

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	2
1.1. Target use cases	3
2. Architecture	3
2.1. Interested Parties	4
2.2. Network Connectivity	5
3. Initial Voucher Request	5
3.1. Cloud Registrar Discovery	5
3.2. Pledge - Cloud Registrar TLS Establishment Details	5
3.3. Pledge Requests Voucher from the Cloud Registrar	5
4. Cloud Registrar Voucher Request Operation	6
4.1. Pledge Ownership Lookup	6
5. Voucher Request Redirected to Local Domain Registrar	6
5.1. Pledge handling of Redirect	7
6. Voucher Request Handled by Cloud Registrar	7
7. Protocol Details	7
7.1. Voucher Request Redirected to Local Domain Registrar	7
7.2. Voucher Request Handled by Cloud Registrar	8
8. Pledge Certificate Identity Considerations	9
9. IANA Considerations	10
10. Security Considerations	10
11. Informative References	10
Authors' Addresses	11

1. Introduction

1. Introduction	2
1.1. Terminology	3
1.2. Target Use Cases	3
1.2.1. Owner Registrar Discovery	4
1.2.2. Bootstrapping with no Owner Registrar	4
2. Architecture	4
2.1. Interested Parties	5
2.2. Network Connectivity	6
2.3. Pledge Certificate Identity Considerations	6
3. Protocol Operation	6
3.1. Pledge Requests Voucher from Cloud Registrar	6
3.1.1. Cloud Registrar Discovery	6
3.1.2. Pledge - Cloud Registrar TLS Establishment Details	7
3.1.3. Pledge Issues Voucher Request	7
3.2. Cloud Registrar Handles Voucher Request	7
3.2.1. Pledge Ownership Lookup	8
3.2.2. Cloud Registrar Redirects to Owner Registrar	8
3.2.3. Cloud Registrar Issues Voucher	8
3.3. Pledge Handles Cloud Registrar Response	9
3.3.1. Redirect Response	9
3.3.2. Voucher Response	9
4. Protocol Details	9
4.1. Voucher Request Redirected to Local Domain Registrar	9
4.2. Voucher Request Handled by Cloud Registrar	11
5. YANG extension for Voucher based redirect	13
5.1. YANG Tree	13
5.2. YANG Voucher	14
6. IANA Considerations	16
7. Security Considerations	16
8. References	16
8.1. Normative References	16
8.2. Informative References	17
Authors' Addresses	17

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.

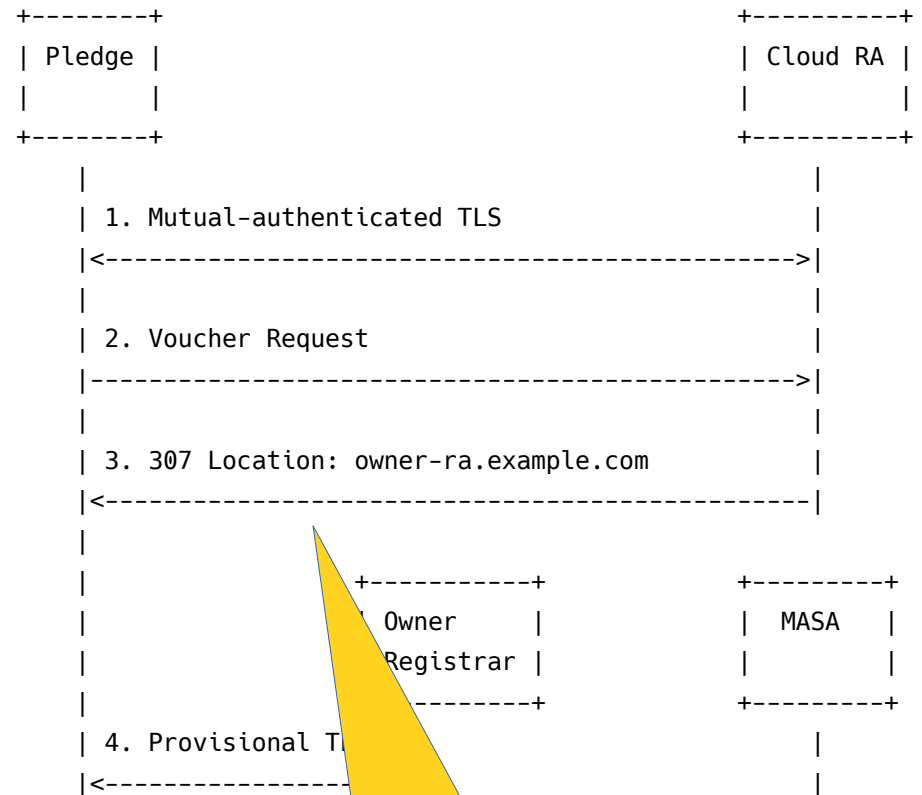
Cloud Registrar: The default Registrar that is deployed at a URI that is well known to the pledge.

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

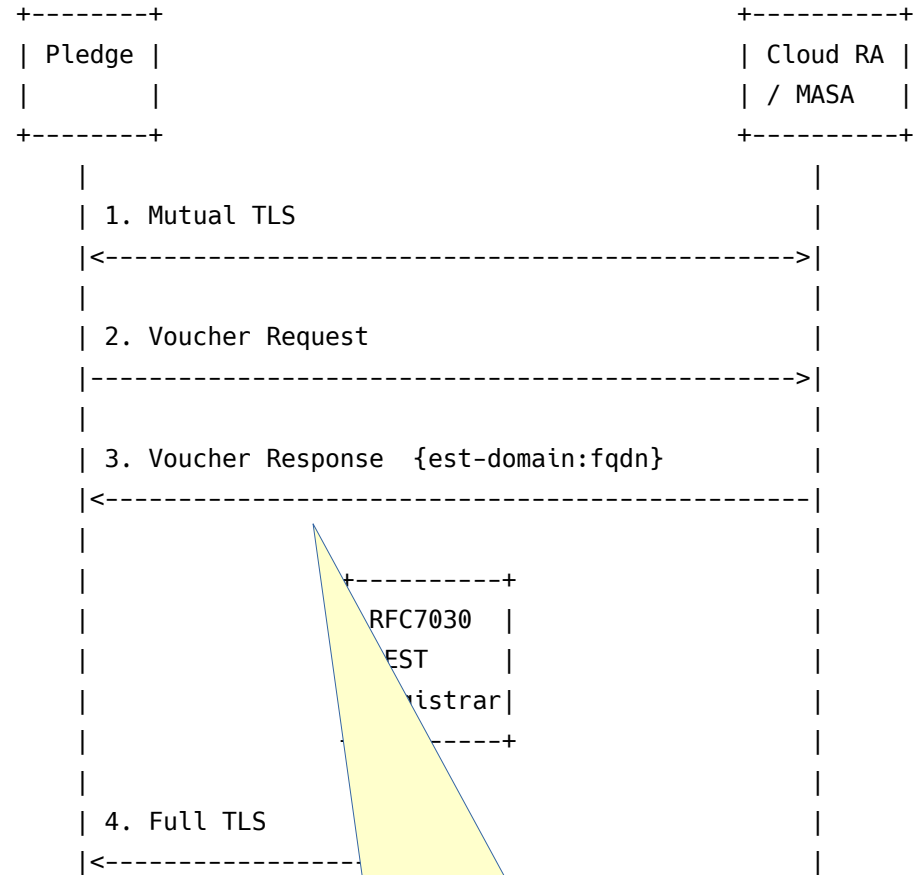
- When there is no local infrastructure to provide join proxy
 - But, enterprise has BRSKI Registrar
 - For devices that plug-in (wired), or for which wifi /802.15.4 is not relevant!
 - For instance sending a (new) device home with a employee during a... pandemic



Redirect **BEFORE**
Issuing 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



Redirect **AFTER**
Issuing voucher

Questions?

Adopt?