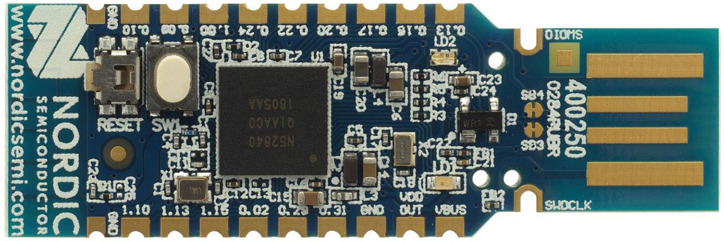
MANUAL PUBLIC KEY ENTRY

# DRIP and Bluetooth 5

USB BT500

nRF52840 Dongle and Development Kit



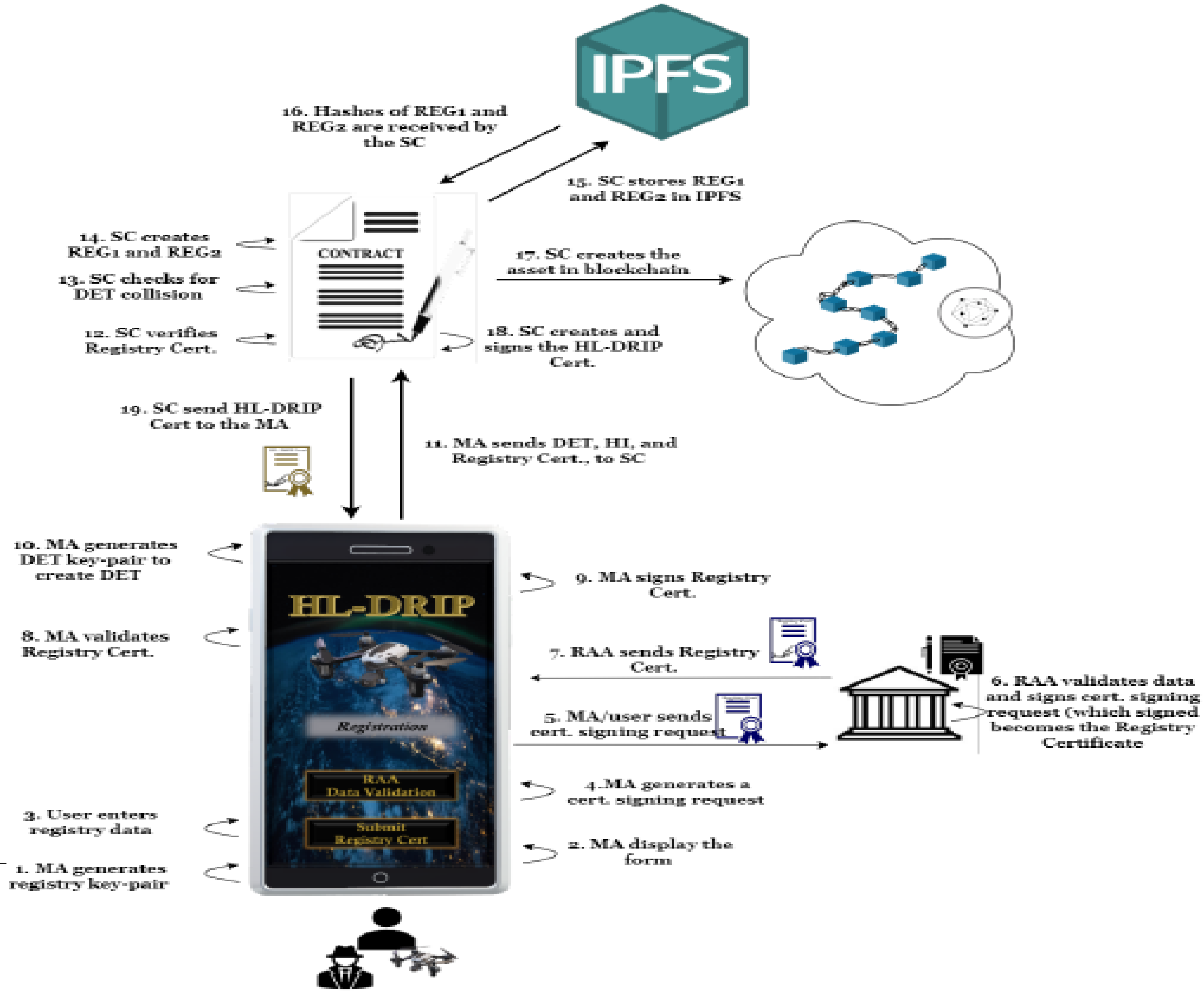


Problem with Linux Drivers, also new external Bt5 dongle, now operational on RP4 after install of Ubuntu drivers. Drippy script updated for BT5. BT5 works in NUC.

LINKÖPING
UNIVERSITY

# A Master Thesis on DRIP Registries

- HL-DRIP: A Blockchain-based Remote Drone ID Protocol registry management - Evaluation of a Hyperledger Fabric-based solution to manage DRIP registries
- Juan Basaez, ~100 pages
- Completed, will be published soon at [http://liu.diva-portal.org/](http://liu.diva-portal.org/)



1. MA generates registry key-pair

2. MA display the form

3. User enters registry data

4. MA generates a cert. signing request

5. MA/user sends cert. signing request

6. RAA validates data and signs cert. signing request (which signed becomes the Registry Certificate

7. RAA sends Registry Cert.

8. MA validates Registry Cert.

9. MA signs Registry Cert.

10. MA generates DET key-pair to create DET

11. MA sends DET, HI, and Registry Cert., to SC

12. SC verifies Registry Cert.

13. SC checks for DET collision

14. SC creates REG1 and REG2

15. SC stores REG1 and REG2 in IPFS

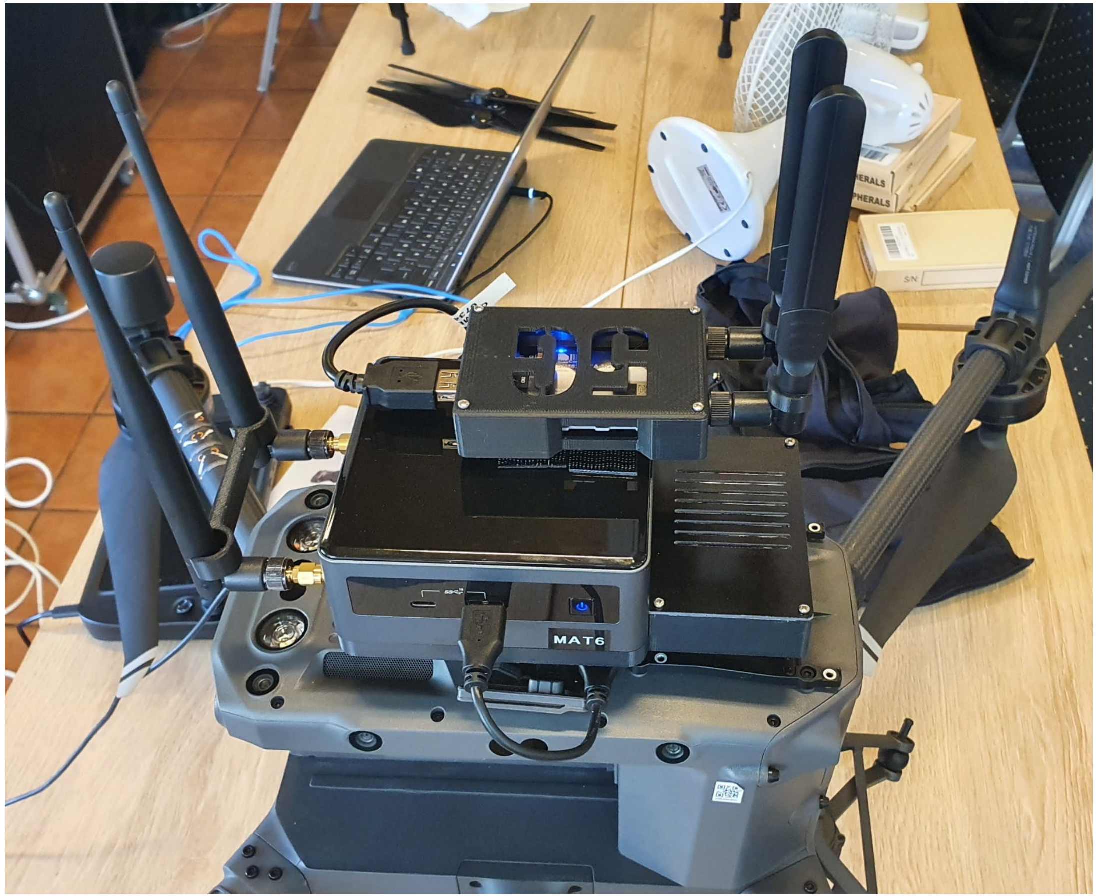
16. Hashes of REG1 and REG2 are received by the SC

17. SC creates the asset in blockchain

18. SC creates and signs the HL-DRIP Cert.

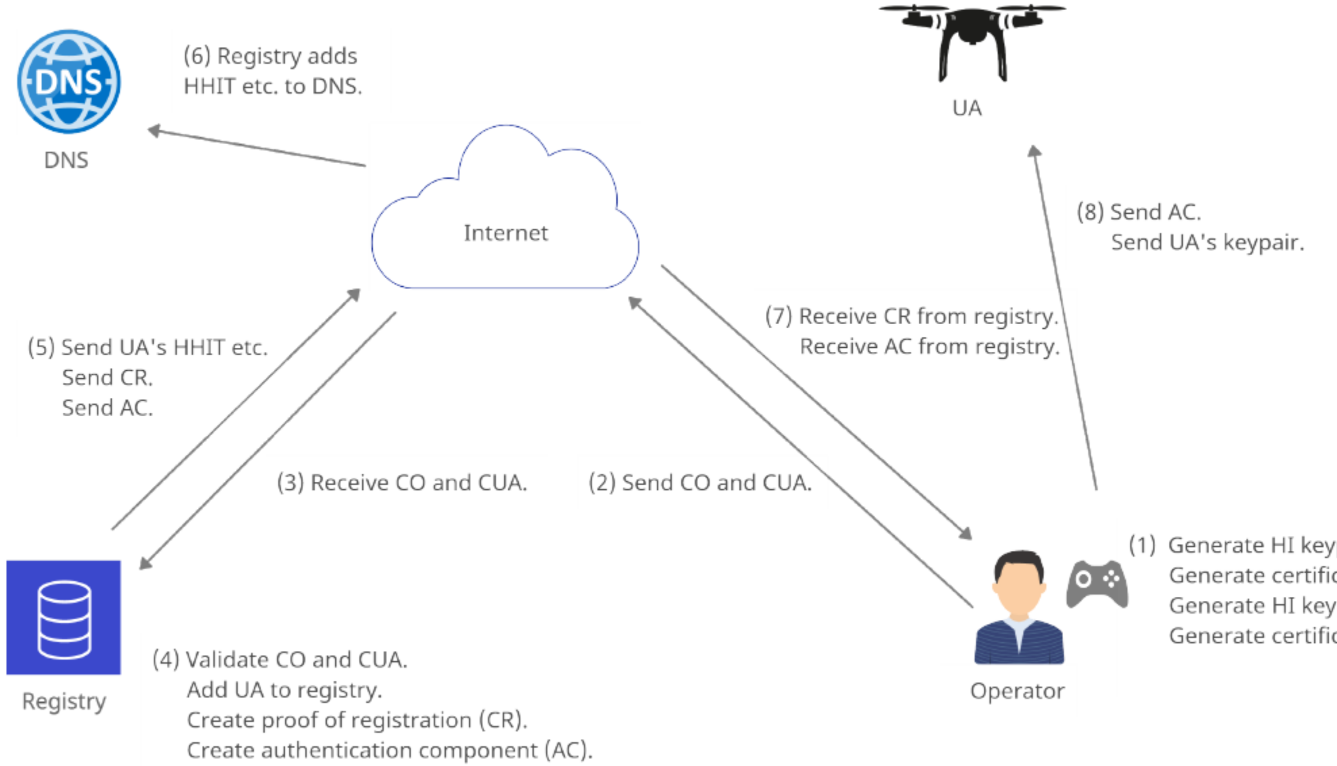
19. SC send HL-DRIP Cert to the MA

# New Unit of Computing on DJI Matrics 300



- New Unit of Computing (NUC) Intel running DRIP remote ID over BT4 via API to a drone hardware (power, GPS)
- x86 architecture, Ubuntu Linux
- 5G modem
- Built-in BT4, BT5, WiFi

# Formal Analysis of DRIP with Tamarin - Revising



(1) Generate HI keypair for himself.
Generate certificate for himself (CO).
Generate HI keypair for UA.
Generate certificate for UA (CUA).

(2) Send CO and CUA.

(3) Receive CO and CUA.

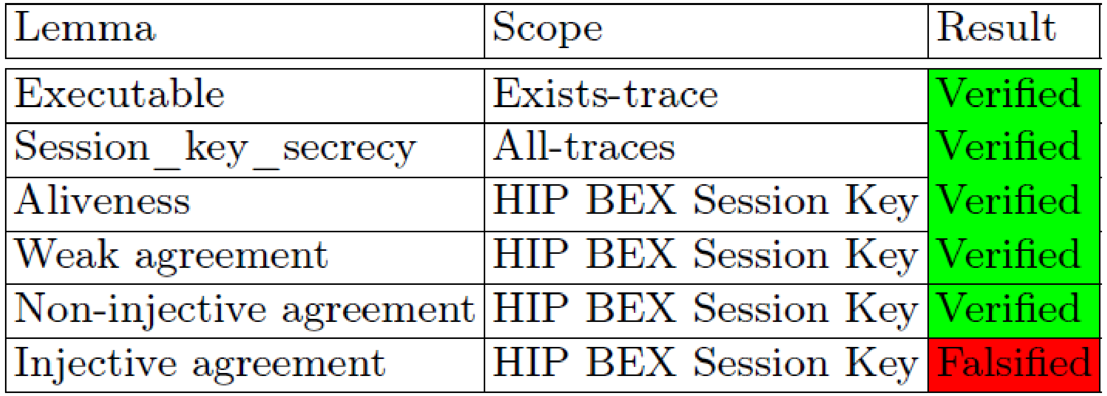
(4) Validate CO and CUA.
Add UA to registry.
Create proof of registration (CR).
Create authentication component (AC).

(5) Send UA's HHIT etc.
Send CR.
Send AC.

(6) Registry adds
HHIT etc. to DNS.

(7) Receive CR from registry.
Receive AC from registry.

(8) Send AC.
Send UA's keypair.



| Lemma | Scope | Result |
|---|---|---|
| Executable | Exists-trace | Verified |
| Session_key_secrecy | All-traces | Verified |
| Aliveness | HIP BEX Session Key | Verified |
| Weak agreement | HIP BEX Session Key | Verified |
| Non-injective agreement | HIP BEX Session Key | Verified |
| Injective agreement | HIP BEX Session Key | Falsified |

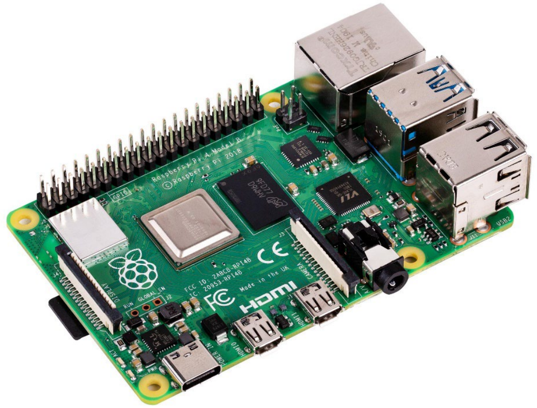
# Wallenberg AI, Autonomous Systems and Software Program – New session in May

- Public Safety Arena (sea rescue)
- Demo at WASP-PS Arena (Thanks Tommy and AIICS group)
- Pick up BT4 signal at 160m using Galaxy 10 phone.
- Focus more on BT5 tests
- Integration to common visualization platform

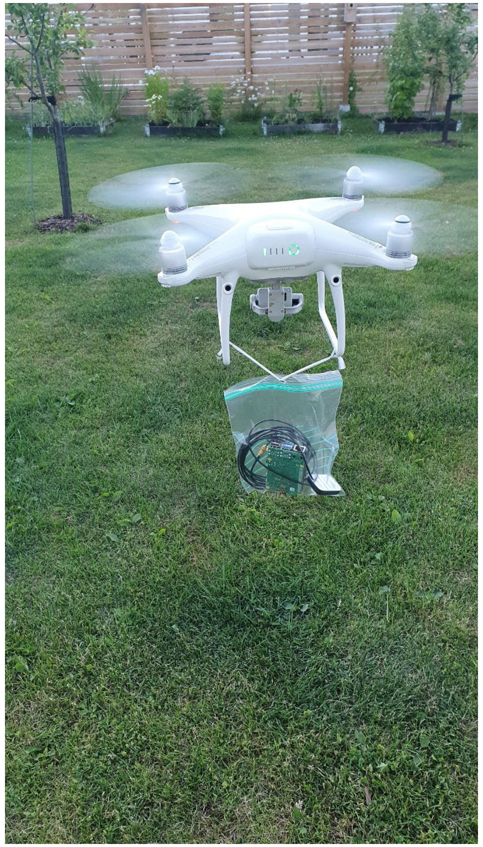
# Thanks! - Some backup slides (with links) attached

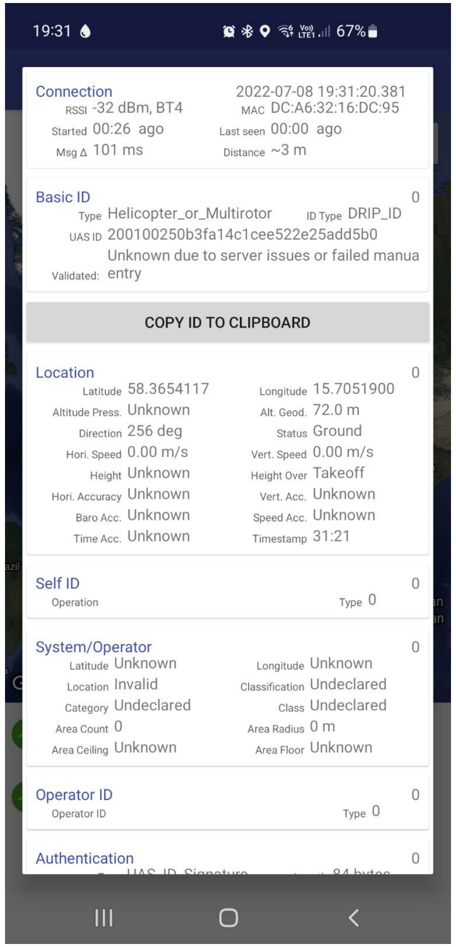
# Hardware Kit for RP4

- Integrate with GPS and Battery Hat for on-the-drone mounting
- Antenna magnets disturbs drone compass -> remove!



# DRIP on RP4 (ARM) and Phantom pro





19:31 67%

Connection
RSSI -32 dBm, BT4
Started 00:26 ago
Msg Δ 101 ms
2022-07-08 19:31:20.381
MAC DC:A6:32:16:DC:95
Last seen 00:00 ago
Distance ~3 m

Basic ID 0
Type Helicopter_or_Multirotor
ID Type DRIP_ID
UAS ID 200100250b3fa14c1cee522e25add5b0
Validated: Unknown due to server issues or failed manua entry

COPY ID TO CLIPBOARD

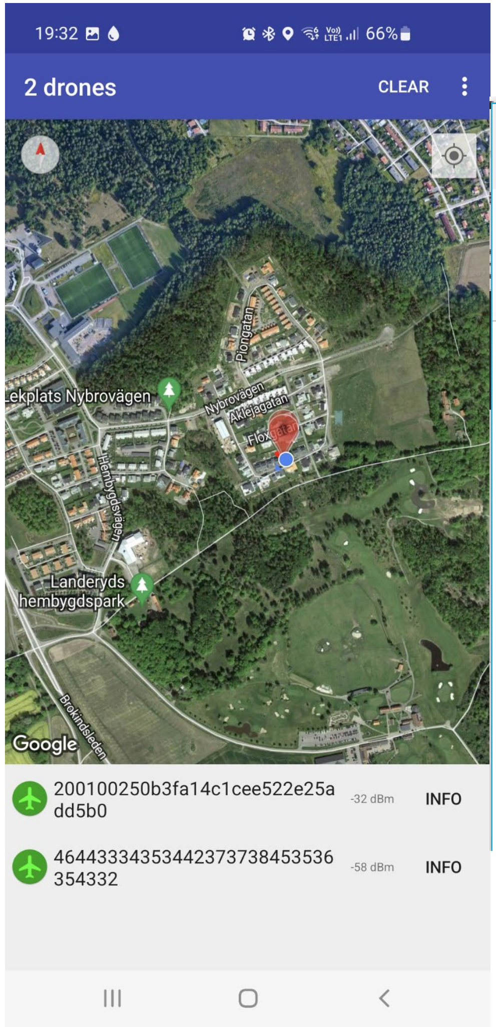
Location 0
Latitude 58.3654117
Longitude 15.7051900
Altitude Press. Unknown
Alt. Geod. 72.0 m
Direction 256 deg
Status Ground
Hori. Speed 0.00 m/s
Vert. Speed 0.00 m/s
Height Unknown
Height Over Takeoff
Hori. Accuracy Unknown
Vert. Acc. Unknown
Baro Acc. Unknown
Speed Acc. Unknown
Time Acc. Unknown
Timestamp 31:21

Self ID 0
Operation
Type 0

System/Operator 0
Latitude Unknown
Longitude Unknown
Location Invalid
Classification Undeclared
Category Undeclared
Class Undeclared
Area Count 0
Area Radius 0 m
Area Ceiling Unknown
Area Floor Unknown

Operator ID 0
Operator ID
Type 0

Authentication 0

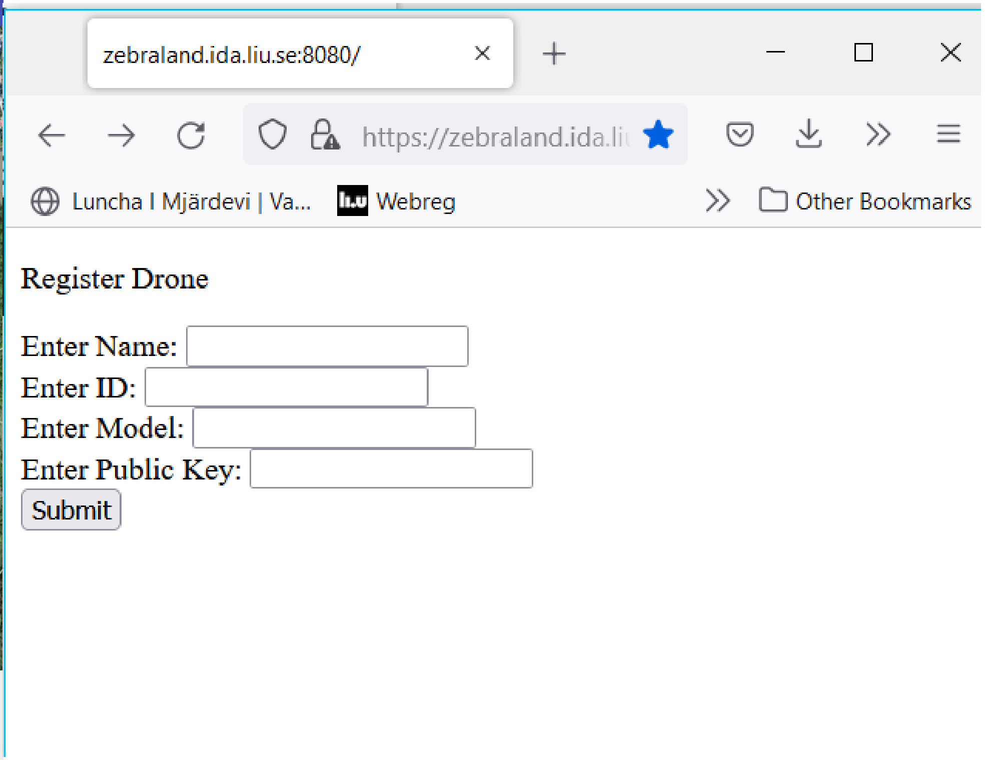


19:32 66%

2 drones CLEAR

200100250b3fa14c1cee522e25add5b0 -32 dBm INFO

464433343534423737384535363354332 -58 dBm INFO



zebraland.ida.liu.se:8080/

https://zebraland.ida.li

Luncha I Mjärdevi | Va... Webreg Other Bookmarks

Register Drone

Enter Name:

Enter ID:

Enter Model:

Enter Public Key:

Submit

# DRIP Interops & IETF hackathon

- Interops at IETF’115 Hackathon (London, Nov 2022)
  - HHIT format issues
  - Broadcast <-> app mutual compatibility
  - Adam Wiethuechter <adam.wiethuechter@axenterprize.com>
  - Their implementation is closed source
    - USA DoD demos at NY test site
  - Our (LiU) is open source
  - https://gitlab.liu.se/hamr0777/tdde21-drip-2022.git

# OpenHIP Updates

Host Identity Protocol (HIP) is the inspiration for DRIP, also for C&C

https://bitbucket.org/openhip/openhip/src/master/

HHIT support, new crypto, HIPv2 branches

Added Docker container for easier cross-platform installation and testing

# OpenSSL 3.0
# Current Status

- OpenHIP used OpenSSL 1.0.x
- Added support for OpenSSL 1.1.0 in Fall 2020
- OpenSSL 3.0.0 was released in September 2021
- 1.1.1 support ends in September 2023

- Current OpenSSL implementation lacks forward compatibility
- High cohesion in the code that uses OpenSSL
- Large amount of deprecated methods
- Not all deprecated methods have one-to-one equivalents in 3.0.0
- Code compiles, but needs testing