

draft-ietf-anima-brski-cloud-01

Authors:

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

IETF 111 – not San Francisco

Irresponsible party who created slides:

Michael Richardson
mcr+ietf@sandelman.ca

Changes since adoption of -03

Table of Contents

<https://www.ietf.org/rfcdiff?url1=draft-friel-anima-brski-cloud-03&url2=draft-ietf-anima-brski-cloud-01>

Table of Contents	
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

Table of Contents	
1. Introduction	3
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	5
2.1. Interested Parties	6
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	7
3.1.2. Pledge - Cloud Registrar TLS Establishment Details	7
3.1.3. Pledge Issues Voucher Request	8
3.2. Cloud Registrar Handles Voucher Request	8
3.2.1. Pledge Ownership Lookup	8
3.2.2. Cloud Registrar Redirects to Owner Registrar	8
3.2.3. Cloud Registrar Issues Voucher	9
3.3. Pledge Handles Cloud Registrar Response	9
3.3.1. Redirect Response	9
3.3.2. Voucher Response	9
4. Protocol Details	10
4.1. Voucher Request Redirected to Local Domain Registrar	10
4.2. Voucher Request Handled by Cloud Registrar	12
5. YANG extension for Voucher based redirect	14
5.1. YANG Tree	14
5.2. YANG Voucher	15
6. IANA Considerations	17
6.1. The IETF XML Registry	17
6.2. The YANG Module Names Registry	17
7. Security Considerations	17
8. References	18
8.1. Normative References	18
8.2. Informative References	18
Authors' Addresses	19

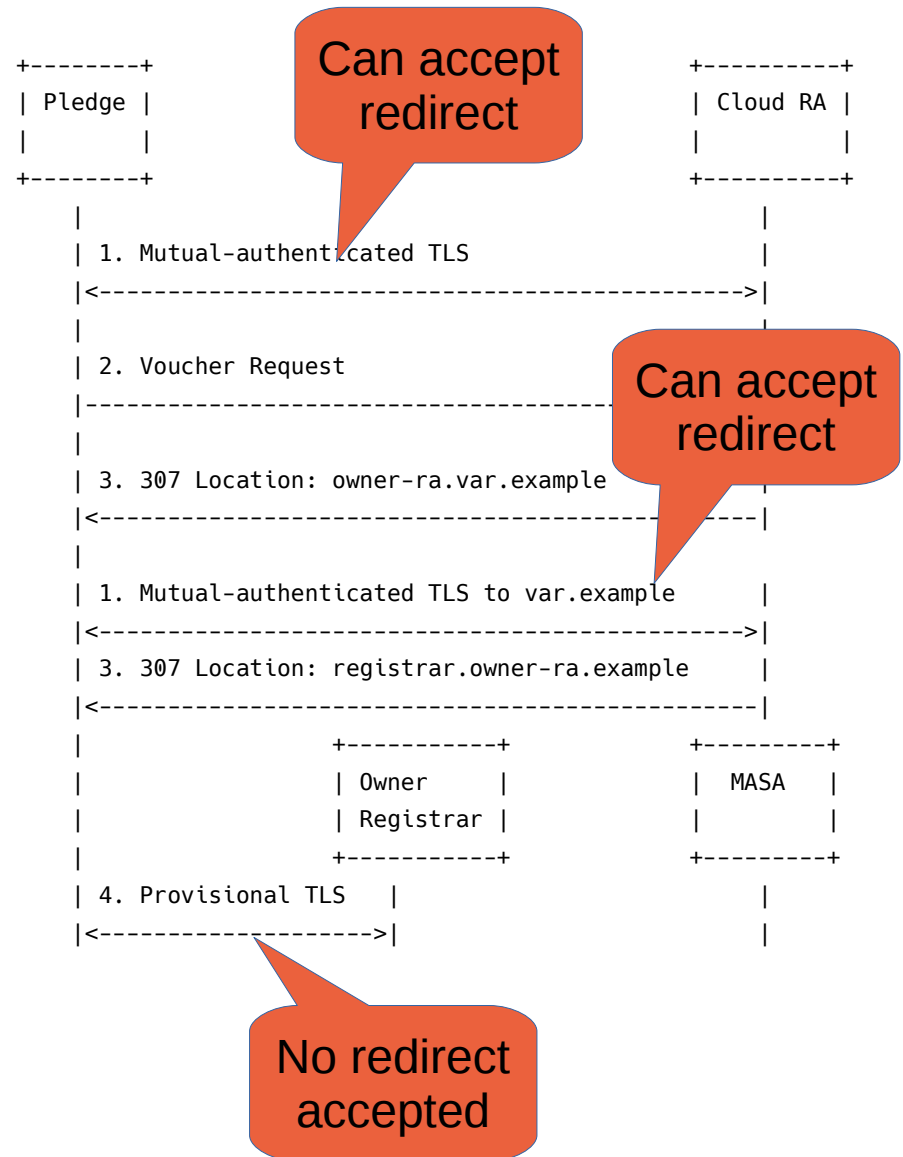
WG adopted Document on April 28, 2021 Thank you!

Things still to do

- Security Considerations
 - <https://github.com/anima-wg/brski-cloud/pull/7>
 - Issues with Security of HTTP Redirect
 - Security Updates for the Pledge
 - Trust Anchors for Cloud Registrar
 - Issues with Redirect via Voucher
- Applicability Statement needed to match RFC8995
- How and when to allow multiple 307 redirects
 - <https://github.com/anima-wg/brski-cloud/pull/8/files>

Multiple Redirects?

- Provisional TLS connection can be hijacked
 - But will eventually be validated by voucher
- Cloud Registrar connection is RFC6125 validated
 - Can accept 307 redirect
- If new destination can be validated with RFC6125
 - Then can also accept 307 redirect



WG-wide issue on RFC8366 derivatives

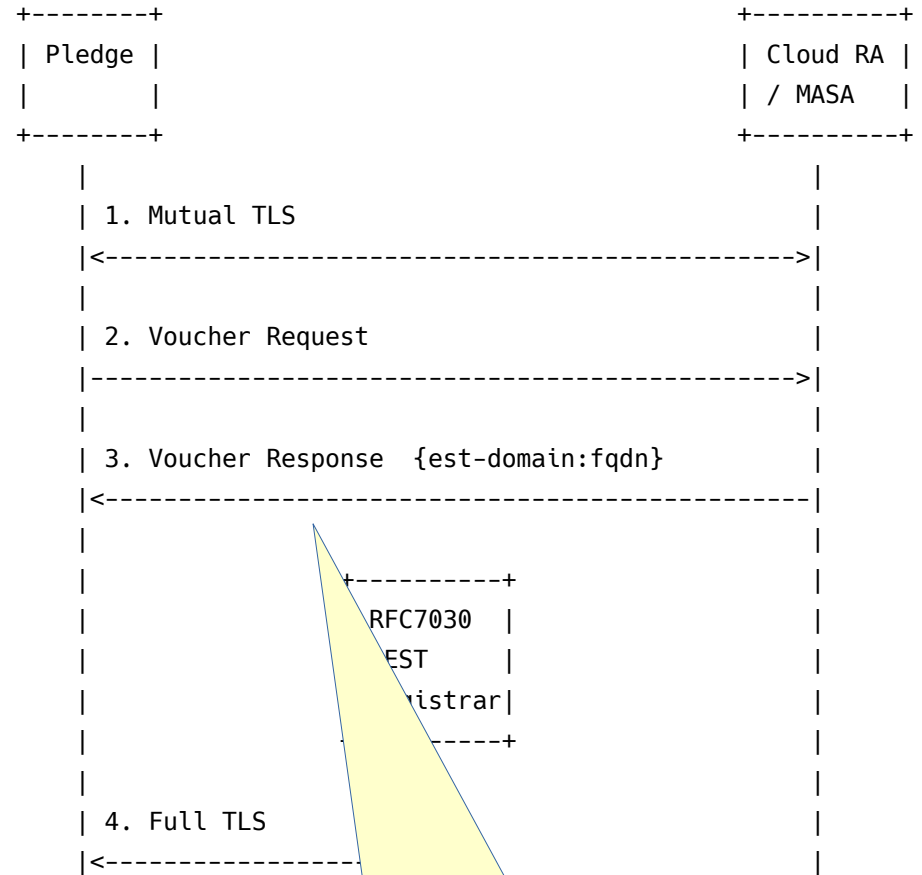
- ietf-FOOBAR-voucher sorts and associates poorly with other ietf-voucher things
- Suggest that we always call them ietf-voucher-FOOBAR
- YANG module renamed from “ietf-redirected-voucher” to “ietf-voucher-redirected”
- So also:
 - ietf-constrained-voucher -> ietf-voucher-constrained
 - ietf-constrained-voucher-request -> ietf-voucher-request-constrained
 -

Questions?

Adopt?
(aux slides follow)

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