Veracruz Attestation

Derek D. Miller

12 April 2022

Brand A Attestation Service

Brand B Attestation Service

Attester

Brand A System

Relying Party

Brand B System

CONFIDENTIAL COMPUTING CONSORTIUM

arm

Proxy Attestation Service

Brand A Attestation Service

Brand B Attestation Service

Brand A
Attestation
Service

Brand B
Attestation
Service

Proxy
Attestation
Service

© 2022 Arm
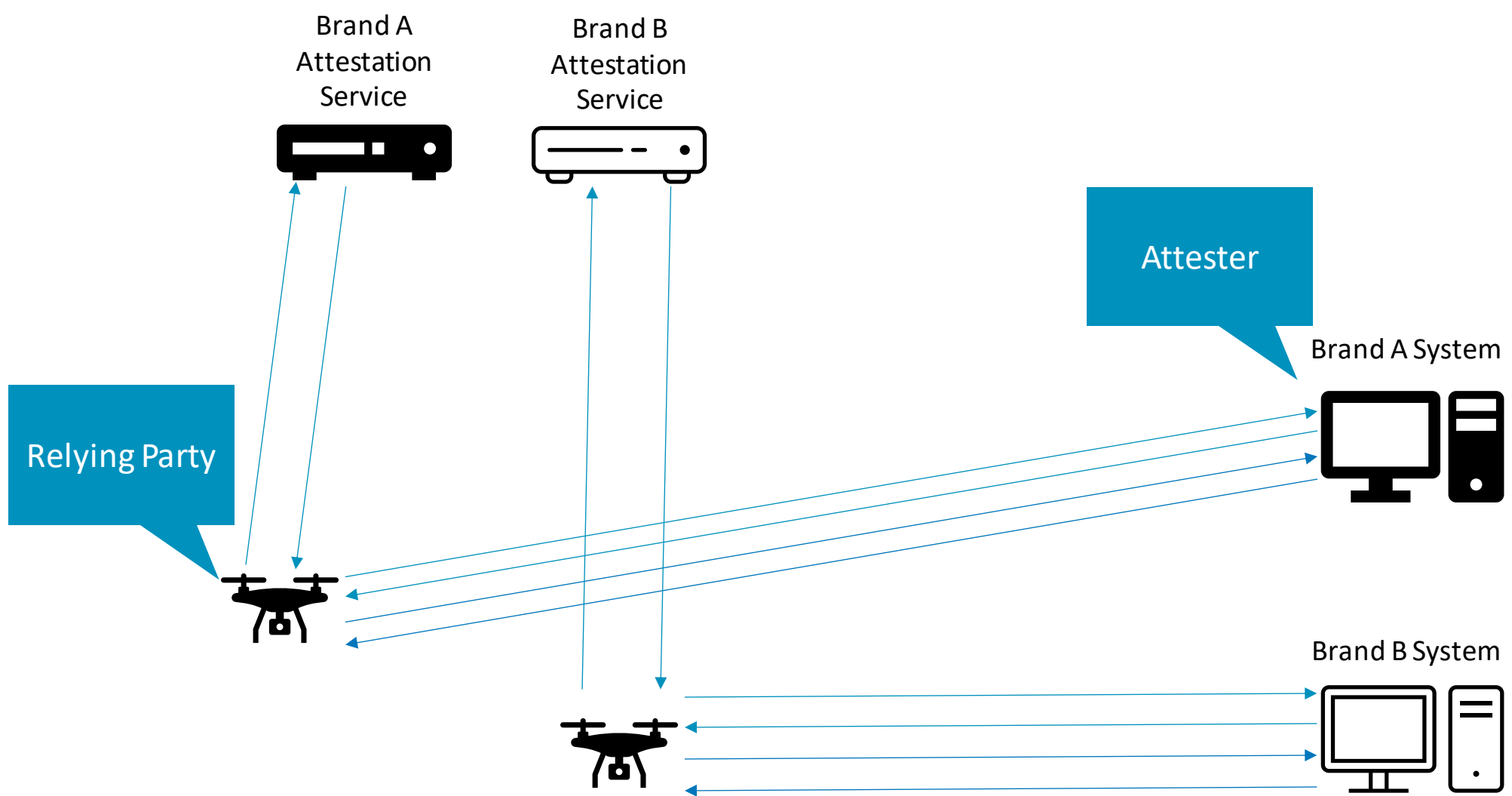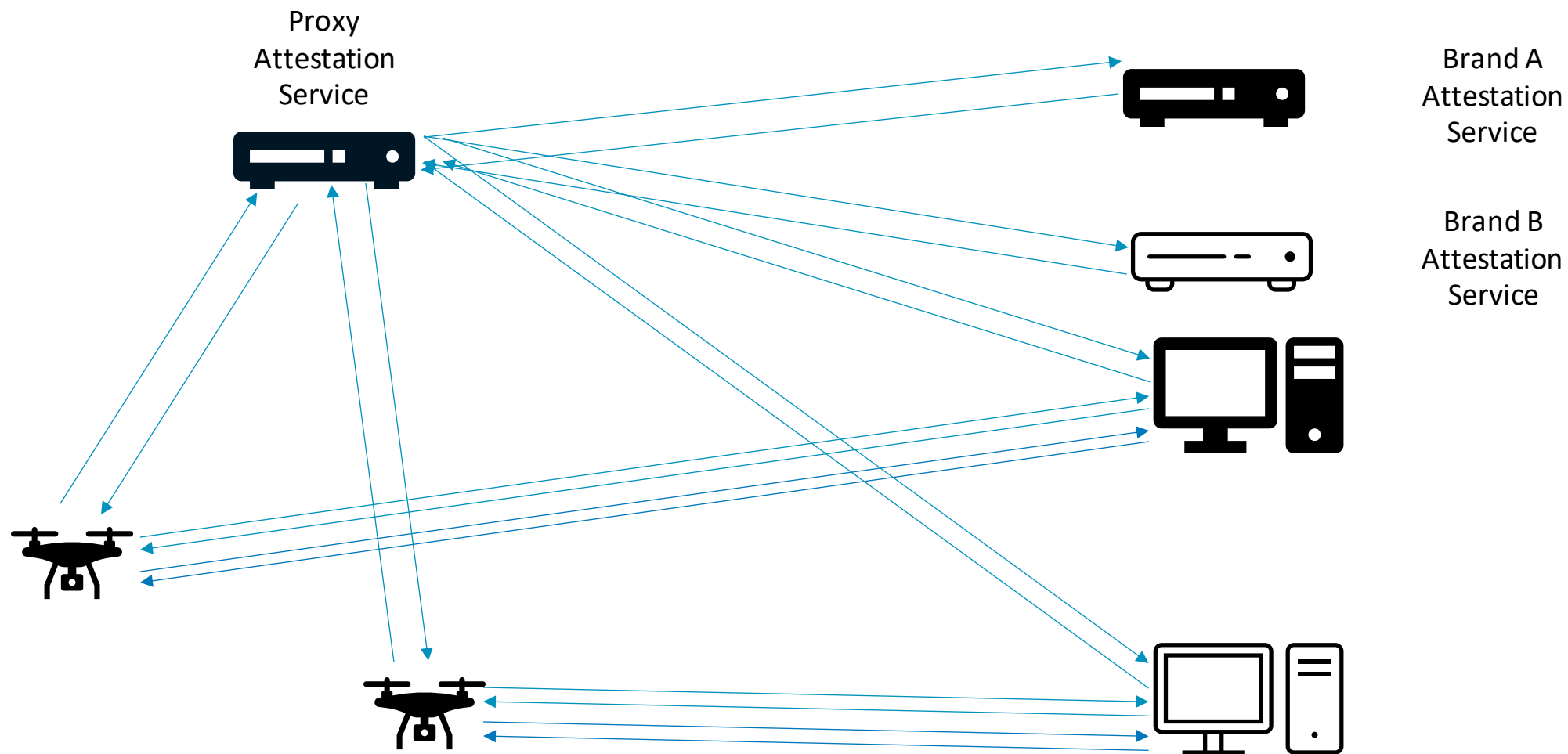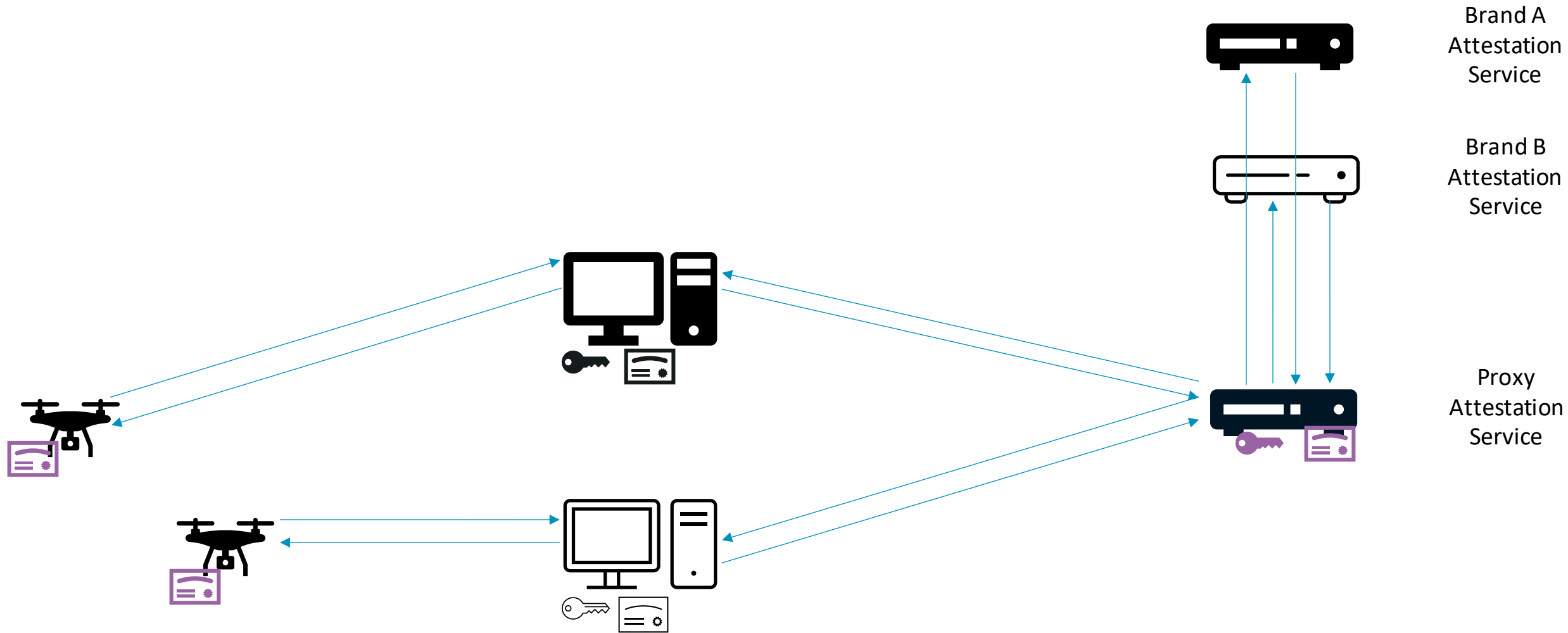
In the Style of the IETF RATS

```
***********        *************        *************        ******************
* Endorser *       * Reference *        * Verifier  *        * Relying Party  *
***********        * Value     *        *  Owner    *        *    Owner       *
    |              * Provider  *        *************        ******************
    |              *************            |                      |
    |                  |                     |                      |
    |Endorsements      |Reference            |Appraisal             |Appraisal
    |                  |Values               |Policy                |Policy for
    |                  |                     |for                   |Attestation
    |                  |                     |Evidence              |Results
 .----------.         |                     |                      |
             |        |                     |                      |
             |        |                     |                      |
             v        v                     v                      |
          .----------------------------------.                     |
 .------->|             Verifier             |------.              |
 |        '----------------------------------'       |             |
 |                                                   |             |
 |                                      Attestation| |             |
 |                                      Results    | |             |
 | Evidence                                        | |             |
 |                                                 v v
 .----------.                            .----------------.
 | Attester |                            | Relying Party  |
 '----------'                            '----------------'

            Figure 1: Conceptual Data Flow
```
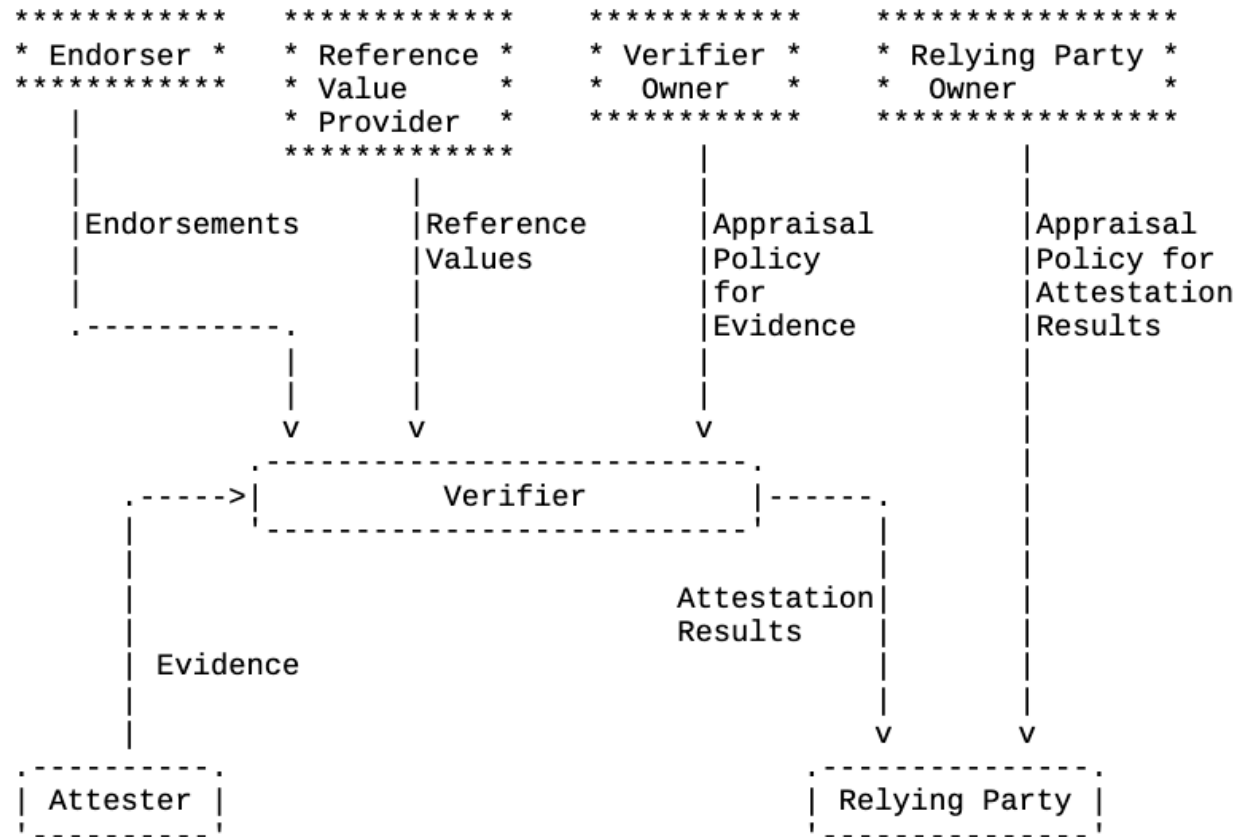
The Proxy attestation service acts as a passport issuer.
It acts as a Reference Value Provider/Verifier depending on the platform

The enclaves act as the Attester.

The clients are the Relying Party.

arm

arm

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

arm