# Remote attestation over EDHOC draft-song-lake-ra-02

Yuxuan SONG

Inria

# New sections

- *Remote attestation in EDHOC*
  - Target
    - IoT device attestation (**IoT**)
    - Network service attestation (**Net**)
  - Model
    - Background-check model (**BG**)
    - Passport model (**PP**)
  - EDHOC message flow
    - EDHOC Forward message flow (**Fwd**)
    - EDHOC Reverse message flow (**Rev**)
- *Instantiation of Remote Attestation Protocol*
  - (IoT, BG, Fwd) IoT Device Attestation
  - (Net, PP, Fwd) Network Service Attestation

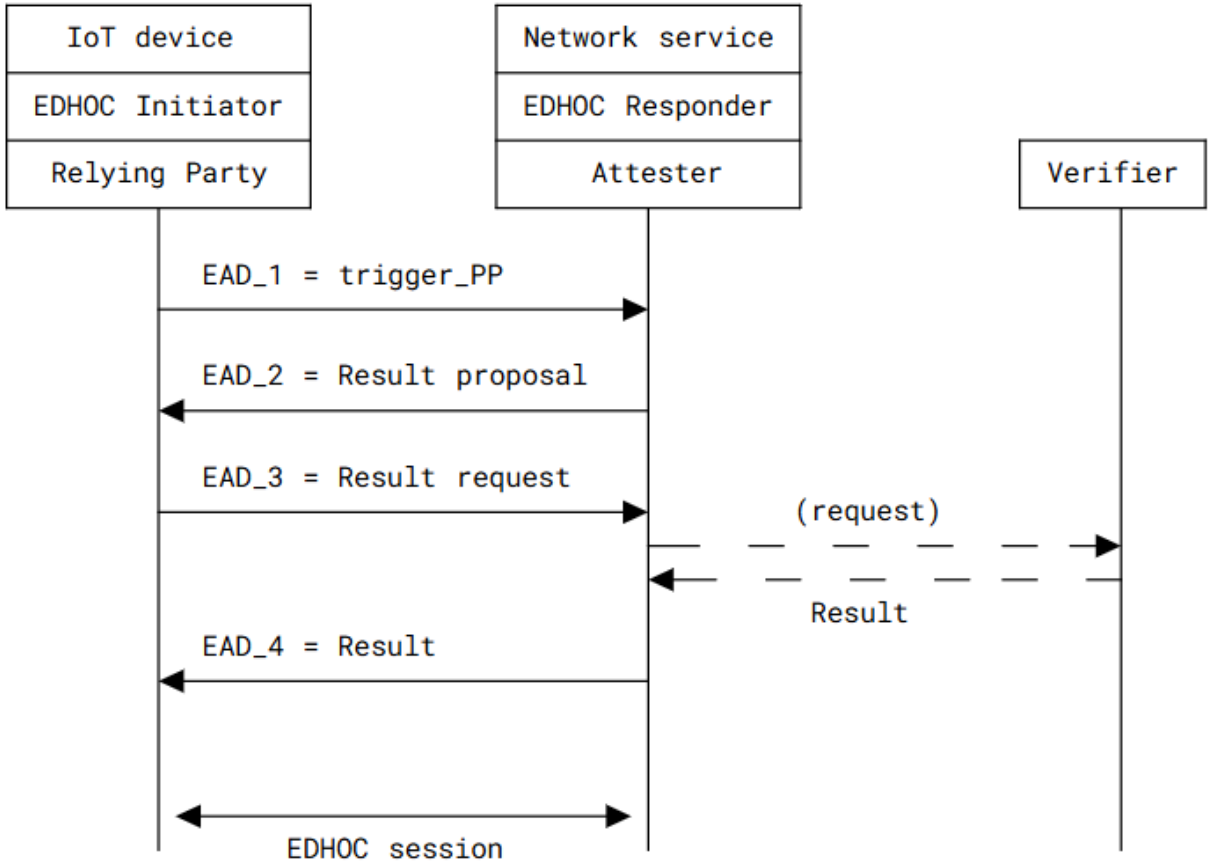
# New EAD items

- Trigger_BG
  - Trigger the receiver to start a remote attestation in background-check model
  - a ead_label with empty ead_value

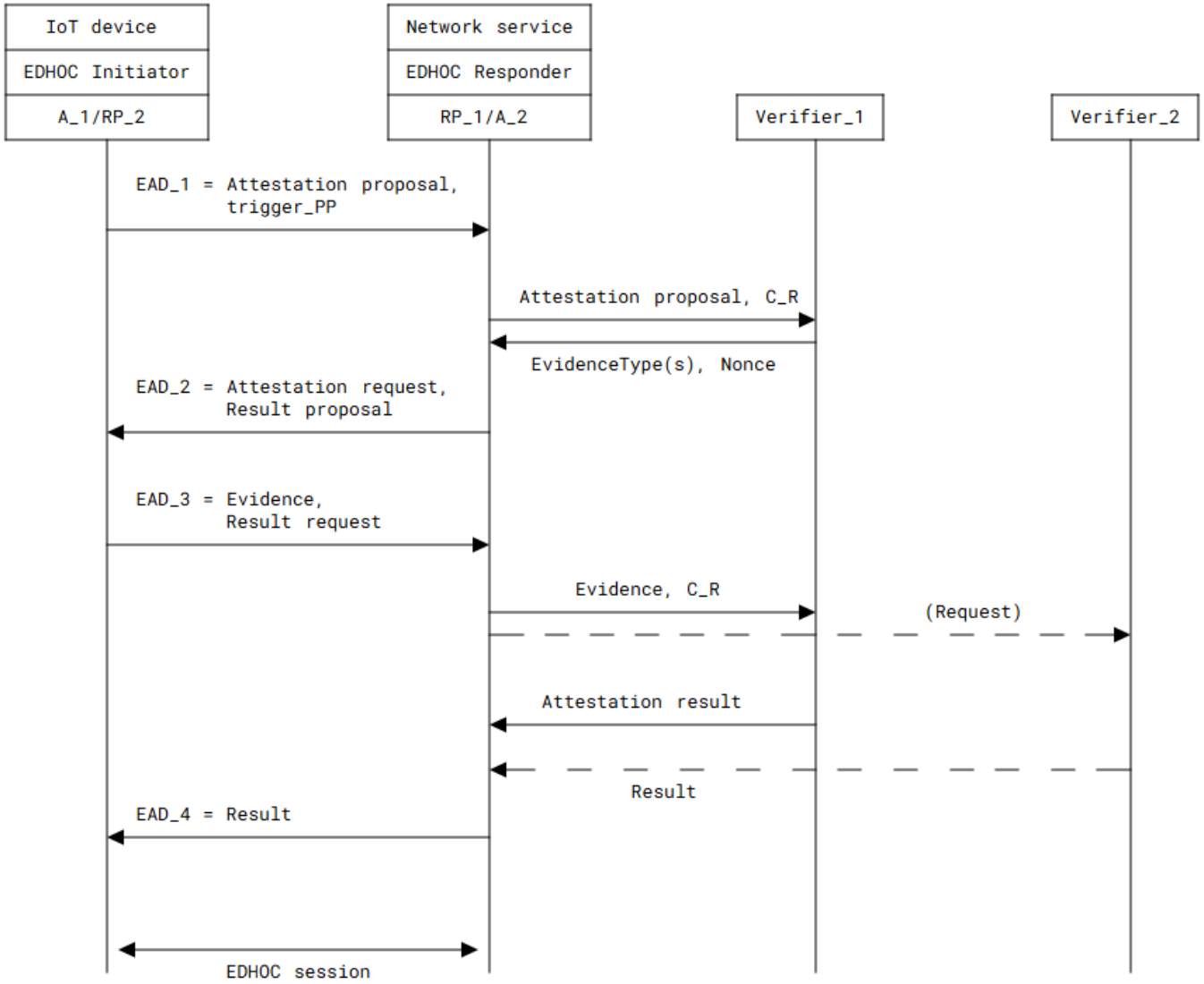
- Trigger_PP
  - Trigger the receiver to start a remote attestation in passport model
  - a ead_label with empty ead_value

# New Instantiation of remote attestation

## -**(Net, PP, Fwd)**: Network Service Attestation



# Update: Mutual attestation **(IoT, BG, Fwd) - (Net, PP, Fwd)**



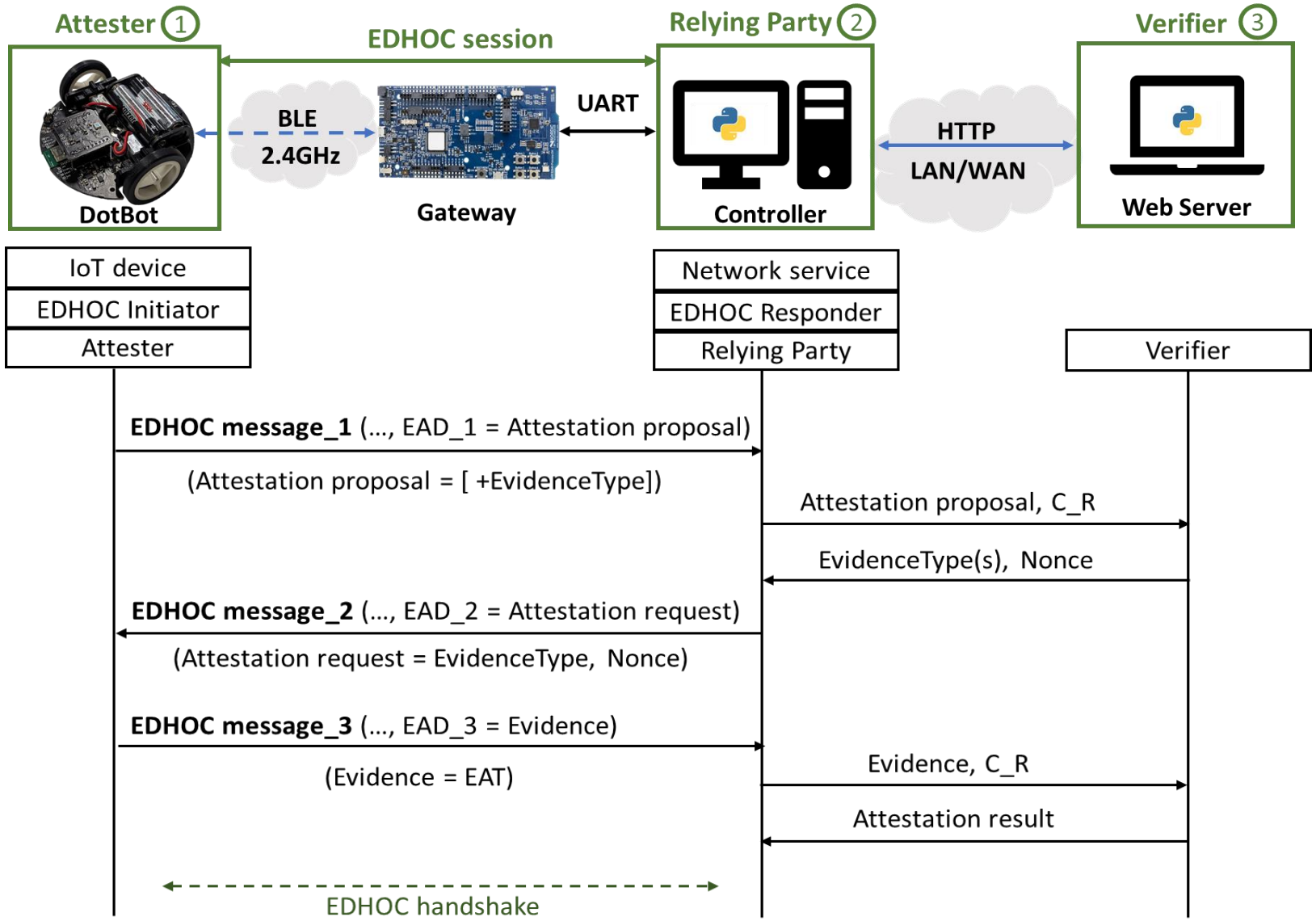
# Appendix C. Example: Firmware Version

Entity Attestation Token with measurements claim formatted in CoSWID [RFC9393]:

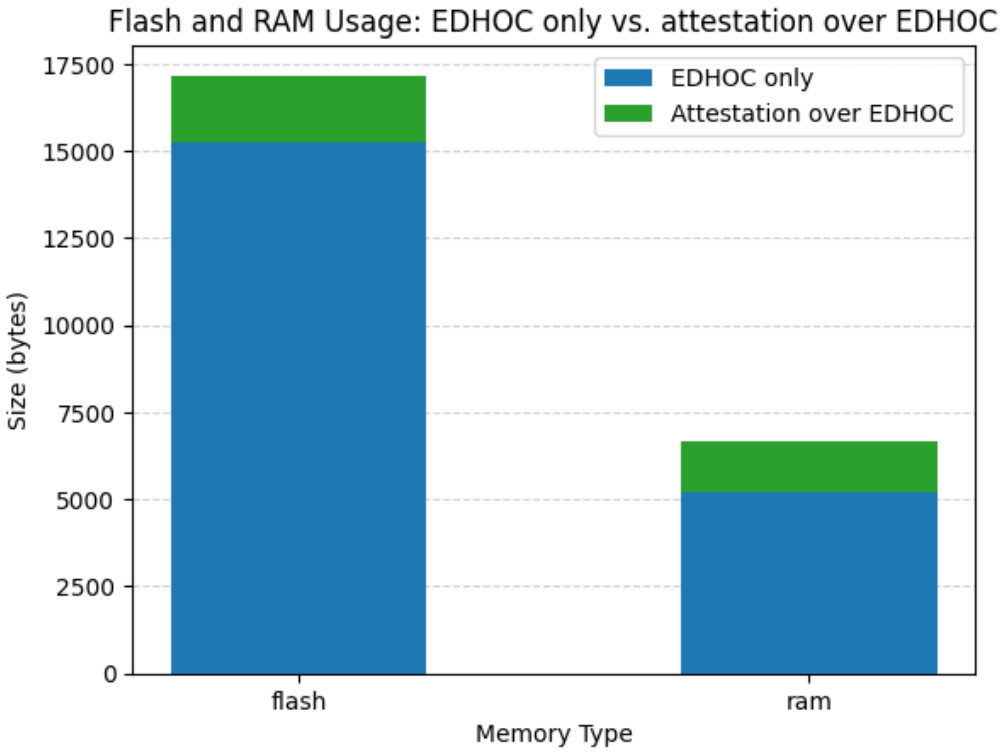
```
{
/eat-nonce/                10: h'a29f62a4c6cdaae5',
/ueid/                     256: 'aaabbcc',
/measurements/             273: [
 /CoAP Content-Format ID/      [ 258,
 /evidence in CoSWID/                {
                                       0: 'tagID'                                    /tag-id/
                                       12: 0                                         /tag-version/
                                       1: "DotBot firmware"                          /software-name/
                                       2: {                                          /entity/
                                           31: "Attester"                            /entity-name/
                                           33: 1                                     /role/
                                        },
                                       3: {                                          /evidence/
                                            17: [                                    /file/
                                                 {
                                              24: "03app_dotbot-nrf5340dk-app.bin", /fs-name/
                                              7: [                                  /hash of file/
                                               1,                                    /alg SHA-256/
                                               h'06294f6806b9c685eea795048579cfd02a0c025bc8b5abca42a19ea0ec23e81a'
                                                 ]                                   /hash value/
}]}}]]}
```

# Implementation of (IoT, BG, Fwd)

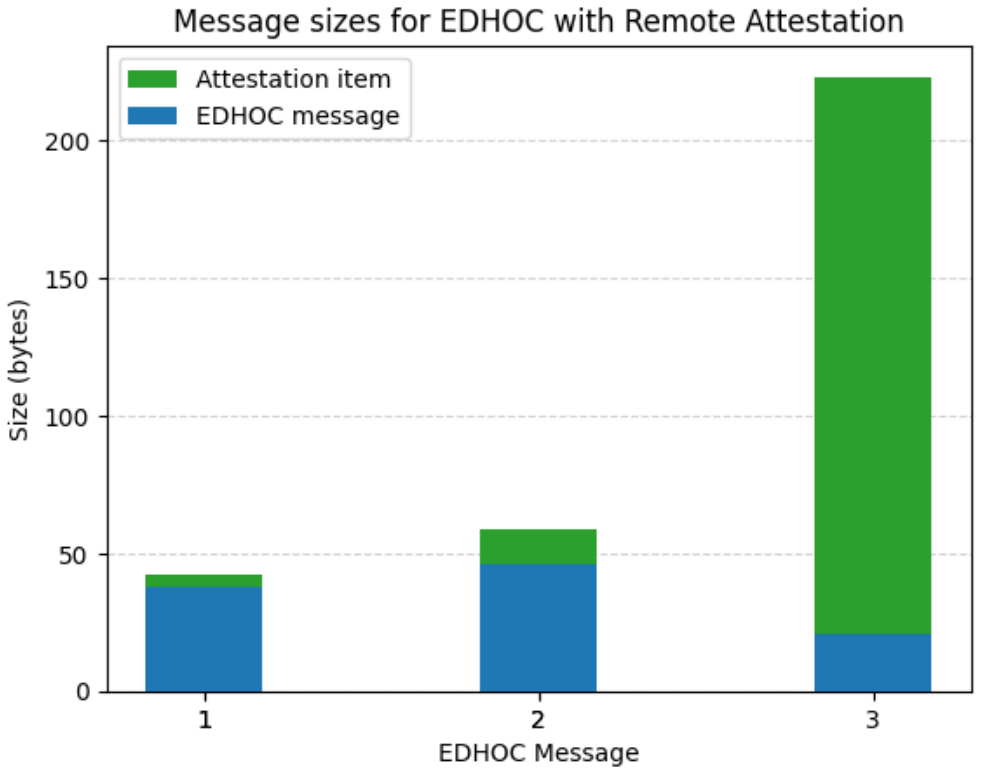
Attester: DotBot running on nRF5340 at 64MHz



# Evaluation results

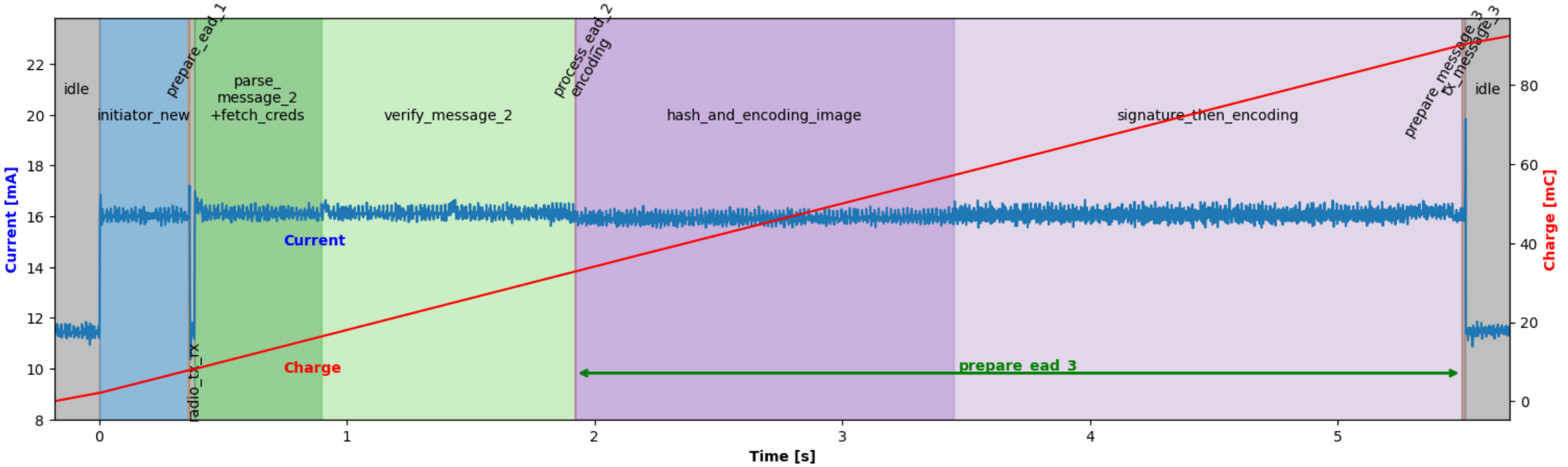



**Credential transport by reference**



# Current consumption benchmark

**Crypto done in software**



# Conclusion

- Restructured the draft
- Defined two new EAD items
- Full implementation and evaluation of the (IoT, BG, Fwd) attestation in the draft

# Next step

- Call for adoption?
- Implement mutual attestation

# Thank you!

Open for more discussions and collaborations: yuxuan.song@inria.fr

https://github.com/ysong02/draft-song-lake-ra

# Welcome any comments and advice ☺