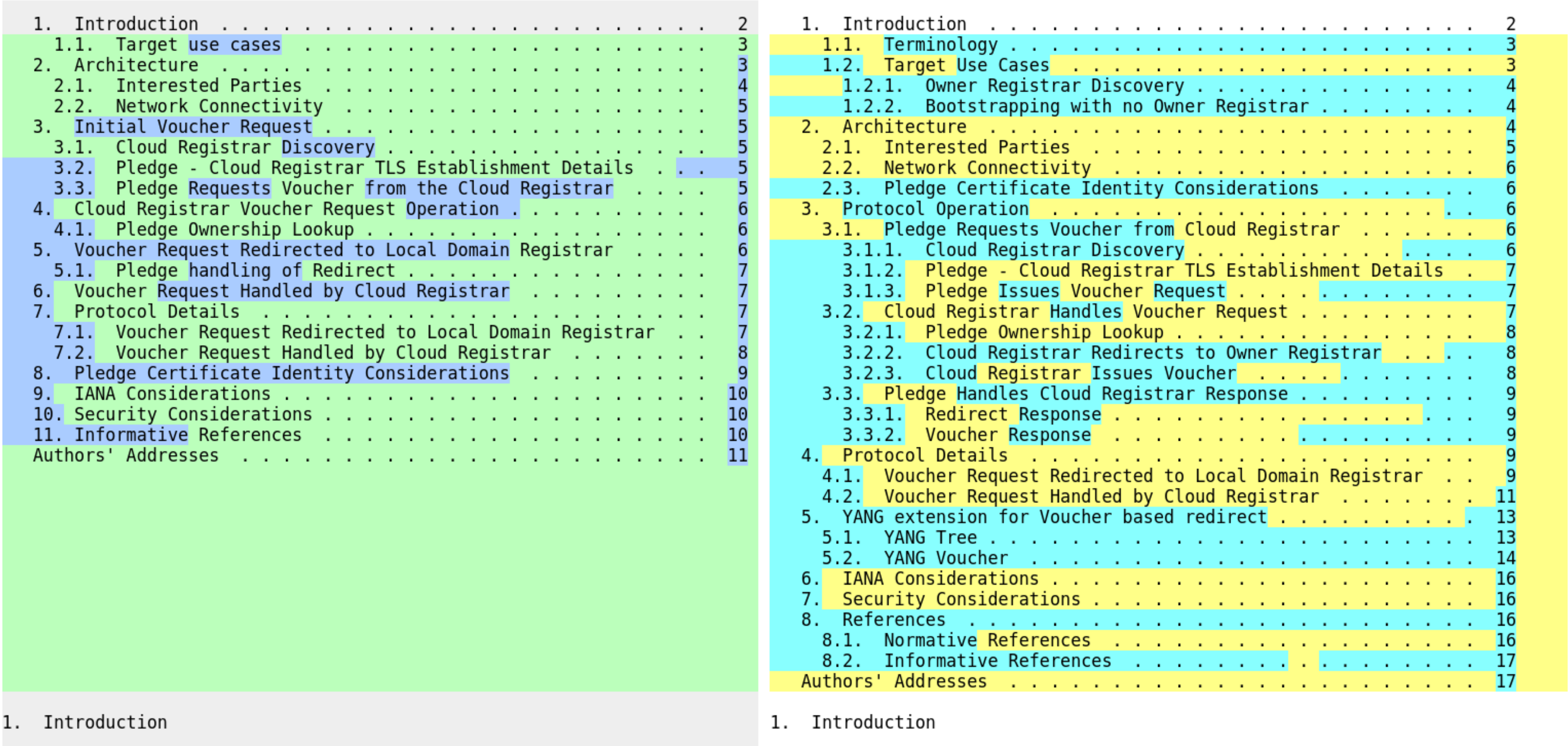
draft-friel-anima-brski-cloud-03

Authors:
Owen Friel (Cisco),
Rifaat Shekh-Yusef (Auth0),
Michael Richardson (SSW)

IETF 109 – not Bangkok

Irresponsible party who created slides:
Michael Richardson
mcr+ietf@sandelman.ca

Changes since -02: Table of Contents



1. Introduction

1. Introduction

Substantive changes to brski-cloud

https://www.ietf.org/rfcdiff?url1=draft-friel-anima-brski-cloud-02&url2=draft-friel-anima-brski-cloud-03

- Reworked terminology
- Two key use cases:
  - 1.2.1. Owner Registrar Discovery
  - 1.2.2. Bootstrapping with no Owner Registrar
- YANG addition to voucher: est-domain
- YANG addition to voucher: additional-configuration

Terminology

Local Domain: The domain where the pledge is physically located and bootstrapping from.

This may be different to the pledge owner's domain.

Owner Domain: The domain that the pledge needs to discover and bootstrap with.

Cloud Registrar: The default Registrar that is deployed at a URI that is well known to the pledge.

Owner Registrar: The Registrar that is operated by the Owner, or the Owner's delegate.

There may not be an Owner Registrar in all deployment scenarios.

Local Domain Registrar: The Registrar discovered on the Local Domain.

There may not be a Local Domain Registrar in all deployment scenarios.

Owner Registrar Discovery

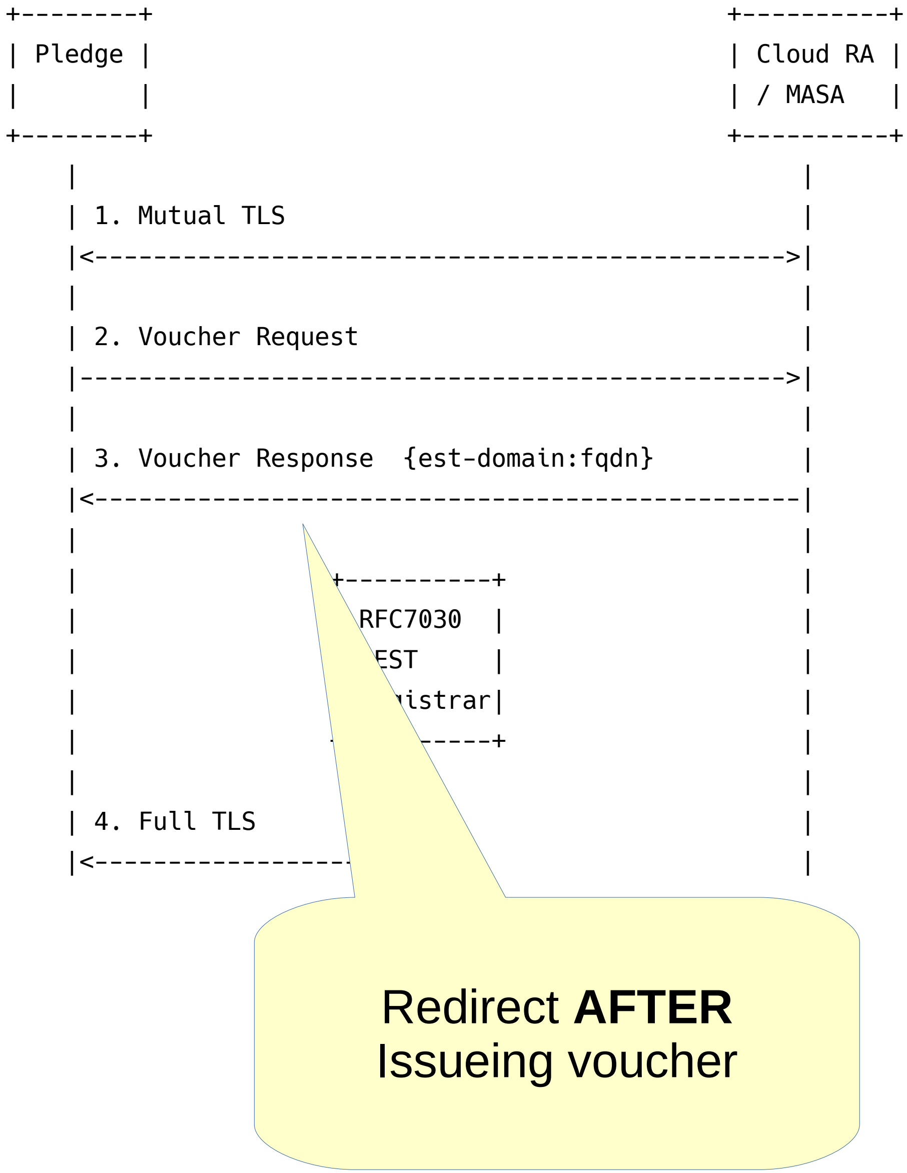
- When there is no local infrastructure to provide join proxy
  - But, enterprise has BRSKI Registrar
  - For devices that plug-in (wired), or for which wifi /802.15.4 is not relevant!
  - For instance sending a (new) device home with a employee during a... pandemic

```
+---------+                                      +----------+
| Pledge  |                                      | Cloud RA |
|         |                                      |          |
+---------+                                      +----------+
    |                                                 |
    | 1. Mutual-authenticated TLS                     |
    |<----------------------------------------------->|
    |                                                 |
    | 2. Voucher Request                              |
    |------------------------------------------------>|
    |                                                 |
    | 3. 307 Location: owner-ra.example.com           |
    |<------------------------------------------------|
    |
    |                  +-----------+             +---------+
    |                  | Owner     |             |  MASA   |
    |                    Registrar |             |         |
    |                      --------+             +---------+
    | 4. Provisional T                                |
    |<----------------                                |
```

Redirect **BEFORE** Issueing voucher

Bootstrapping (to EST) with no Owner Registrar

- When there is no local infrastructure to provide join proxy
  - But, enterprise has ordinary EST/RFC7030 Registrar
  -



```
+--------+                                               +----------+
| Pledge |                                               | Cloud RA |
|        |                                               | / MASA   |
+--------+                                               +----------+
    |                                                         |
    | 1. Mutual TLS                                           |
    |<------------------------------------------------------->|
    |                                                         |
    | 2. Voucher Request                                      |
    |-------------------------------------------------------->|
    |                                                         |
    | 3. Voucher Response  {est-domain:fqdn}                  |
    |<--------------------------------------------------------|
    |                                                         |
    |                        +----------+                     |
    |                         RFC7030  |                      |
    |                          EST     |                      |
    |                           istrar|                       |
    |                             -----+                      |
    |                                                         |
    | 4. Full TLS                                             |
    |<------------------                                      |
```

Redirect **AFTER** Issueing voucher

Questions?

Adopt?